SYNGRESS®

Zero-Day Exploit

COUNTDOWN TO DARKNESS

"So much of our critical national infrastructure hinges on technology, which is so fragile, that a zero-day bug in the wrong hands could lead to any equally bad attack. I'm not, for a moment, going to speculate on what or how that attack may come, but suffice to say that the potential is there; the threat is real."

—David Litchfield, Managing Director, NGSSoftware

Rob Shein (Rogue Shoten)
Marcus H. Sachs Technical Editor

FOREWORD BY DAVID LITCHFIELD

Register for Free Membership to

solutions@syngress.com

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2000*, Brian Caswell and Jay Beale's *Snort 2.0 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy to search web page, providing you with the concise, easy to access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

SYNGRESS®

Zero Day Exploit

COUNTDOWN TO DARKNESS

Rob Shein aka Rogue Shoten
Marcus H. Sachs Technical Editor

KEY	SERIAL NUMBER
001	NKLOP45D5F
002	PO9823DN72
003	822NBVVG42
004	NMKOPW4W4H
005	C6WQ23BV88
006	VBP9NAAQ39
007	HJJEBB772M
008	298MKVBPPL
009	62DJT49725
010	IM6TVBH639

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Zero-Day Exploit: Countdown to Darkness

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 1-931836-09-4

Acquisitions Editor: Christine Kloiber
Technical Editor: Marcus H. Sachs

Cover Designer: Michael Kavish
Copy Editor: Amy Thomson
Page Layout and Art: Patricia Lupien

Distributed by O'Reilly Media, Inc. in the United States and Canada.

Acknowledgments

We would like to acknowledge the following people for their kindness and support in making this book possible.

A special thank you to David Litchfield of NGSSoftware, one of the true poineers in the world of computer security, for sharing his insight on 0-day vulnerabilities in the Foreword of this book.

Jeff Moss and Ping Look from Black Hat, Inc. You have been good friends to Syngress and great colleagues to work with. Thank you!

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc. The enthusiasm and work ethic at O'Reilly is incredible and we would like to thank everyone there for their time and efforts to bring Syngress books to market: Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Lynn Schwartz, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop, Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, and Rob Bullington.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack, and Krista Leppiko, for making certain that our vision remains worldwide in scope.

David Buckland, Daniel Loh, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Geoff Ebbs, Hedley Partis, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.

Author

Photo by Scott Suchman

Rob Shein, also known as **Rogue Shoten**, works as an independent consultant in the Washington, DC area. Rob has worked in the IT field for approximately a decade, with the past six years focused on information security. He learned to program at the age of eleven, and computers have been a passion of his ever since. His experience includes doing hard time at Network Solutions, followed by VeriSign, where he was a member of the FIRE Team, providing incident response, vulnerability assessment, risk mitigation and penetration testing services. He also served on a red-team at Titan, during which time he did work he's not supposed to even talk about to himself. Work in recent years has included consulting to several Fortune 100 corporations, USDA, the Treasury Department, and the United States Army. Rob has presented at several conferences, including DefCon and e-Gov, and is currently working on a book covering home computer security for non-technical users. His greatest love is resolving significant problems under intense pressure, which explains both his affinity for incident response and the way he drives.

Technical Editor

Marcus H. Sachs is the Director of the SANS Internet Storm Center and is a cyberspace security researcher, writer, and instructor for the SANS Institute. He previously served in the White House Office of Cyberspace Security and was a staff member of the President's Critical Infrastructure Protection Board. While a member of the White House staff, Marcus coordinated efforts to protect and secure the nation's telecommunication and Internet infrastructures, leveraging expertise from United States government agencies, the domestic private sector, and the international community. He also contributed to the National Strategy to Secure Cyberspace, upon his joining of the National Cyber Security Division of the US Department of Homeland Security. While working for DHS, he developed the initial concept and strategy for the creation of the United States Computer Emergency Response Team. Marcus retired from the United States Army in 2001 after serving over 20 years as a Corps of Engineers officer. He specialized during the later half of his career in computer network operations, systems automation, and information technology.

Foreword Contributor

David Litchfield leads the world in the discovery and publication of computer security vulnerabilities. This outstanding research was recognized by Information Security Magazine who voted him as 'The World's Best Bug Hunter' for 2003. To date, David has found over 150 vulnerabilities in many of today's popular products from the major software companies (including Microsoft and Oracle).

David is also the original author for the entire suite of security assessment tools available from NGSSoftware. This includes the flagship vulnerability scanner Typhon III, the range of database auditing tools NGSSquirrel for SQL Server, NGSSquirrel for Oracle, OraScan and Domino Scan II.

In addition to his world leading vulnerability research and the continued development of cutting edge security assessment software, David has also written or co-authored on a number of security related titles including, *SQL Server Security*, *Shellcoder's Handbook* and *Special Ops: Host and Network Security for Microsoft, UNIX and Oracle* (Syngress Publishing, ISBN: 1-931836-69-8).

Appendix Contributor

Ryan Russell (aka Blue Boar) has worked in the IT field for over 13 years, focusing on information security for the last seven. He was the lead author of *Hack Proofing Your Network, Second Edition* (Syngress, ISBN: 1-928994-70-9), contributing author and technical editor of *Stealing The Network: How to Own The Box* (Syngress, ISBN: 1-931836-87-6) and *Stealing the Network: How to Own a Continent* (Syngress, ISBN: 1-931836-05-1), and is a frequent technical editor for the Hack Proofing series of books from Syngress. Ryan was also a technical advisor on *Snort 2.0 Intrusion Detection* (Syngress, ISBN: 1-931836-74-4). Ryan founded the vuln-dev mailing list, and moderated it for three years under the alias "Blue Boar." He is a frequent lecturer at security conferences, and can often be found participating in security mailing lists and website discussions. Ryan is the QA Manager at BigFix, Inc.

Author Acknowledgements

I spent a lot of time pondering who to thank, and why. When tallying up everyone in my life who has had a real impact on this effort, I'm overwhelmed by the list. And it's very difficult to restrict myself to recent events as well; I can think of people whose support years ago laid the first pavement of the road that led here. And there's always the fear of having to rate the various people in order of their impact, which is utterly impossible. Last of all, I won't be mentioning the name of everyone I need to thank, and so for those who are included in "all the guys," or some similar phrase, please do forgive me.

So, let me begin in a semi-chronological order, rather than try to rank people. I would like to start off with my colleagues from LAN Solutions, way back in the day. Spencer, Vic, Matt, Alyssa, Steve and everyone else. Working with you was amazing, and while there, I really started to engage my own potential, and see what I could accomplish down the road. I never saw a book in my future, but I don't believe for a moment that I'd be writing this right now but for my experiences working there.

I want to thank Mala for her support, and her inspiration as an example of how grounded a person can be. She helped me come up with the moniker that became my primary "hacker undergound" alias…"Shoten." I know I kept rescheduling, but really, we will sit down for a drink someday this year (I promise) and catch up. I've just been really busy!

I also want to thank Buddy Horton, Bob Richel, Ahmad Habib, Chris Stark, and my other red-team colleagues from Titan. I loved working with you guys, and we need to get together for lunch at some point. Also, the guys from the SOC…Rob, who christened me "Rogue", Bart, Vlad, and the rest. I do hope I'll get to work with at least some of you again down the road.

I need to thank Drew Miller for being a friend, a colleague, and an amazing hacker. Of all people I've ever worked with, you're the one I most hope to work with again. (Hey, it's *mad fast*!) I'd like to thank Jeff Moss as well, for his seemingly thankless role for coordinating DefCon and the Black Hat Briefings.

A big hello to the members of the former FIRE Team, who I loved working with during my days at VeriSign. It was an honor to work with all of

you, and I still feel what I said back at the Rodeo dinner. And hello, Ren, I hope travel has been easy on you.

Thank you, Lee, for helping me hold everything together. I want to thank my circle of friends in general for being good friends and good supporters. I especially want to thank Rich and Jon, Rich for being a special voice of reason as well as someone to admire, and Jon for being almost fanatical in his support. Writing a novel is a particularly scary thing when you've never written fiction before. The support of my friends and the occasional reality check made the difference, helping me see this not as a hopelessly huge challenge but as an opportunity that many hope for but few get.

I want to thank my trio of safe havens, where I would go to write or just to unload my mind and relax. *Tryst*, the coffee house mentioned in this book, is entirely real, and I recommend it without hesitation. If you're ever in DC and want a good cup of coffee, do stop by. *The Reef*, also mentioned in the book, is a fantastic place to go at night, particularly for a local, and Brian is as real as I could portray him. The people who run Reef are a special group, and the place is truly sacred to me. And I want to thank David from *Chez Antoine*, for the hospitality, coffee, beer, and electrical power for my laptop as I cranked out marathon writing sessions.

I want to thank everyone at Syngress for the way they welcomed and supported me, but especially Christine (my editor), Marc (my technical editor), and Andrew, who first asked me about writing this book. I know it must have been some extra work to deal with a first-time fiction writer, and I really appreciate it. And, in a double-billing, I'd like to again thank Chris for introducing me to Syngress, even though I thanked him from when we worked at Titan together.

I want to thank Lori, for her support and help whenever possible, and for acting as ambassador on my behalf to my friends at all those gatherings I couldn't get to because I was busy writing. I know it's been hard, with my being so busy, and I could not have done it without you helping me keep a grip.

Finally, I want to thank the *real* Mr. Donegal, the man who got the Apple computers and taught me how to code back in 1980. Mr. McAniff, yours was the first spade in the dirt, at the groundbreaking ceremony of a fulfilling and successful career. I cannot count the good that has come from what I learned from you; all good things in my life are in some way tied to that. *Thank you!*

—Rob Shein

Contents

Foreword

The opening sequence of the film Armageddon is visually stunning. One day, quite unexpectedly, a meteorite storm bursts from out of the clear blue sky to blast into the city of New York, destroying many of the landmarks and leaving the people frightened, bemused and panicked. Of course, we don't need to turn to fiction to find such an unexpected calamity. The terrible events of the morning of September 11, 2001 left the world shocked, not only for the tragedy that it was, but that it was so unexpected. I debated long and hard with myself and sought advice from friends and colleagues as to whether I should actually bring up this horrible terrorist attack in a book about the exploitation of zero-day vulnerabilities: were the two comparable? I think that the answer is yes. So much of our critical national infrastructure hinges on technology, which is so fragile, that a zero-day bug in the wrong hands could lead to an equally disastrous attack. I'm not, for a moment, going to speculate on what or how that attack may come, but suffice to say that the potential is there; the threat is real.

We can, however, look at recent history to find answers. Consider the Slammer worm. Slammer was unleashed on the world in late January 2003 and exploited a vulnerability in Microsoft's SQL Server. While this bug was not a zero-day, as the patch for this vulnerability had been available from the Microsoft website for six months, Slammer wreaked massive havoc across the globe. The worm was benign, as far as worms go, and simply replicated itself, but this "benign" worm still caused infrastructures to fail, even taking out the emergency telephone systems in certain parts of the United States. It demonstrated the weaknesses of our digital infrastructures and highlighted how a failure in one component could cause cascading failures through other systems due to interdependencies. How much more severe would this worm have been if it was a zero-day? The same could be asked about worms such as Nimda, Blaster, and Code-Red. A worm that exploits a zero-day bug as its attack vector will be

devastating. The reason for this is quite simple: there'll be no defense against it. The best that one could do to attempt to mitigate the risk would be to filter Internet traffic with a firewall. The good news is that the powers that be understand the risk that is posed by such a cyber-attack and are taking steps ensure that, should such a day come, they'll be prepared. There's still a lot of work to do, though, and everybody, software vendors, CNI, businesses, and home users, have a role to play.

The vendors of software are now leading the way. Microsoft, for example, as I write this, is soon to release Service Pack 2 for Windows XP. Service Pack 2 contains a great number of security fixes, but more importantly, a great number of security enhancements. The Internet Connection Firewall (ICF+) is now going to be turned on by default. This alone will help to dramatically mitigate the risk of worms. Further to this, Microsoft has modified the operating system, making it more resilient to exploitation; while there may be a few buffer overflow vulnerabilities that remain, due to these changes, chances are that they won't be exploitable. Microsoft has also spent a great deal of time performing an in-depth code review to ensure that they've found and fixed as many security bugs as possible. The best way to summarize all of this is as follows: of the still undiscovered bugs that were in Windows XP when it first came out, maybe five percent will remain. Of these, only five percent will be exploitable. And these will hopefully be stopped by ICF+. Defense in depth. As far as security is concerned, things will look much better when XP Service Pack 2 is released and everyone installs it. Note the caveat there—to be effective, it has to be installed, and the more the merrier!

Security researchers have a large role to play here, too. When they discover new security vulnerabilities, in any product, they need to work with the vendor to ensure a timely patch can be delivered to consumers of the product. While this is the norm, there are wildly varying views on how information about new security bugs should be disseminated. On one extreme, there are those that believe in full disclosure and may even publish an exploit, otherwise known as *proof of concept code* to demonstrate the problem (one interesting point to note here is that many of the Internet's infamous worms' authors have used a researcher's "proof of concept" code as their template. I myself have fallen victim to this: the Slammer worm was based on code that I once presented at the Blackhat Security Briefings conference. Due to this I no longer publish proof of concept code). On the other extreme are those that don't disclose at all. Both methods of "disclosure" have

their problems. The former provides a roadmap to those that would seek to exploit vulnerabilities. The latter does nobody any good, as lessons can't be learned, and further, if the public at large don't know about a problem, then it can't be fixed. Somewhere in the middle of these two extremes is probably best.

One of the major problems with disclosure is this: when a new bug is announced with a vendor security alert, everyone, both those who need to patch and those that want to exploit, hears about it at the same time. Patches need to be fully tested, which can take a considerable amount of time, before they are deployed on production systems; this presents a window of opportunity for the attackers. In this window, an exploit is invariably published and systems are compromised. In an attempt to help mitigate this problem, NGSSoftware, the company I work for, now works closely with the U.K. and U.S. governments. We provide them with information about the bugs we find and how to mitigate the risk in the *absence* of a patch at the same time that we tell the vendor of the problem. This information is then disseminated by the government to those that are responsible for the security of Critical National Infrastructure systems so steps can be take to protect these systems before the public at large is informed. This removes the window of opportunity as far as CNI systems are concerned. I would encourage other security researchers or organizations to adopt a similar practice.

But, back to the problem of zero-day vulnerabilities, which is what we are concerned with in this book. Every new bug, when discovered, goes through zero-day status, but the discoverer is the one that determines its future. Some bugs are discovered by "whitehat" security researchers who seek to have the bugs fixed. Others are found by "blackhats" and are used to break into systems. As the bugs are new, and so therefore is the exploit, the compromise will often go unnoticed. It's a difficult task of trying to ascertain if Internet traffic contains a new exploit for a freshly discovered hole. Intrusion Detection and Intrusion Prevention systems still can't effectively catch a zero-day. One of the more publicized cases that involved a zero-day exploit concerned the compromise of some U.S. military web servers. The attack involved exploiting a buffer overflow vulnerability in a core Windows component; the attack vector was by making a specially crafted request to an Internet Information Server web service. The important point here is that it was a previously unknown vulnerability that allowed the compromise. No one noticed that the servers had been compromised at first. It was only when the network administrator noticed some

"unusual" traffic originating from the web server that they investigated. Had the attacker been quieter in their activities after compromising the system, and not left their tag, "Welcome to the Unicorn beachhead", in a text file, then the whole affair may have gone completely unnoticed. Many rumours abounded as to who it was. Some conjectured that it must have been a foreign intelligence agency, due to the obscurity of the vulnerability; to have found the bug would have required a significant amount of investment. While it may have been a foreign intelligence agency, the reasoning is flawed. Writing a simple program that made multiple requests to the web server, with the request getting progressively longer, and then running it against a Windows web server, would have uncovered the problem. Indeed, this is the kind of thing security researchers do all of the time. It just so happens that it was a "blackhat" that stumbled across it first.

The point is taken, however, that it could have been a foreign intelligence agency with nefarious intent. This does pose a real hazard. Terrorist organizations also pose a threat. It would be wrong to underestimate such groups, and I, for one, have made the assumption that they do have the capability and knowledge to leverage zero-day vulnerabilities. Let's face it: if a fifteen-year-old kid can do it by teaching him or herself how to hack from texts they've found on the Internet, then we must assume that anyone can. A few well-placed digital bombs could bring down our critical infrastructure like a house of cards. We need to be ready for when it happens and watching for it, blue sky or not.

— David Litchfield

Chapter 1

Prologue

Southeastern New England: Thursday, 3:45 PM, 1980

"That's wicked cool."

Reuben and his friends looked at the design on the screen, astounded at the result of their hard work. A dragon, complete with chunkily-animated fire spouting from his mouth, filled the small video screen of the computer. They sat for a minute in front of the Apple II+ computer, just watching the fruits of their labor.

They had spent hours working on the code that described the dragon in terms of coordinates on the screen, and then almost as long just to work on the code to overwrite sections of the design to produce the animation. In 1980, this was the cutting edge; low-resolution 16-color animation on a 10" RGB screen, produced on a computer with a whopping 48K of RAM. More importantly, it was the coolest thing they'd ever done.

For seasoned programmers as well as total beginners like these, programming is a journey. Every bug is a surprising disappointment, and every bug fixed is its own victory. But, nothing matches the sense of disbelief, then joy, then relief that comes from having it done and completely functioning at the end. There is something of a masochist in every programmer for renewing the cycle with every new program.

"Good job, guys!" Mr. Donegal peered over their three sets of shoulders to view the screen against the glare of the florescent lighting. As the "media director" for the middle school, he was in charge of the transparency projectors, the movie projectors, and other such equipment. A hobbyist with enough vision to see that computers had a critical place in everyone's future, he also had the courage to push for funding to buy the computers on which a dozen students were now learning to program. "So now what?"

The three kids looked at each other. Reuben spoke up. "I dunno. It's kinda hard to think of things to do with it. I mean, there's a lot that you can do, it's just…I guess it's just that we don't know what you *can* do with it, yet, or how."

Mr. Donegal laughed. "I think that's the exact same thing that a lot of engineers are thinking right now. Computers aren't new, but the possibilities that we have are growing quickly, especially with them being so much smaller now. Some are saying that computers will be everywhere, in cars and on every desk. How'd you like one of these in your home?"

"Oh, that'd be AWESOME!"

"Okay then…but what would you do with it? Think of it that way."

A voice jumped up from a student at one of the other computers. "Mr. Donegal! We've got a problem…what does this error mean? We don't know what's wrong."

As their teacher moved off to help the others, the three just watched the motion on the screen. This was something new, Reuben sensed. Right now, and at the level at which he was programming, computers were fair. They had rules, rules that didn't change, and you knew what the rules were up front. If you didn't follow the rules, your program did not work, but that was okay, because it was your fault for breaking the rules. If you did follow the rules, though…you could create something out of nothing, and every time you'd be rewarded. If only life was this simple everywhere else…

Siberia, U.S.S.R.: June, 1982

The computer chip within the gas turbine had undergone a long journey before arriving at the point for which it was originally designed. The torturous path that took it to this place and time was about to come to fruition, with catastrophic results. Sitting on a remote section of the Trans-Siberia gas pipeline, the turbine was being powered up for use for the first time, having passed all the testing runs thus far. It would play a significant role in the Soviet Union's plans to bring natural gas from the remote expanse of Siberia to the center of the Union, although not the role that its builders had in mind.

In the late 1960s, the acceleration in the development of technology, particularly computer technology, in the United States was envied by the Soviet Union. For the U.S., the fear of falling behind in the space race led to an emphasis on science in schools, and the following decades saw research efforts increase dramatically, with a subsequent harvest of innovation and invention. In the U.S.S.R., however, this did not take place along the same lines. Lacking the industrial mindshare to match the U.S. in innovation and research, the Soviets instead chose to purchase and copy the technology, allowing them to maintain near parity without the exorbitant costs of development. In response to this, President Nixon had placed export controls on many technologies (including computer technology) that prohibited exporting such goods to Warsaw Pact nations. As a result of Nixon's actions, the U.S.S.R. implemented an operation in the KGB to purchase and import such goods clandestinely. Upon discovery of this fact,

via a well-placed agent within Moscow Center, the U.S. came up with a clever countermeasure; they sold the Soviets exactly what they were looking for, but not what they wanted.

Various designs and components with military and industrial applications were sold to the KGB fronts with clever mistakes in them. In many cases, this caused scientists to waste endless manpower as they failed to achieve the desired results using the misappropriated technology. In this case, the computer chip itself was the trap.

This chip was designed to appear entirely healthy, but had a deliberate fatal flaw. As the pump it controlled on the pipeline spooled into action, this flaw imposed its will violently. A special algorithm in the firmware on this chip (that the legitimate version lacked) was triggered, and the chip went rather insane. Consequently, the controller directed the turbine to run at a much higher rate of flow than was safe, while the safeguards in the firmware ceased to function. Valves were opened and closed, the result being a pressure wave many times that of the safe limit allowed by the pipeline's walls.

On the other side of the planet, deep inside Cheyenne Mountain, the headquarters of NORAD felt its pulse quicken as satellites detected a sudden, brilliant flash of thermal energy deep inside the Soviet Union. A blast equivalent to 3 kilotons of TNT had just erupted, and all eyes widened with fear that a nuclear discharge was to blame. These were the days of enmity between the two nuclear superpowers, and there was nothing even remotely calming about the prospect of a nuclear blast on any soil , as open-air nuclear testing had ceased between the two countries years earlier. With no indications of any electromagnetic phenomena which would result from such a blast, and after very careful consideration and examination of the satellite intel, it was left as a mystery.

What had occurred was that the pipeline had severed abruptly, leading to the largest non-nuclear explosion ever witnessed by mankind. The CIA had, through their own front organizations, sold faulty turbines to the U.S.S.R. with this end in mind. The only thing that saved face publicly for the Soviets was that the explosion was in a remote area, and had no direct witnesses. It would be a year before they traced the path the small computer chip

followed, figured out exactly what happened and executed the original mole in the KGB who leaked the information to the French.

Tagig, The Philippines: Tuesday, 2:34 PM, 2000

"What's the point," asked Agpalo, "since we know we're not going to get jobs anyways?"

The teacher stopped and was silent, not sure how to respond to this question. For a moment there was no sound but the whirring of the fans inside the computers, the hum of the overhead lights and the sound of some random insect buzzing inside the classroom. He had heard the same question dozens of times and overheard it even more, but still had no answer. He knew all too well that he was lucky to have this job, and didn't want to lose it by admitting the truth: that the good jobs went to those from wealthy families and "good" backgrounds, and that for these students, studying computer science was like studying space flight, for all the chance they'd have to apply it in the workplace. None of the students in this room came from the right neighborhoods, and they never would. They didn't have connections, their fathers didn't have important positions, and they didn't get to go to private schools. And it never ended, regardless of how talented they might be. But why talk about it? What was the need to admit it, since everyone knew anyway? What would it change? Everyone here knew that they were stuck with no options of real upward mobility, and talking about it didn't help.

Next to Agpalo, his friend Lualhati shrank in his plastic chair, not wanting to draw attention to himself. This was the last thing he needed, to attract the instructor's ire on top of all the taunts and insults from other students and people in his neighborhood.

"In many other countries, a large supply of programmers helped make it possible for a big growth in IT industries. In India, they make billions from overseas programming and other IT staffing. This will happen here too," he lied. "Just think of how nice that will be…to be ready when it happens!"

Agpalo looked at Lualhati and rolled his eyes. There was no point in even discussing it; there never was. They both knew that even after graduation, there wouldn't be any jobs for them, at least not here.

After class, the two walked away from the technical college, through the busy streets back to their neighborhood. As blocks passed, the businessmen and shops gave way to residential buildings, and these grew smaller and less dignified as the distance continued still. The surroundings here never really changed; they'd always been like this, and probably always would be. This far out, the squalor permeated everything, from the smell in the air of small cooking fires and rubbish to the grungy look that nothing escaped. All of it…walls, roads and even people…seemed to lack the smoothness and consistency that better neighborhoods and cities shared. The only thing that seemed consistent was the hopelessness, the fact that nobody from here had much of a chance of ever leaving or going anywhere better.

For Lualhati, this was particularly cruel. Years earlier, his mother and he had moved here from Mindanao in the South Philippines, looking for better opportunity; the move took all the resources they could muster. It made no difference; in many ways it made things worse. At least down south, they weren't subject to distrust and ridicule for being Muslim, but here everyone looked at them differently. And in the past year, it had only gotten dramatically worse. The police had been cracking down, trying everywhere to find and eradicate members of the MNLF, and everyone looked at him like he was a potential suicide bomber. Why didn't they understand that half the reason why the people of Mindanao wanted to have their own country was because of this kind of treatment?

They were hardworking people who just wanted to be left alone so they could pursue a better life. His mother worked hard to provide for the two of them, and managed to scrape together enough money to cover the tuition of trade school so Lualhati could learn. He didn't think she really understood, though, that there wasn't going to be a miracle. Learning to be a programmer wasn't going to be a ticket to a better life after all. He didn't have the heart to argue the point with her, so he just kept trying.

It wasn't fair; Lualhati had never done anything to hurt anyone. He was a Muslim…so what? He wasn't a terrorist, and he didn't want to be one.

He just wanted to be left alone, not teased and jeered at by other kids. Things were no better here than they were down south; in some ways, they were much worse. Sure, there were better chances here, but not for the son of a Muslim family, not for the kid that everyone teased growing up. He no longer thought of better things.

Chapter 2

DefCon in Las Vegas, 2000

Las Vegas, Nevada: Friday, July 28th, 12:34 PM, 2000

The brutal desert heat wasn't too easy to bear in standard DefCon clothing. Black was the order of the day, and despite the low humidity, Reuben was looking forward to getting inside, back into the air conditioning. He looked around the pool area and wondered if anyone else was feeling the same way; if they were, it didn't show. Most perplexing of all were a couple of the members of Phenoelit, the German hacker think-tank, who were wearing not just black, but black leather pants. Reuben could feel the sweat under his backpack, and wondered what it must feel like under those pants. Phenoelit was well-known for their understanding of (and ability to poke holes in) various networking protocols, especially those used for communication between devices like routers. FX, one of their members, was a talented researcher and speaker with regard to router vulnerabilities, and had the ear of Cisco when it came to fixing problems.

Most people seemed to think that the main source of security research in the IT world was the government, or large corporations. In reality, it was small, non-commercial groups like Phenoelit, L0pht, Attrition, and a select few independent researchers, like Rain Forest Puppy, Dan Kaminsky, Greg Hoglund and David Litchfield, among others, each with their own particular specialties and focus. The research was rarely done under contract, but was rather the result of a natural curiosity just to see if something was really secure or not…and if not, how to break it. The benefits of this research varied from many factors, but without it, the only people finding new vulnerabilities would be the criminal hackers, who produced "0-day exploits."

When a vulnerability was discovered, the normal plan of action was to develop a program that could "exploit" it. The reason for this was simple; software companies tended to vehemently deny that their software was vulnerable. This could be attributed to the desire to avoid bad publicity, their personal attachment to their work, or ego, it didn't matter. What mattered was that you often had to demonstrate the vulnerability to convince them that it existed, and get them to fix it. When security researchers did this, they normally contacted the software producer first, keeping the knowledge under wraps. They then had the option to reply in kind, get more details, and fix the problem; once the fix was available, the researcher would release details of the vulnerability (and how to get the fix) to the world, and claim credit for the discovery. The threat of vulnerability (and exploit) disclosure tended to keep the software companies honest; if they refused to acknowledge or address the problem, they risked being seen as unconcerned about the security of their product, and thus the security of their customers. Indeed, on rare occasions, the company would be unresponsive, and the exploit code would be given to the public to attack their systems at will, which would force the issue. Sometimes the researchers were called "hackers," sometimes they were called "security researchers," and there was no rhyme or reason to it, really. Even the meanings weren't necessarily stable. To many people, a "hacker" is someone who breaks the law and does bad things. But to most in the field of computer security, a "hacker" was just someone with some solid skills, and perhaps not even

security-related skills at that. It just meant someone who was one hell of a programmer.

Sometimes, however, the first person or group to discover a vulnerability were those with no such moral goals or distinctions. To a black-hat, a vulnerability that nobody else has found is valuable; the attack to exploit it is a sword against which there is no armor, essentially. The vulnerability that had been known to the general public for zero days so far, and thus was known as a "0-day vulnerability," and the exploit ("0-day exploit," naturally), would be kept secret from the public and the vendor; if the vendor came to know of the flaw, they would likely fix it, and the attack would lose much of its effectiveness. In addition, IDS vendors would add signatures to detect it, and people would know to watch for the attack in general. Such exploits were sometimes traded among very close friends, and eventually leaked, but usually they became known after a seasoned admin with a watchful eye noticed the attack, and was able to conclusively see that it was a new attack that exploited an unknown vulnerability. At that point, the researchers went to work and recreated the vulnerability, and the vendor was notified. Sometimes, the first hint of such an attack was a large amount of scanning (searching on the Internet with automated tools) for a particular application for no apparent reason; the person in control of the 0-day exploit would be looking for targets en masse.

And DefCon was *the* annual conference for hackers and the like. Thousands of people of many ages and backgrounds churned through the conference: script kiddies who knew little besides how to cause havoc and destruction (both digitally and interpersonally), old-school hackers who still knew more than most other attendees, feds of one kind or another (in varying degrees of disguise), academics, and probably quite a few professional criminals. They all readily mingled with each other, fully aware that anyone they spoke to at any time could belong to one or more of these groups. On top of that, everyone drank, almost perpetually, all weekend long; this seemed not to hinder intellectual discourse at all, oddly enough. In fact, it actually seemed to foster it, as fears of who one talked to and what one said diminished.

The resort hosting DefCon was the first to ever allow them back a second time. It was no surprise that a conference of this sort inevitably

included people who lacked a moral compass. Past events included hacking the radio communications of casino guards. That prank was at least amusing, as it involved periodically replaying the same "There's a fight on level two!" sound (recorded off the airwaves from the dispatcher), causing dozens of guards to converge in the same spot repeatedly. This went on for over ninety minutes before the guards caught on. Other pranks descended into raw stupidity, such as tossing a smoke bomb into an elevator. It seemed that script kiddies were not entirely aware of the degree to which video surveillance permeated a Las Vegas casino hotel.

Attempting to bring at least some degree of order to the situation was the intimidatingly large, viciously sarcastic and incredibly humorous man known only as "Priest," who acted largely as referee and MC for the event. A former NSA employee, he embodied the duality of the security industry, helping organize and run an event that brought both sides of an online war face to face in the spirit of mutual learning.

One of the lighter sides of DefCon was the "Spot the Fed" competition, which had its origins in a less-than-fun act of community self-preservation. In the early days of DefCon, federal agents (usually from the FBI) would attempt infiltration of the event and attendees, in hopes of gathering intelligence. Their hope was to collect information that would lead them to catch hackers, although they never had any particular crime in mind when they attended. The problem was, it's fantastically difficult for a person with an FBI mindset (not to mention background and age) to fit in among such a crowd. Thus, their presence did not go unnoticed for long, and the attendees amused themselves by pointing them out publicly. This eventually evolved into a game; "spot the fed," as it came to be known, which had every hacker looking at any fellow attendees that appeared "feddish." If an attendee spotted one successfully, they got a black (of course!) t-shirt that said, "I spotted the fed!" on it. In later years, as DefCon grew, the surveillance and the contest both became more light-hearted; the fed got a t-shirt also, proudly proclaiming, "I am the fed!" By then it was a fun and jovial game, and the feds and hackers alike delighted in it. It was also a nice break from often contentious and always mentally taxing debate and discussion of incredibly technical concepts…the simple joy of

everyone uniting in agreement as they looked at the short-haired blond thirty-something man on stage and chanted, "FED! FED! FED!" in unison.

Curiously looking about to see if he could spot anyone looking "fed-dish" in plain sight before giving up for the moment, Reuben looked down at his program and tried to figure out which sessions he wanted to see. The topics were all over the place, including IDS evasion, network-level steganography, and some hardware hacking. He noticed an interesting session on penetrating secured systems that have been certified "B1." This certification essentially meant that the systems in question were about as secure as can be realistically expected, even under the worst of conditions. *Well, won't be attending that one. Too many bad guys will be interested,* he thought. That's part of the problem at DefCon, you can learn much from what your opponents will tell you, but you can also end up being improperly identified with them too. The trick was to avoid unnecessary risks and focus on the benefits, and learning how to break into DoD classified systems had no benefit to a commercial-world whitehat like him whatsoever. Neither did the session on writing buffer overflows for the SPARC architecture…he didn't write exploits, and few of his clients used Sun hardware yet in any case. Likewise, some of the less technical sessions, like the one covering the sociology and psychology of virus writers, appealed to him, but had little value to his client base. He had to remember that he was there to learn, but more importantly to learn what would serve him in his work. Still, there were some overlaps, and some sections of time where one thing seemed as good as any other, job-wise.

Looking down at his badge, he noticed that this year it was plastic and colorful, unlike the previous year. A large red pill was featured, with the label, "DefCon 8," a clever metaphor. It was widely felt that DefCon was the conference where one "took the red pill." He looked around the pool area again, and it struck him how the sight was bizarre on some level, and yet comforting. Everyone around was, on some level, like him. Nobody here would look askance at him for being a "geek" (although the word was by now becoming a compliment rather than an insult, thanks to the dot-com boom), or try to talk sports with him. Conversely, nobody looked at him like some mystical member of a new priest-class, able to speak to the computer gods on behalf of mere mortals either; Reuben felt particularly

uncomfortable when people did that. Here, he could strike up a conversation with someone about extremely technical concepts and actually *feel challenged* by the resulting conversation. Back at home, in Washington DC, he worked with some very talented engineers, but none of them were security geeks, in the pure sense of the word. He could learn a lot from them about networking and various server apps, but when it came to security, Reuben was increasingly feeling like the big fish in a small pond. He was "that guy," who knew the wizardry of such things, in office lore. He wanted to get into larger jobs, into work that challenged him more. He wanted to do some of the really high-stakes work for the larger companies.

Reuben walked inside and went to the vendors' area. A peculiar hackers' bazaar filled the large room, with people vending everything from old hardware to t-shirts with funny or artistic designs. "Got root?" questioned one shirt, a slogan also available on stickers of various sizes. Another shirt sported a diagram of the OSI Model…but with two extra layers on top. Instead of the normal 7 layers, ranging from "physical" to "application," there were perched the "money" and "politics" layers, a witty reference to how the best-laid plans of geeks were often utterly trashed by non-technical realities. Another shirt was a cross between a type of vulnerability and a quote from a recent popular movie…"I am Jack's overwritten stack pointer…" He pulled out his wallet, and bought a few shirts as well as a couple of witty stickers. Someone else was offering copies of a database of what looked like DMV information, and another vendor produced false identification. *God, they're just asking to get raided, being out here like that,* thought Reuben as he smirked to himself and moved on. Just because the feds who attended DefCon were good-natured didn't mean they were blind, stupid, or derelict in their duties.

New this year was the open-access wireless network. Reuben didn't have a wireless card yet, so he wasn't participating. He wasn't sure he wanted to just yet either. An open network at DefCon would have to be the most hostile network on the planet, with such a concentration of hackers of every level of moral character populating it. He didn't have to wait long to see an example of what he feared.

"That's odd. I've only been up and running a few minutes, but I have core files all over the place," stated one attendee with a wireless card. Core

files were dumps of sections of running memory, produced when an application failed unexpectedly. While many things could cause such an event, it was too much of a coincidence here that the core files all seemed to be from listening daemons on the operating system; the laptop had been hit with a slew of buffer overflow attacks, which invariably caused the targeted application to crash as it was subverted to a hacker's purpose. Apparently the puzzled owner of this laptop had just finished installing and configuring RedHat Linux 6.2, and had joined the network without installing any patches or using a firewall. Inside of two or three minutes, he'd been hacked multiple times, and his laptop was now like a piece of meat that a dozen dogs were fighting over. Reuben just shook his head and kept walking, laughing to himself quietly and metaphorically imagining the computer as an inept beekeeper who decided to provoke several hives worth of hornets simultaneously. The computer had been taken over, or "rooted," not once but several times, or perhaps even dozens. The expression derived from gaining access to the "root" account of a UNIX-based system. Root had the power to do anything, and thus being able to use that account gave a hacker unstoppable access to everything else on a machine.

Reuben strolled into the room where "Capture The Flag" was starting. The CTF competition was really amazing; several teams set up systems on a network, and the teams then tried to hack each other while fending off attacks. Points were awarded for successful hacks, and at the end, the team with the most points won. One organization dutifully recorded every packet that passed on the network, and made the data (by that time one *huge* file) available to the general public for whatever purpose. It was well-known that many of the newest and most clever attack techniques were contained in that data, and IDS vendors took good advantage of the intelligence provided therein. Mostly, Reuben was just impressed with the notion of such talent set up in a gladiatorial setting, digitally speaking.

He noticed that an IDS vendor was actually participating in CTF this year, in an odd sort of way. Network Security Wizards was here, with their Dragon IDS. The CTF had to be a nightmare to monitor like that, with every imaginable attack underway. An IDS, or Intrusion Detection System, was a security system for a network, kind of like a burglar alarm. It listened

in on network traffic, quietly observing like a chaperone at a high school dance, watching for any sign of bad activity. The problem was defining "bad activity," since good activity could look like almost anything. While hackers typically used traffic that defied normal definitions of what should be seen on a network, misconfigured systems, poorly written software, or even heavy network traffic could do the same. On top of that, there were emerging methodologies that hackers used to evade detection, and IDS vendors were still struggling to address these methods; it was common knowledge that there had not yet been an IDS that could not be evaded by some method or another.

Reuben walked up to the console of the Dragon IDS and looked at its management console. He'd never seen this one before, but he was still learning about IDS, so that wasn't anything particularly surprising. Apparently it was running a pretty heavy set of rules, plus some extra custom ones that Reuben didn't even recognize. The number of alerts on the network was truly insane; the sensor console sitting next to the management station listed each one as they occurred, and with intermittent pauses, the screen rolled at a speed that no human eye could follow as attack after attack unfolded within milliseconds of each other.

"Pretty neat, huh?" The vendor's representative was clearly as proud of the IDS as Reuben was impressed. "It's recording every attack, and we've put some nice custom rules into it, so that if it detects a root compromise of one team by another, it'll RST-snipe the connection and hijack it, and we'll take the root instead. Let me show you how the management interface works…"

Reuben watched as the man demonstrated how to view a single alert on the interface (which was web-based) and "drill down" into it to see more detail. He was able to examine the raw data pulled off the wire, complete with all the intricate detail of each packet like checksum and sequence number.

The interface was remarkably intuitive; inside of twenty seconds, Reuben had taken control of the mouse and was navigating himself. He went back to the list of signatures running on the system, and looked at some of the custom ones. Indeed, he saw that if the IDS detected that one team had rooted another, it would interrupt the connection and take over,

turning one team's hack into theirs. Crafty, indeed, and a bold demonstration that they knew how to build a solid IDS. Of course, the real challenge was for their system to keep running all this time, as many IDS were prone to crashing, or "falling over," when subjected to excessive alerts or traffic.

Reuben thanked the man, and got his card before walking away to sit at an empty table. He just sat for a minute, tossing his backpack onto the table, and rubbed his forehead. His mind was aching from the mental exertion of the past two days. Immediately prior to DefCon came another convention, the Black Hat Briefings, which (despite the irony of the name) was aimed exclusively at security professionals like himself. While the "Briefings," as they were called in this context, were only two days in length, Reuben suspected that he wouldn't have survived a third day. The information was fantastic, the depth of it was challenging beyond any other training or education he'd had, and the learning continued even after the sessions were over. As always in the geek world, when geeks got together they talked shop. *I need to pace myself this weekend. I need to take it easier; I can't absorb it all and I need to just relax about that,* he thought to himself. He always craved learning, particularly when it came to computers. He'd always been able to keep up at any pace he could find, until now. That's part of what he loved about the two conferences, he really felt like he got his fill of data. Perhaps that would change as he learned more, but at least for now these two conferences remained the deepest fountain of knowledge from which he could drink.

And little surprise that was, as they were both organized by the same person; Jeff Moss, also known as "Dark Tangent," organized the first DefCon years earlier, when it had only a select few elite attendees. Over the years it had evolved, and during this time Jeff had noticed a need for something a bit less raw, a more professionally-aimed equivalent. And thus, the Black Hat Briefings were created to fill that need. The differences between them were as interesting as the similarities. While DefCon was being held at a perfectly fine but nonetheless no-frills resort, the Briefings were held at Caesar's Palace. They pumped up the "posh" quotient a bit, with catered breakfast and lunch plus an open-bar reception, and speakers from heads of industry and government. The price, obviously, reflected this as well, as such a production wasn't cheap.

Well, he thought, *if I can't do anything really productive at the moment, I might as well relax and have a beer like everyone else.* Besides, socializing a bit would probably get him into the swing of things. He loved nothing more than the constant string of security-geek conversations with both total strangers and familiar friends that happened at DefCon once he really got into it, and it always started with drinking.

Getting up, he found his way to the bar, which was already well-populated with attendees, and eventually got a Heineken from the overworked bartender. Reuben wished they carried better beer; his past as a home-brewer had spoiled him, and he couldn't stand the taste of most run–of-the-mill domestic brews by now. Heineken wasn't his favorite, but at least it was good. Taking a deep gulp from the bottle and pulling out the program, he decided not to care too much about which sessions he went to. He was already tired and starting to burn out, and figured that if he pushed himself too hard, he'd not only be useless when he got home, he'd be useless for the duration of DefCon as well. There was plenty to keep him interested, and if some of it was more for fun than for practical use, well, that was alright too. After all, he learned most of what he knew that way, and almost all of it ended up being practical in the end at any rate.

He looked at the program guide…he saw that Mojo was speaking again, this time on Windows 2000 security. He'd spoken the year before on Windows 98 security, and it had been pretty interesting. Before that session, Reuben hadn't ever thought about the havoc a hacker could cause by attacking workstations instead of servers, but from that point onward, he paid careful attention to the issue. Windows 2K hadn't been widely deployed by his client base yet, but it was a certainty, and this time he might be a step ahead of things if he knew how to secure them correctly in advance.

Also looking good was the session on IDS evasion. Reuben was interested by the technology in general, and knew that he'd be working with it down the road. His curiosity was all the more piqued for having played with Dragon and walking away so impressed with it. The problem was that so many IDS vendors had products that were hard to compare to each other. It was like apples and oranges, some boasted of one aspect, others of another. And it was starting to come to light that none of the boasts were

about anything particularly substantive, but that the real important factors were pretty subjective. The one thing that was important across the board, however, was how well they avoided evasion, and how many false alerts they were prone to throw. While there was no way to objectively produce a number against which one could be compared to another, that also meant there was value in knowing how to make a judgment call when helping a client determine which one they should implement. And this largely had to do with asking the right questions when sitting across the table from a vendor, which required having the right information with which to challenge them in the first place.

Reuben had no interest in the session on number theory and quantum computing; this was best left to those doing original research. But the session on source routing and spoofing using Linux was of immense interest. The concept of spoofing was rife with mystique and misunderstanding, and while he understood the realities behind the technology, he wanted to learn more about actually doing it, rather than just the academic challenges and awareness of how it needs to be done, in concept. It looked like the session involved setting up a Linux box as a specialized form of router to transform traffic passed through it…in essence making the entire process a lot simpler. The issues posed by securely-configured systems at the target still existed, but at least spoofing became something to be set up once when doing a penetration test, rather than once for each application used.

Reuben was definitely going to pass on the speaker from the ACPO. An anti-child-porn hacker group, the ACPO was the new reincarnation of the ACPM, which sought to hack child porn sites. The problem with this notion was twofold: one, it was in of itself an illegal act and as much of a risk to the hackers as to the child pornographers, and two, it fostered a form of Darwinism whereby the hacked websites came back online days or weeks later but with far better security. Realizing this, the group changed their methods along with their name, and instead chose to gather online information about purveyors and distributors of child porn, passing that data on to law enforcement authorities.

He was also going to pass on the session about building a firewall in Linux using "ipchains," the firewall component of the Linux operating system. While an excellent packet filter, ipchains wasn't "stateful," and

therefore couldn't compete with the stateful inspection systems that Reuben had already become quite accustomed to installing for his clients. He greatly preferred these to standard packet filtering, as they were much better at preventing certain types of probes. At any rate, if he built firewalls nearly from scratch for his clients (instead of relying upon commercial products), he'd have to spend enormous amounts of time keeping them updated, rather than merely applying patches that the firewall vendor researched, created, and supplied. It just didn't make sense for his clients to spend the money for that labor either. He'd heard, however, that a stateful module was in the works for Linux, which was something that Reuben very much wanted to see.

Utterly out of the question was the event that Cult of the Dead Cow was putting on the next day. Certain to be packed with people, the standing-room-only crowd would heat the room like an oven. And for what? cDc, while made up of some of the brighter people in the hacking scene, seemed like a fraternity gone bad. Reuben had always felt that the individuals who comprised it were great on their own, but horribly strange when combined together as a group. He felt a certain reverence for their aims and goals lately, such as combating state-level censorship of Internet links, but still found their behavior a bit unsettling.

Looking through the crowd, he absent-mindedly observed the wide cross-section of people in attendance. People with piercings, goth types, more generic geek stereotypes, and all in a fairly wide range of ages. The one thing that they all had in common was an interest in computer security, from one side or another, or even both. It wasn't hard to notice that most of them didn't seem to get much sunlight either. Reuben relaxed, starting to feel the effect of the beer. He always was a lightweight drinker, and noticed how when he was here, surrounded by this particular crowd, he really felt at home, perhaps more so than anywhere else at any other time.

Behind him, some newbie was trying too hard to prove himself, and failing even more horrendously than he knew. That was often a problem; many came here with something to prove (either to others or to themselves), and this was the surest way to alienate everyone else and have a miserable experience. There was too much talent and far too many brilliant

and unconventional minds for anyone to expect to gain adoration or envy on any significant level. The point of DefCon was not to show off, but rather to learn, and you could not learn while trying to show off. The fact that those with something to prove usually seemed to feel that way because of some inadequacy only made it worse. This year there was a session on general DefCon etiquette, which seemed well overdue. Reuben was inwardly deeply relieved that when he felt out of place, he tended to introvert rather than overcompensate by bragging or doing anything that interfered with his ability to learn. Had it been otherwise, he'd surely have made as big a fool of himself as the guy he was now listening to.

It could have been so different, if only one thing had changed along the way, he thought. If he hadn't learned how to use computers when he was eleven. If he'd not enjoyed them so much…no, more like if he hadn't found them so addictive that he barely lifted his hands from a keyboard until six years later, when he traveled a bit of Europe for a month with family. If he'd not gotten a crash-course in how to interact with other people while in Europe. He got back from that summer trip to his senior year in high school, a different person. No longer as shy, he participated in more than one school play that year, and started dating, albeit still a bit behind the learning curve compared to his classmates. He actually became a geek with some popularity, in that last year, without having to compromise his views, standards, or beliefs. Too bad it was only that last year that went so well. At any rate, when he got to college, he was in good shape for a social renaissance, and he was proud to be a geek with better-than-average interpersonal skills, particularly in groups.

Finishing the beer, he stood up and tossed it into a nearby trash can. He walked back through the lobby to the makeshift cafeteria, and bought a slice of pizza. If there's one thing he knew to do, it was to keep eating; he normally ate constantly, and working mentally at this level made it worse. You'd never know just how many calories he consumed in a day by looking at him, luckily. Now quite active, he was still slight of build if physically fit. Years of cycling and other stereotypically un-geeky activities had given him a good body, though his metabolism ran so fast he had trouble keeping even muscle weight on if he didn't eat enough on a regular basis.

Reuben downed the pizza and looked for the "Haxor" area. DefCon had three basic tracks of speakers: Newbie, Haxor, and Uber Haxor, in increasing order from least technically challenging to most. The trick every year was remembering which room was which, as for some mystical reason nobody could ever remember even after the second or third day. It helped that this was the same place DefCon was held the year before, however, and he found the room and took a seat at the beginning of a session that intrigued him.

The speaker was identified only as, "Noise," the female (and rather fetching, to the notice of the overwhelmingly male audience) admin of a kind of anonymous mail system that Reuben had never heard of before called "mixmaster." It was a poorly-known fact that anonymous remailers served a terribly useful purpose on the Internet, allowing people in countries less free than the United States to speak freely, among other reasons. Other reasons were plentiful too, if less life-threatening. The problem was that any such remailer had to be set up in such a way that even the people who ran it couldn't divulge the identity of the users, which was quite a technical hurdle. Everyone in the hacker world knew what happened to the old and widely-used anonymous remailer, anon.penet.fi. While the admin refused to turn over logs, he realized that he eventually would be forced via legal means to do so, and thus he shut down the remailer rather than risk compromising the users. Mixmaster apparently used a multi-server approach, such that no single server knew with any credibility who the user really was…or if they were even the start, middle, or end point of the route for any piece of e-mail. The challenges were even more complicated than Reuben had imagined, and so were the solutions. What if someone wanted to snoop on the traffic, and under false pretenses joined the mixmaster network? What if an admin accidentally logged the connections, and those logs got subpoenaed? What if a hacker broke into the network and listened to traffic going by? The mixmaster system was designed to address all of these, no matter how paranoid the scenario. Reuben was sure there were things that weren't quite covered, but damned if he could figure them out. It made his head…not quite hurt, but definitely feel as though there was too much physically inside it at the moment. It felt good. He knew he was pushing himself again, and he loved how it felt

almost as much as he loved that he was learning something entirely new again.

After the speaker finished, the next session was on legal issues of hacking, by Jennifer Grannick, a prominent attorney in the field. Having defended more than one person accused of hacking (including Kevin Poulsen, who was particularly clever…save for the polaroid he took of himself breaking into a telephone switching exchange), she was an expert on the cutting edge of cyber-crime law. The presentation was more humorous, and far less technical, giving Reuben's overworked mind a bit of a break. In college, he'd taken some business law along with criminal justice classes, and enjoyed both topics immensely. It seemed to be the case that while criminal statutes had evolved to clarify the definition of hacking as a crime, cases were still being prosecuted to a ridiculous degree and in some overzealous ways. That was perhaps to be expected, as the public view of hacking was still loaded with emotion, uncertainty and fear. There weren't a lot of surprises in what he learned in the presentation, but it was still quite interesting, and gave a lot of insight into how things might go if he ever needed to help with a prosecution on behalf of a client who had been hacked. In the end, though, Reuben was left with some interesting insight into the perspective of a hacker who had been caught, prosecuted, and had become a good guy. Poulsen seemed like a nice guy, really…it was painfully obvious in his case how boredom was a major factor in many of the older hacking cases. People with exceptional computer skills but who were too young to get jobs to use them found whatever challenges they could to occupy their minds, and that led to hacking into computers, albeit with no intent of actually causing harm.

Looking at the schedule, Reuben decided to stay put for the next session as well, which covered privacy protection. He remembered this speaker; the year before, he'd spoken on a novel form of crime known as identity theft, and it was relatively chilling. The ease with which a criminal could research, select, and impersonate another person was shocking, and the financial reward for such criminal activity was not slight either. This year, however, seemed to be less bracing in content, mostly focusing on how to keep from using certain forms of identifiers (like social security numbers) in many places. The idea was that if there wasn't a single

common thing (besides your name) in every transaction you completed, it was harder for someone to compile a database of everything you do. There was also some coverage of such databases, like the FINCEN (the Financial Crimes Enforcement Network) used by the Treasury Department to detect and track certain forms of criminal activity. The typical DefCon attendee was a little (or more than that, perhaps) paranoid, particularly when it came to activities of governments to track citizens and their actions, and thus these activities were commonly covered during the conference. For weeks after the first time he attended DefCon, Reuben felt exceptionally paranoid himself, after learning just how much tracking went on, unbeknownst to him previously.

When the presentation ended, Reuben got up to go to the Uber Haxor room, to catch the session on IDS evasion. There was much along the lines of the famous paper by Ptacek and Newsham, plus a few extra little twists, but ultimately it wasn't anything that Reuben didn't already know about, oddly enough. Sometimes part of attending a session was to learn how much you already knew rather than fill in the gaps you had.

Afterwards, he decided that it would be better to call it a night (early as it was) and go back to his hotel. Rather than stay where DefCon was held, Reuben preferred to book a hotel room elsewhere. There were just too many noisy people around, and he felt safer being away from the crowd of hackers at any rate, although he really didn't know that there was much real risk in staying with the conference. It just felt nice to have the option to get away from it if he felt the need, and tonight he felt the need. On top of the mental fatigue, he was still fighting jet lag, and wanted to have a more comfortable evening.

Outside, the brutal desert heat of Vegas assaulted him again. Getting into one of the plentiful Las Vegas taxis, he lay back in the backseat during the quiet but visually-stimulating ride back to the Luxor hotel, where he was staying. For some reason he always found the lights and activity of Las Vegas to be curiously soothing. Strangely enough, it was kind of calm and even a bit boring compared to the psychological and mental spectacle that was DefCon. Arriving at the hotel, he tipped the driver well and got out, walking through the lobby without a care for the odd looks he got, dressed as he was in black BDU pants with combat boots and a black t-

shirt, with a large futuristic-looking laptop case on his back and a DefCon badge hanging from his neck. Added to his trimmed goatee and ponytail (the veritable badge of a computer security researcher), he looked quite different from the middle-American fanny-packers, standard yuppies and occasional high-wealth high rollers. They clearly didn't know what to make of him, and that seemed to scare them a bit. *Serves them right,* he thought. *Avoiding the things you don't know out of fear just makes you weaker, and probably a bit stupid as well.* He kind of liked the way they feared him…he liked feeling a little bit dangerous, even if he knew that there was no way he was going to do anything to hurt any of them.

In his room, he tossed the backpack onto his bed and quickly tromped into the bathroom to start the shower before getting undressed. He felt filthy from all the sweat that had dried on his skin, and wanted to clean up before going out for dinner. He loved the way he could shift gears from rebellious hacker to well-dressed yuppie, and was looking forward to going out in better clothing than he'd been wearing that day.

Friday, July 28th, 9:22 PM, 2000

"So, why are you in Vegas if you don't gamble?"

Reuben had forgotten why most people came to Las Vegas, until the stranger (who called himself "Jack") sitting next to him at the bar asked this. "Well, there's this conference in town…two of them, actually. The first one is the 'Black Hat Briefings,' which are basically for computer security professionals, the good guys. The second one is a bit less cut-and-dried, and it's going on right now. It's called DefCon, and it's attended by people on both sides of the equation. That's why I'm here."

Jack looked at Reuben warily now, but was clearly more drawn than repelled by the possibility that Reuben was a hacker of the bad type. "Who's side are you on?"

Reuben laughed a bit. "Don't worry, I'm a good guy. I get asked that a lot though; the bad guys and good guys look a lot alike." He always found it so funny how back at home, he was the only guy with long hair and a goatee that he knew…but at the Briefings and DefCon, he was practically a

conformist. In any event, he was not unaccustomed to being treated like a scumbag by the Washington D.C. police, whose professionalism left something to be desired, in the same way that a total vacuum leaves something to be desired when breathing.

Jack relaxed, now apparently feeling unfettered to be intrigued without fear. "So you're like a hacker, but a good one? That's got to be so cool! What do you do, break into networks to see how safe they are? That sort of thing?"

"Yeah, that's a part of it, but in truth there's a much wider range of things that I do. How much do you know about computers and networking?"

"Not much. I can do e-mail and the web, but I don't use the computer more than that. You should ask my kid if you want to meet the real techie in my family. At home I have AOL. Hey, do you know how to stop spam?"

Reuben inwardly cringed at the request for one of several holy grails of the industry. "Ah, spam. Everyone's trying to find the solution, trust me, but nobody really has it yet. There are a few things that work OK, but the problem is that the better solutions require geeks to maintain them. The spammers keep changing the verbiage they use, so the means of identifying spam keeps changing also. Hell, even the geek community has a hard time coming up with an exact definition for 'spam'. Think of it like this…you use AOL, and they have partnerships with other companies. Let's say AOL decides to make your e-mail address available to them, but first they ask all their subscribers for permission. Only, what they do to go about it is tell everyone that the privacy policy has changed, and that if they want they can change their settings in this new web page that controls whether they can share your e-mail address with others. If you go to this web page, you see that the default answer for every question is 'yes'. But if you don't go looking for and check those settings, and start getting e-mails from all these legitimate companies that want to sell you things, is that spam? You weren't expecting it, but in a legally-binding sense of the word, you gave permission for them to send it to you, basically. It bothers you just as much as the totally unsolicited e-mails pushing penis enlargement… whatever… but in legal terms it's a completely different animal. Is it spam or not?"

Jack thought about that for a minute, clearly not expecting there to be a shade of gray in the world of technology. "I never thought about that, in fact I think I'm a bit confused now. I'd still call it spam, though."

"Okay, but then what do you do when you consider that spam, but someone else actually wanted to get them, or at least some of them, because they did go to that web page and decided that they were interested in the 'special offers' in question? How do you write a program that knows what the user wants, when two people get the exact same e-mail but one welcomes it while the other hates it?"

Jack didn't like this answer. Nobody liked finding out that technology wasn't a magic wand that could make all their problems go away. Reuben never got over how many people who thought that geeks were some kind of hit men who could whack the difficulties of life for the right price, and how these same people expected that they could somehow remain at arm's length from the dirty work that would be done on their behalf, wistfully as "ignorant" as a mafia Don. Technology didn't change the facts of life, and it never would, but this was not a view of the world supported by the sales literature of many tech companies. Too bad people weren't less willing to buy into the sales pitch. "There's one thing more I should say; in reality, for the most part it's been figured out how to define spam. It's best-described in an acronym…'UCE'…meaning 'unsolicited commercial e-mail.' Basically, spam almost always contains those three characteristics, and the amount that doesn't fit that definition is so small as to be inconsequential. But still, the problem exists that anti-spam software can't tell if a person wants the e-mail or not."

"I see your point. I never thought of that. So what do you do?" Now Jack was thinking right, starting to catch on and get the hang of it.

"Well, you have to think about it in terms of a threat model. It also helps to think in terms of the real world, which the Internet is part of, believe it or not. It used to be traveling salesmen, then it was telemarketers, and now it's spam. Of course, each version is more annoying and less trustworthy than the one before, but that's not important, the key is that it's something that we know in multiple forms already. Traveling salesmen were less like spammers than telemarketers are, so let's talk about telemarketing. The telemarketer needs a phone number to call you, and he also

needs you to answer the phone, which is why they block caller ID and call when you're sure to be home. Then, there's the spammer, who wants to send you e-mail, and there's you, who doesn't want to get it. What's the first thing he needs?"

"Uh. My e-mail address?"

"Right! But how do you think he gets it?"

"I dunno."

"There are a few ways. Do you shop online?"

"Oh, no, I knew it! I *told* her that it wasn't safe…"

Reuben wasn't prepared for this reaction. "No, no, relax, it's fine to shop online. That's not what I was getting at. My point is, some of these places ask for your e-mail address. Some of them do share that with other people."

"But don't you need to give them that to buy from them?"

"Yes, but you can have more than one address, right? Create one for just that sort of purpose, and use it just for that. Any e-mail that goes to that address is suspect then, unless you're expecting something like a receipt or a quote, right? And in the meanwhile, your normal e-mail is left clean from spam that would come from that method."

Jack paused for a second, seemingly remembering what options he had that were underused. "Yes, I get you…makes sense. There's more, yeah?"

"Yes, and good thinking to guess that. You're getting the hang of this! Do you have a website?"

"No, why?"

"Because a lot of people who set up websites create a kind of link, called a 'mailto' link, that enables people to e-mail them. The problem is, spammers search through websites en masse, harvesting e-mail addresses from these links. It's one more way to get your address out there where people can see it without you knowing it, and therefore spam you."

"Got you so far, OK. But I don't have a website. What else do they do to get e-mail names?"

"A lot of people are on mailing lists, which are kind of like e-mail turned into a common forum of communication. If you're on one, you know what I mean, but it's easier to demonstrate in use than it is to explain. Most of these are archived in some way, and those archives are

available on the web. Spammers harvest e-mail addresses from these archives, or if the list has enough members, they'll even join it just to be able to snag addresses if there's no archive."

"So what do you do about that?" Jack was really into this now, but seemed to feel like a lost babe in the woods.

"Well, it depends a bit. That's a hard problem to deal with; my solution has been to create yet another e-mail address to use for lists like that. I participate in about, oh…I think six at the moment, and they're all archived. But each of the lists has something unique about their traffic, whether it's a special word that gets added to the subject line to demonstrate which list it's from, or the address from which it originates. I have all e-mail that goes to that address pass through a set of rules…if the e-mail doesn't turn out to be from one of the six lists, it gets treated as spam. The problem is that sometimes people respond directly to one another regarding list content, without going through the list, in which case I'll get a legitimate e-mail that doesn't match any of the rules. I don't have a better solution for that one yet."

"Alright, but I see your point. So you use one e-mail address that you tell only your friends about, yeah? And the rest of everyone gets something else because you don't know if spammers will get it from them or not."

"Exactly. You've got it! When you really think about it, what you're looking to do is defend that primary e-mail address. And the first step in the whole chain of security is prevention. Unfortunately, with regard to spam, it's also your best step, as you can't get spammers to stop knowing the address when they get it, and there are still a lot of problems with the means to mitigate the impact when they start to spam you."

"I have no idea what that last part was about, but OK!"

"Alright, I can put it another way then. Look at it like us versus them. We know who 'us' is, but who's the enemy?"

"The spammers?"

"Right. What do they want?"

"Uh…for me to have a big dick?" Jack laughed.

Reuben smiled in response, "Basically, yeah…to spam you. And you can't control the actions of other people directly; all you can do is make it

infeasible for them to act on their intentions. The spammers need something first."

"My e-mail address."

"Right. So that's something that you can control; it's like an asset you can defend. Er…it's like a prison in a certain sort of way."

Jack was totally taken off guard by this. "What??"

Reuben laughed at the reaction, "Relax, it's not like what you're probably thinking, whatever that is. What I mean is, you've got all these prisoners, who obviously would do bad things if they could. If you've ever been inside a prison, or seen a scene like that on TV or in a movie, you notice how there are no guns inside the prison itself, even in the hands of many of the guards, right?"

"Yeah…so that the prisoners can't use them if there's an uprising."

"Exactly. If there's an uprising, you can't control the prisoners, but you can still limit the harm they can do by keeping them from getting what they need to do that much harm. You can't keep spammers from spamming, but you can prevent them from getting what they need to spam you. In every prison, there's an armory I think, in case of an uprising, but it's kept out of reach and wellprotected. That way, if there is a prison break, the prisoners cannot become dangerous enough to actually leave the prison itself, and they are still contained."

Jack seemed to get it now, "Ohhhh…so what you're saying is that I need to think of spammers as like prisoners who are doing a prison break, and my e-mail address as the guns. Don't let the prisoners get them, and they can't do too much."

"Right. The key here is like lots of other things in security. You figure out what your opponent is trying to get to, and keep them from getting it. The basic principle is old and universal, really…it applies to protecting servers on a network from hackers just as it applied to protecting the guns of Navarone from attack by commandos in World War II. Except, of course, we hope to do a better job of it than the Nazis did." Reuben smiled.

"Got ya. But how do I do that? It's not a thing, you can't touch it. You can't lock it up and keep the key!"

"Yes, that's why things are a little different in my world. If someone steals a diamond or money, you can get it back. If someone steals information, you're screwed; there is absolutely no way to put the genie back in the bottle with absolute certainty. That's why spam only seems to get worse. When you start out, your e-mail address is known only to you. Eventually, though, a spammer gets it, and then he starts spamming. Then, another does, and he joins in. After time, more and more of them join in, and in the meanwhile very few of them ever stop. So, the number of spam e-mails you get only goes up as time passes. Unlike a diamond or a specific dollar bill, the same bit of information can be held by more than one person at one time."

"Good point. But what do I do?"

"Start off with a new e-mail address. If you're feeling brave, you can even get your own domain; that way you can basically keep the same address, even if you change ISPs."

"I'm not that kind of brave. "

"Okay, that's fine. But you need to start anew, anyways. Spammers trade e-mail lists. Then you start protecting that one address, the way I said. Use it only with people you know, and have other addresses for use when shopping online, or posting to websites or mailing lists. Oh yeah, if you use instant messaging, make sure the e-mail address isn't in your profile either. Spammers look there too."

"So that's it, basically?"

"Yeah, that's it. And use anti-spam software too. A lot of it isn't too good yet, but it's going to get better. Some very talented minds are working hard to make them better, and it's only a matter of time."

"After all that, the answer seems too simple. That's it? Just kind of divide up the world and trust the pieces differently?"

"Well, yes. OK, think of it like this. What does the CIA do with their information?"

Jack finally got it. "Oh, I get it! So my main address is 'Top Secret,' and the other ones are less classified."

"Exactly! And as for it being simple, any good solution is simple. Complexity always brings problems."

"Cool. I'll do that. Hey, thanks man. Can I buy you a beer?"

"Sure, if you want. I'll let you in on a secret. Beer is like currency with geeks. We all drink it, we all love it, and we all have good taste in it. You can usually tell how seasoned a geek is by how much of a beer snob they are. Me, my favorite kind of beer is something in the style of a Belgian ale, typically a Trappist ale," he grinned.

"Uh…OK, you've lost me again. You guys must get out a lot more than I thought!"

Reuben laughed, "Not all of us, I like to think I'm a bit better about that than most. I live in the fun part of D.C…kind of like Greenwich Village, or at least as close to it as there could be in Washington. The city is kind of stiff."

Jack's eyes widened a bit. "Do you do anything for the CIA? Anything like that?"

Reuben waved his hand, "No, no…I only work in the commercial realm. I don't have a clearance or anything like that, and I've never done work for the federal government. They don't trust guys like me, usually. I don't blame them; a lot of people who do what I do used to be hackers on the wrong side of the law, and some of them still have a foot in each world. There's not much reason to risk the kind of harm they could do if they didn't stay clean, what with foreign intelligence organizations willing to recruit them with offers of cash or God knows what else. Most of the security geeks in that world have a military background, but that's a problem too, because the military typically seeks to engender conformity, and an unconventional mind is key to doing this well."

"Yeah, I bet. Hey, are other countries trying to attack us like that? With hackers?"

"Er…I don't know if I have the whole story on that. I can say this, a lot of probes come from other countries. It's hard to be sure who's doing the probing though. Some from China or Russia originate from universities, and so it could either be college students, who tend to hack, or it could be the information warfare researchers which they have, who are also affiliated with universities. Others could just be computers that were hacked by bad guys somewhere else, and used as routing points for probes. It's a complicated, uncertain thing that everyone's trying to get a grip on.

But to answer your question simply, I think yes, they're looking into it. But I don't see them doing much with it."

"What? Why?"

"That's simple. Here's the concept behind it. One, nobody wants to face us on a modern battlefield. Ten years ago, Saddam Hussein had the world's largest standing army and we took it apart in days with a numerically inferior force. We just massacred them; in slightly less than a month, we killed a huge portion of their soldiers and absolutely gutted their warfighting capacity. This was a modern army, with modern weapons. It just wasn't as modern as our army, and nobody is anymore, really. Our tanks weren't restricted to roads as they were because we had GPS; we could navigate in the desert without any landmarks, and they could not, so we could outflank them. Our tanks have depleted uranium armor, which nobody else in the world has, we have stealth aircraft, we have communications and control systems that are unmatched. We can move and fight with more speed and flexibility than anyone else.

"Alright. So, if you can't fight us normally, then what? It's called 'asymmetric warfare,' and it's a new term for an old concept. It describes a situation where you fight the enemy using one method, and they fight with another. In Beirut, when we shelled the city with rounds from the USS New Jersey, they were taking hostages and using suicide bombers to blow up our Embassy and Marine Barracks. That's asymmetric warfare. So terrorism is one example…but the problem is that not too many Americans are really into that. It's not that bad living here, and we're not really an imperialist, oppressive regime, no matter what our enemies say. And it's awfully hard to move in any society in secrecy without the assistance of people who are native to that society. So terrorists are hard-pressed to find help here, while the FBI does an excellent job of hunting them down for even trying. So that doesn't really work."

Jack stopped him for a second. "Okay, wait. How the hell do you know all this? You look like a kid."

Reuben laughed a bit, leaning back. "Oh, yeah, I see your point. Yeah, I don't look like what I am, entirely. First of all, I'm from DC. You tend to hear a lot more in that area about things like this. There are a lot of people who live, breathe, and eat the stuff, and you end up rubbing against it. And I actually studied both marketing and counterterrorism in college at

GWU. I went there to go to business school, but it's the same old DC story. I got the chance to study when they got this amazing new researcher there, so I took it. Kind of funny, I never studied computer science in college, but what I did study, I've been able to put to good use. I always had an interest, anyways. When I was seventeen, I went to Italy to visit some family there, and it was only weeks after the Rome airport massacre, in 1986. I remember the impact that the event had on everyone there, how you could just tell. That's always stuck in my mind."

"Wow, I bet. You sure you're not CIA or something? No, wait, don't tell me, I don't wanna know. Sorry to interrupt." Jack redirected back to the topic at hand.

Reuben nodded and continued, "So what else can they do…hack us, right? After all, the attackers can route it through systems in other countries, and by doing so hide the source of the attack. There are all these computers that we depend on for all sorts of things, and it's only getting more so. And lots of them aren't very well secured, either. You don't need a lot of people to be able to do a lot of damage, and the people wouldn't be in any immediate danger. You can't spot hackers with a spy satellite, and it is really easy to keep them a secret. So they can hack us from afar and cause all sorts of damage and not have to worry, right?"

"Yeah…so why not?"

"Well, that's simple enough, but you have to look at the wider picture. It's a kind of terrorism, so I'll use another attack as an example. Pan Am flight 103 was blown out of the air by an attack that was the model of a terrorist act. It was unexpected, entirely effective, and the attackers themselves got away clean. We were guessing for years at what country was behind it, even trying to figure out why they did it. But guess what? We have a long memory. We eventually, through intelligence gathering, figured out what country was behind it; it was Libya. They did it for hire, and we even figured out the names of the men who ran the operation; two men were the principal masterminds. And we leveraged sanctions against Libya for it, and put the screws to them in every way imaginable. It wasn't the kind of thing that we'd invade them over, so we didn't. But the point is this; just because someone doesn't want to face us on a modern battlefield doesn't mean we won't make them, by invading them as we did Iraq. And

the more damage the attackers do, the worse the pain will be when we find out who was behind it. And let's not forget, we're one of only two superpowers with the ability to do so much damage to a country as to make the rest of the planet uninhabitable. We can literally wipe a nation off the face of the earth; there is no limit to the amount of retaliation we can muster."

"Wow. I never thought of it that way. Good point. That's kind of cool!"

"Yeah, side effect of the Cold War…we're the world's biggest bad-asses. But, the problem is with organizations that have nothing to lose, you don't have to be a country to want to hurt us, and you don't need the support of one to do that kind of attack. So, if you ask me if another country will attack us like that, I don't think it'll happen anytime soon. But, some non-country organization? Maybe. I don't see it too soon; something like that doesn't exactly come out of nowhere, and it requires practice; every time there's a sea change in warfare, it's preceded by smaller events. Those smaller events haven't really happened yet. But I don't know how obvious the events will be either, since they are usually only spotted in hindsight after the sea change happens."

Saturday, July 29th, 10:02 AM, 2000

Reuben was regretting not getting more sleep the previous night. He had a chance to get more rest, but instead ended up speaking with Jack for quite a while. It was rewarding in that he helped another person understand how to be safe online and did a bit to fight the misconceptions about his line of work, but he really needed more sleep than he got. More importantly, he needed to go to bed on a local timetable, rather than the arbitrary one he seemed to be keeping now. *Ah, well,* he thought. *I seem to do this every year, why change it now, eh?* At least the first sessions of the day, which had just started, didn't really interest him. He had an hour or so to get his "con-fu" working. DefCon needed better coffee though…beer really wasn't going to help this process along just now. More coffee sounded great, but he just couldn't get himself to drink what they were serving there; it tasted awful. Unfortunately, his time as a professional had garnered him enough personal wealth to become coddled about such

things, but so be it. Despite the occasional value of being able to suck it up and drink corrosive sludge for the caffeine, he much preferred being able to consider Starbucks 'slumming'.

Deciding instead to just let himself get up to speed, he walked outside into the already-warm morning air. *So odd, how it's always so dry here,* he thought. It was nice in a way, but it also felt a bit like being in an oven, literally. Growing up on the coast of New England, Reuben was used to cold and water - lots of water. Being in a place where the land was so flat, and the visibility so good (dry air is clearer for longer distance) was odd to him. At least there were mountains in the distance, unlike the Midwest, which he just found disorienting after a day or so. He wondered how much water had to be pumped into the pools every week to keep the levels up; he'd heard that the fountains in front of the Bellagio went through tens of thousands of gallons of water every day from evaporation. There was something so surreal about all the effort it took to make Vegas work the way it did. Lawns by some casinos, gargantuan fountains, trees, enormous swimming pools, artificial ponds…all in a place that saw less rain in a year than his hometown got in some weeks. At least they didn't have to heat the pools much, if at all.

He sat down on one of the chairs outside, and thunked down his pack, opening it and grabbing his minidisc player. Maybe some music would help…and while there wasn't anything going on yet, it was a good time to just chill out and listen to some mood music to fit the setting. He rummaged around, pulling out some trance music…nothing too hard, just something to reflect the feel of all the hackers spooling up mentally as the morning heated. He put in his earphones, thumbed the remote…

"Hey man! How've you been? Good to see you here!" It was Paul, someone Reuben knew from the 2600 meetings in his area, but hadn't seen in a while. He hadn't ever been a long-term steady attendee of the meetings, and luckily hadn't been around for any of the few raids that took place.

2600 was a quarterly magazine about hacking and other related subjects, and one thing that they started were monthly gatherings in myriad large cities. For Washington, DC, the meetings were in the food court of the Pentagon City Mall; the funny thing was that you could walk right

past it without noticing, if you didn't know what to look for. At any rate, at one meeting he met a group of guys who drove up from central Virginia together. After the meeting, which Reuben missed much of, he joined them to go out to a strip club. They were the only people in the club who weren't intently watching the dancers, instead preferring to speak geek with each other.

Paul was one of the newer people to start attending 2600 meetings in the DC area, in the long-term scope of things. Back in the early 90's, Reuben was a more constant attendee, and in those days he was also typically one of a small minority that were over eighteen. In more recent years, the typical age of those at the meetings climbed, as the younger crowd by then had gone off to college, to be replaced by others who had been to college and were now working in the DC area with an interest in security. Reuben missed some of those guys. He had started going to the meetings shortly after "The Bust," when the Secret Service decided to goose-step their way into the meeting and violate at least one of the first ten amendments of the Constitution. Mall security at that event had been reported as being unprofessional, and to this day Reuben preferred to bring his business to other malls whenever a choice was possible.

"Paul! How's life? I didn't expect to see you here!" Nobody expected to see people from back home at DefCon, unless they were in contact with them on a nearly daily basis. Reuben wondered why that was for a moment before his mind came back to the conversation.

"Not too bad. Were you here for the Briefings too? I didn't see you…"

"Yeah, I was. Funny…if I knew you were here…oh well, at least we know now! We need to go out for a drink later—are any of the other guys here?"

"Yeah, they are…I don't know that they're all up yet though. We went out last night and blew WAY too much money and far too many brain cells. But hey, it's Vegas, right?"

"True enough! So have a seat, man…tell me what's been up? How are things with your wife…uh, I forgot her name…"

"She's good…she's with me this year, actually. Today she's going shopping…God knows how much it's going to cost me! How about you, seeing anyone right now?" Paul was like Reuben in that he didn't just

think tech; he also was a people person, more so than the average person and WAY more than the average hardcore geek.

"Nope…well, not entirely nope. There's someone that it's going well with, but I've been busy, and we haven't exactly gone out yet. I plan to fix that when I get back, God willing."

"Cool, cool…hey, I'm off to check out the CTF stats…catch you later?"

Reuben wasn't sure if he was happy to be left alone to get himself up and running, or sorry that Paul was heading off and leaving him without any company. "OK…if there's anything really shocking, come back and let me know, OK?" Reuben didn't closely follow Capture The Flag, not caring so much about who won as much as about the general concept.

"Will do. Oh, hey, got my cell phone number?"

"Yeah, think so…wait, let me call you, then I'll know for sure, and you'll have mine; I just changed it." Reuben pulled out his cell phone and toggled to the name in it, hitting dial.

Paul's phone rang. "Yep, you got my number alright!" He answered it and hung up, saving the number. "Cool…talk to you later on today, alright?"

"See you then! Have fun."

Reuben put the earphones back in his ears as Paul walked inside, feeling better. That was the one thing about business travel, for any reason; it was so isolating. He was so used to people in D.C., who were as cold as ice usually. He didn't know whether it was partially because the city was so predatory…politics was the ultimate industry for 'us versus them' thinking and professional grudges…or if it was something else. All he knew was that when he went to other cities, including New York, he was astounded at how friendly everyone was compared to home. You'd be lucky in D.C. if anyone returned eye contact, much less smiled back or engaged you in conversation. But even that was more contact with people than you had when on business travel. You could only know someone so well in an hour, and it was only worthwhile to do so much to talk to them; odds are, after that hour or so, you'd not see them ever again. And it was so much work to be social in other ways too; if you wanted to unwind at the end

of the day, you had to find a place that you liked. And then, when you were somewhere else, you started all over again.

He got up, deciding to move around…maybe he'd see more familiar faces while moving through things, before it got too hectic. Enough of this sitting around crap.

Saturday, July 29th, 11:07 AM, 2000

"Hello…my name is Robert Graham, and I'm the CTO of Network Ice, and the chief architect of the BlackICE intrusion detection system, and what I'll be discussing today is some of our experiences with running IDS systems on the battlefield," stated the speaker. This session was on IDS evasion, a topic Reuben was eager to learn about. As much as he wanted to know how to pick an IDS, he also lusted to evade one on a penetration test, as much to show off as for any other reason, he had to admit.

"IDS Systems are sort of like weaponry in the war against hackers. Uh, but they're kind of like flaky weaponry, it's kind of like a tank that you might take out to the battlefield, and an enemy soldier can walk up behind it, and shoot a gun at it and it explodes." IDS technology seemed like something that was not as ready for public use as it was needed by the public. Necessity is the mother of invention, but invention has a sibling called "expedience." Reuben knew this already, but wanted to know just where the problems were. He had to admire Graham's candor and frankness in discussing this; it was rare as hell to hear a vendor talk about what was *not* right about their products, especially the man who was primarily responsible for their creation and design.

He raised many excellent points early on, such as the fact that an IDS does not prevent or stop attacks, but merely detects them. He also talked openly about how the "number of signatures" bragging by vendors was largely misleading, and that when you eliminated port number-based alerts, cgi-based alerts, and other simple things, you ended up with only a short list of truly interesting or sophisticated triggers. He further described the propensity for numerous false alerts and for crashing under heavy network traffic loads (or highly-fragmented traffic), both of which plagued most, if not all IDS at that time.

On the upside, he also detailed what an IDS *was* good for, like alerting admins to an attack or probe in progress, determining the nature of the attack, and sorting out where the attack hit. But what was really amazing were all the various ways that you could evade an IDS, even above and beyond the very cool methods that Reuben already knew about.

An IDS, for the most part, typically looks for familiar patterns in network traffic, patterns that are part of an attack. What wasn't widely known was that it was possible to deliberately cut the attack into multiple parts that would be re-assembled at the target computer; this was known as "fragmentation." Sometimes in TCP, for reasons of network configuration or other problems, it was necessary to be able to break what would be a full-sized packet in one network into smaller bits before it could pass through another network. Within TCP there were standards and protocol specifics that allowed for this to happen smoothly, and the receiver of the traffic would put the packets together to get the larger piece of data. The problem was that most IDS sensors didn't do this; they just looked at every fragment like it was the whole thing. So instead of seeing, "ThisPacketIsGoingToHackThe HellOutOfSomething," they saw "ThisP," "acke," "tIsGoi," and so on. A tool, known as fragrouter, was already out, and helped greatly with this form of obfuscation; any TCP traffic passed through it would be fragmented according to one or more of a number of methods specified by the user.

This much, Reuben already knew. What he did not know was that there were facilities in many higher-level protocols to perform fragmentation of a different sort. RPC, for example, could have record requests (used to locate a particular RPC-based service) spread over multiple packets, and Graham even demonstrated a small C library that would do this for you with just a minor change to exploit code that used RPC. Even nastier, it would slice the request up and add bits to it, doing so with a degree of randomness that meant that even the same attack against the same target wouldn't look the same twice.

Also notable were the ways that FTP traffic could be munged to be unrecognizable by using options. FTP's command-channel was based on telnet, and included in many servers the recognition of options that only telnet would need; by inserting these options (which, although recognized, were ignored by the server, but not ignored by the IDS) into a string, the

attacker could hide what command they were really sending, and thus many forms of attack against FTP servers (like brute-force login attempts). And if most IDS vendors hadn't addressed TCP fragmentation yet, this would really take them a while to fix, since it wasn't a simple matter of an attacker properly following a well-documented standard in their attack, but rather co-opting an otherwise ignored detail of a standard, in an unplanned way, to hide their attack. As a result, it wasn't yet defined what forms the method could take on, at least not in a clear way; it was up to the vendors to figure that out first. And obviously, since most of them didn't act on the easier-to-fix oversight of TCP fragmentation, even after over a year since it was first demonstrated as a problem, who knew when they'd get around to this problem. At least the speaker was the architect of an IDS; Reuben knew one company that would have it under control. Hopefully, competition would bring the other companies into line as well.

As the brief question and answer session unfolded, Reuben got up, not interested in the next session in that room. His mind swam with the data of some of the attacks he'd just seen described; they were pretty formidable, and deeply detailed. The problem was, the program didn't have much information about the other two speakers, aside from the fact that one was going to be speaking about LDAP, and the other about web application security. Thinking the fact that neither one presented even a short blurb about what they'd be discussing in time for the conference was a bad sign, he decided instead to get some lunch.

Looking at the schedule further, he realized that after the next session was another block with nothing that really appealed to him. The newbie track was about recon on NT-based networks, which was something he excelled in…not like it was really hard, with SMB announcements, the ability to enumerate with null sessions, and all the other goodies of a relatively immature network structure. The uberhax0r track was about steganography used to circumvent censorship, which was useful but not something that Reuben needed to know the nuts and bolts of. And finally, in the hax0r room, Cult of the Dead Cow was putting on their press conference/session, which Reuben definitely did not want to get caught in. With this in mind, and feeling hungry, he decided to get a more satisfying

lunch and crossed the street to the Hard Rock Café to get a sit-down meal, and perhaps go over some work-related items on his laptop.

Saturday, July 29th, 3:05 PM, 2000

Reuben edged into the session as it was starting. The speaker was some former DoD sort, who was going to talk about concepts like Acts of War, the Geneva Convention, and other constructs of international conflict as they applied to the acts of individual hackers. It promised to be particularly interesting to Reuben, who had a limited foreign affairs background from when he dabbled in the subject in college. Things that other people simply never thought about or knew, like the fact that the definition of "terrorism" differed between various federal agencies, were no secret to him as a result of those enlightening classes. While many here in the room looked up at the speaker as some distrustful standard-issue "Fed," in the pejorative sense of the word, Reuben wasn't so sure yet.

As the speaker detailed how the Geneva Convention defined combatants and non-combatants, and why the distinction was important, Reuben thought he was leading somewhere clever and insightful. That changed in short order, as the man went on from there to eventually suggest that China would launch a cruise missile at the home of some teenage script kiddie in Miami for defacing a website in their country. In reaction to the notion of all the hacking activity originating from China, he offered the excuse that it came from IP addresses allocated to universities, which must mean that they were just individual students. The problem with this was something Reuben (and everyone else who studied information warfare in the slightest) knew; in China, as in many countries where Internet access was restricted to the public, the centers of information warfare were in universities. Reuben was tempted to ask the man outright if he thought the audience was stupid. If Jack from last night, who was neither an international affairs specialist nor an information warfare adviser, could grasp what was wrong with everything this cheesehead on the stage was saying now, why didn't the cheesehead get it?

Leaving the session before he got any more annoyed, Reuben learned what he missed at the cDc event. He heard a snippet of a conversation about it, and just had to interject to make sure he wasn't losing his mind.

"Wait, I'm sorry…I don't mean to interrupt, but…did you say that they threw *meat* at the crowd?"

The small group that had been talking energetically about it looked at him with smiles, obviously happy to share the news, "Yup. RAW hamburger. Can you believe it?"

Reuben shook his head as he laughed, looking at the ground in mock disbelief, "Actually, I can…but it's even more out-there than I expected them to be. What did they announce?"

The stranger chuckled, "Nothing, really. It was hella freaky. They started out all serious, like a panel group…we were all, 'what the fuck is this?' But then out came these other guys…it was strange. They did a human sacrifice to protect their new website, and started to let fly with the meat."

Reuben had no idea what to say to that, "Now THAT is hard to imagine. They didn't announce anything, really? Just a new website? No new tool or anything like that? Peekabooty isn't done?" he asked, referring to the anti-censorship system for web browsers that they had been working on.

"Yep, that's it. They said the website would have a bunch of announcements but that it'd be after the Con. Lame, huh?"

"Yeah, I have to admit, it's pretty lame. I'm surprised; as wild as they got, they always delivered something of value…but I guess not this time. It's like a vaporware press conference."

"That's about it, man. They were all there too. Catch you later."

"Yeah, thanks…later, guys," Reuben acknowledged as he walked off. *Raw meat…unbelievable*, he thought. *Only at DefCon!*

Reuben walked to the bar. Waiting his turn to order another beer, he sat down at the last available table. Dragging the laptop out of his pack, he booted up and fished out the CD of presentations from the Black Hat Briefings. As the laptop slowly finished loading services, he popped in the CD and started browsing, looking for more information about the sessions he wasn't able to get into. The thing about the Briefings was that there was usually more than one session that you wanted to catch at the same time. The information was so good, he wished there could be two of him to

catch it all. The CD helped, but he still wondered what was discussed by the speaker and wasn't included on the CD.

The Black Hat Briefings tended to be the kind of in-depth, no-holds-barred bad news about vulnerabilities and cutting-edge attack methods that could only be presented to a fairly trustworthy audience. The price of the conference was far out of reach of any standard teen hacker, and the content was beyond the grasp of any script kiddie at any age, fortunately. As a result, the speakers felt comfortable divulging things in depth that they'd never disclose so fully anywhere else. The bad news was that with multiple sessions of such quality going simultaneously, it was a real challenge to pick the best sessions to attend, and there were always tradeoffs. Of course, this was the best kind of problem to have…better to be immersed in useful data in one session and worrying what you might be missing elsewhere than bored no matter where you went. And during breaks and meals, the intermingling of the audience members invariably acted as fertile ground for enlightening discussion. Whenever possible, Reuben tried to remember which missed sessions most interested him, based on what he'd heard from others, and sought to capture as much of the data as possible. At this point, it was pretty much down to looking at whatever material was on the CD, as many of the Black Hat attendees didn't come to DefCon; those who did tended to be tight-lipped about the real good information, for obvious reasons. He sipped his beer as he flipped through presentation slides, reading rapidly. Putting the beer down, he noticed how quickly he was ripping through the material, and smiled to himself, thinking back…

Reuben had always been a voracious reader throughout his life, reading nearly anything that stretched his mind, but preferring things that added to the stock of information in his mind. Above and beyond the obvious benefits of a life devoted to such absorption of knowledge was the ability to read quickly and extract useful information from a mass of text. These days, it served him particularly well, as he subscribed to over a dozen trade periodicals, some of them weekly publications, and read through them comprehensively. This in turn allowed him to see certain trends before they came to fruition, including technologies that were poised for widespread adoption.

Reuben had learned to program at an early age, and shortly thereafter was lucky enough to have his own computer to play with, but hadn't really figured out how to leverage his proficiency until much later in life. He went to college to study marketing instead of computer science, as he didn't feel particularly interested in what a CS degree would lead him to at that point in time. His other extracurricular activity was Junior Achievement, and he showed promise as a future M.B.A., and thus he picked that path.

In the few short years after college, however, two things became apparent to him; one, that he was not happy in the corporate world, and two, that he was invariably drawn to computer-heavy aspects of his work. Being able to teach others how to best use computers gave way to doing complex spreadsheets for financial modeling, and later on, database design and analysis. Combined with evolution of programming methodologies, the advent of widespread networking and computers on nearly every desktop, the nature of being a professional geek had transformed into something that Reuben wanted to be. From there, it was a fairly straightforward path; the Web was starting to grow, and it was a trivial effort to become a capable webmaster and start his own small business. Once he noticed the glut of web designers coming, he applied himself to learning more about networking, and moved toward that, getting a job with a local integrator, LAN-Incorporated Systems, or just "LIS," as they liked to call themselves.

In his first week there, however, something came to light. Reuben had always been fascinated by hackers, and although he himself had never crossed the line by breaking into systems, he had studied the methods and means over the years, even practicing on his own system and home at times. While waiting outside the office of his new employer one cold morning, he noticed a mistake in how the deadbolt of the door was installed, making it easy to pop open. Once let in, he notified the manager who opened the door for him, and figured that would be the end of it.

Later that morning, the president of LIS came by Reuben's cubicle, asking about it. Reuben quickly explained the nature of the problem, to which the president merely replied with a smile, "Show me." Reuben grabbed his small black bag (he always carried some kind of bag to store

various small handy gadgets) and walked to the door, as other employees started following in curiosity.

Once outside the door in question, Reuben reached into his bag and pulled out his Swiss army knife, opening up the fish scaler. Slipping the metal of the scaler under the bolt between door and jamb, he pulled on the door with one hand and the knife with the other…and the bolt was pushed back into the door, which opened instantly.

The following few seconds marked a turning point for Reuben. He'd always assumed that should anyone know what he was capable of, they'd never believe that he'd not abuse the ability, and instead feel that he'd be untrustworthy. When he told his manager of the problem, he wasn't thinking ahead to how it might turn into a demonstration of his black-bag skills, but now he was beyond the point of no return, and sure that he'd screwed himself but good. But what followed was quite unexpected.

The president looked in smiling amazement. "Do it again!" Reuben stepped back outside and repeated the action, able to do it even more quickly now for having sorted it out once. As he re-entered through the "locked" door, the smiles on everyone's faces helped him relax a bit. Apparently, for some unknown reason, they didn't see him as a threat at all, but rather as something very interesting…and on their side. It was possible to openly dabble in the black arts of security without being branded an enemy or threat. From that point onward, Reuben was "that guy" who knew about "those things," and was a valuable resource for specific insights into security implications when such views were needed. His main focus was other things, though, as the need for such insights was infrequent and unreliable.

As firewalls and other security measures became less exotic to their clientele, however, Reuben increasingly specialized his skills in the arena of security, and eventually even started a fledgling division that focused on offering security solutions to the client base. For whatever reason, though, it didn't quite work out. It could have been that the solutions were too expensive for their type of clients, that there wasn't enough marketing yet, or simply that security wasn't as much of a priority as it became in later years. In the end, Reuben realized that he'd grown to crave work that he'd not be able to do without going to another employer. And that's where he

was now, unfortunately, skilled, trained, innately predisposed, and unable to find enough use for it without leaving a company that had nurtured tremendous growth in his skills and talents. He was very attached to LIS, and hated the thought of leaving…but he also hated the idea of not being able to earnestly pursue security work in the future, which seemed to be where things were heading.

Reuben shook his head, not wanting to think about that just now, and went back to his beer and reading the presentations. There were some things he wanted to play with, but they'd have to wait until he got back home to play with his other machines, as they all ran on Linux, and his laptop wasn't set up with anything besides Windows.

The bar swelled with more people suddenly; the session Reuben had left was over, and it looked like people were getting tired and calling it a day for attending more talks. He didn't blame them, as he'd long since learned to conserve his energy and be selective. It started to seem like the people who didn't attend the Black Hat Briefings prior to DefCon didn't have any more energy left over than he did, at least. Either way, he had little interest in any of the three sessions that were starting just then, and resumed combing through the information on the CD.

Finishing off both the last of his beer and the information on the disc, he shut down his laptop and put it away. Deciding against a second beer, he just sat for a bit and watched the crowd. *I usually hook up with some better conversation by now,* he thought. *I don't seem to have found anyone with anything too engaging, though. Not surprising, I don't know that I have much in mind myself this time. Perhaps tonight at the Black and White Ball, when everyone's partying…* Reuben was starting to worry that this would be a less productive Con than he was accustomed to, in terms of what he could learn directly in conversation.

The Black and White Ball was the big social event of DefCon, the name (and corresponding dress code) a clever play on the mixture of "blackhats" and "whitehats" that attend. A large room was cleared for something akin to a hacker prom, and a good number of people danced and drank and partied. At the same time, smaller parties tended to form ad hoc in numerous rooms around the hotel. It was a time when people got

together and socialized hard, only talking tech because they were geeks and, well, that's something geeks tended to do whenever they meet.

Another attendee stood in the bar, looking around with his open laptop in hand, obviously hoping for an empty table in the bar where he could sit. Reuben motioned him over as he packed up his stuff. "I'm just about to get out of here…go ahead, take this table."

"Right on, thanks." The guy looked a little nervous for some reason. Who knew…maybe he had to work on a deliverable for his job and was behind the eight-ball on it. There always were the demands on geeks, particularly since there seemed to be too few of them. It was only busier for good security geeks, as they were the rarest of the bunch. It seemed like the dot-com boom was undergoing some strangeness, and geeks were under more pressure lately because of it. After a year or two of feeling like perhaps he'd been missing out, Reuben was starting to feel happy he never jumped onto the dot-com bandwagon. Certain things about the companies just never sat right with him, but above all else he despised slogan-shouting, mantra-chanting, buzzword-using, successory-buying managers. People who made much ado about the latest self-help book clearly needed to learn less about psychobabble and more about actually running a business, in his experience. And geeks like this poor nervous guy were getting the brunt of the problems caused by such managers.

Reuben walked out of the bar, and went outside to soak up some of the heat and walk around before the next session, which he was increasingly curious about.

Saturday, July 29th, 4:23 PM, 2000

"Today I'm going to be talking about autonomous nodes, which are…basically…little computer programs that, you can say they have their own artificial intelligence inside. The idea is not that they're artificially intelligent, it's just that they have rules. They live by those rules, and die by those rules, and they don't talk to anyone else, they just do their own thing." The speaker continued, clarifying the difference between autonomous nodes and intelligent agents; an intelligent agent is interactive with something, while an autonomous node actually acts in the opposite way, disregarding input

except for perhaps some very narrow forms of information that it collects. As a result, it becomes far more robust, being invulnerable to countermeasures that would fool them by providing incorrect input.

Interesting…it's like heuristics incorporated into hacking software but a bit more developed. You have to know, in advance, what it is you'll have the node do and what it may encounter, Reuben thought. This was something unexpected. While DefCon often had cutting-edge talks, this was definitely much more surprising; he'd never heard of anything like this before. Looking down his program guide, he saw that the speaker was listed as "MadFast," with no professional affiliation mentioned. It suddenly dawned on Reuben that he was the nervous guy with the laptop in the bar just 45 minutes earlier.

He was much more nervous now, it seemed. MadFast was clearly uncomfortable addressing an audience. The reason why wasn't too hard to imagine; DefCon could be a rough crowd. Heckling was entirely possible, if not inevitable, if a presenter didn't seem to know what he was talking about. What was worse was that heckling here had a powerful cerebral bite to it; only the worst of fools dared open their mouth loudly without being entirely sure what they were saying. I'd be nervous too, thought Reuben.

MadFast elaborated upon real-world tests of similar concepts, in particular something that Sandia had done. They'd set up a network where the server applications incorporated the technology, for purposes of coordinated defense against attacks. The end result had been a network that seemed to be unhackable; it just reacted too quickly. Every attacker they let try utterly failed to make a dent in it. The problem was that everything needed to be integrated, and the task of doing such a thing in a non-test environment was too much to handle. Still, it demonstrated the principle of an organic network, capable of something akin to an immune response. So, autonomous nodes weren't just something that could be used offensively.

My God, I just watched the world change a little bit. Reuben listened to the presenter nervously discuss the subject matter he was presenting, and pondered the implications. Most of the people in the audience were losing interest, probably for a variety of reasons ranging from fatigue to inability to see the ramifications to just plain inebriation, but that didn't matter. While at DefCon the future was often described years in advance, that

didn't mean that everyone noticed the future when they saw it. The concept of multiple autonomous programmatic entities that operated independent of even outside input (and what this could achieve in terms of both attacking and defending a computer network) was by no means an easy thing to grasp. But just the same, it was fascinating. If only we can overcome the integration challenges. There needs to be a way to standardize, to make it modular.

Unfortunately, the demonstration wasn't going to happen, as there had been some recent and major changes to the planned design, and the proof of concept wasn't finished yet. Still, it was easy enough to see the potential strengths and weaknesses of such a system.

After the presentation, Reuben hurried to the side of the stage to meet MadFast, wanting to pick his brain for more information and toss some ideas back and forth. "Hey, great talk man! I want to know more…can I buy you a beer?"

"Right on! Sure, just let me answer some more questions, and let's go," he replied. Reuben relaxed, and thought about what he wanted to discuss. The challenges of defending against such a thing, the complexity of programming even the simplest of such systems, considering that they didn't react on any level to outside input…this was likely to be the most interesting conversation he'd ever had over drinks.

At the bar, Reuben promptly bought a couple of Heinekens and sat down with MadFast. "So, where are you from?"

"Ah, Seattle. Lived there all my life. You?"

"Originally from Rhode Island, but went to college in DC back in '87 and never left. So I guess I'm really from there now."

"Right on…so, do much government work?" MadFast asked the question casually, not with the kind of almost accusatory suspicion that Reuben would expect here at DefCon.

"Ah, no. Been strictly in the commercial realm, really. The company I work for does a little federal stuff, but I'm not usually involved in it. Seems pretty crazy too, with all the paperwork needed for a contract, I'm glad I don't have to sweat it."

"Right on…what kind of work do you do?"

Reuben was surprised that MadFast was so curious about him. He expected to be the one with all the questions. "Well, did networking, but now I'm mostly a firewall guy, with some penetration testing. Getting into IDS though."

"Right on, cool. I'm mostly a coder myself, I don't know about what happens on the wire exactly. I'm into crypto, and I've been playing around with some number theory, higher math sort of stuff. I've been coding pretty hard since I was about fifteen or so, and now I'm just doing independent projects here and there." MadFast wasn't what Reuben expected; he was a lot more down to earth than many people who spoke here, and seemed utterly devoid of any kind of ego. Good hackers were known to puff their feathers up pretty hard at times; Reuben was as guilty of it as anyone, and if ever was the time, coming off the stage at DefCon had to be it.

"Ahh…I've done some programming, but nothing too hard. I guess we're from different parts of the whole equation then. That's cool. So, tell me…it seems to me that an autonomous node would either have to be really simple or really complex. If it's really simple though, wouldn't it be easy to recognize it with some kind of signature?"

"Yes, but they have to know it's coming first. You can keep it simple, and write them as one-shot attacks. Or even more interesting, you can fragment the node; you can have two nodes do separate tasks of the larger goal. You could even go so far as to have the nodes all work like separate pieces of a larger goal, and put them in place gradually. Only when they are all there does the big picture become apparent."

Reuben leaned back a bit, assembling the pieces in his mind. Every program he knew of that detected hostile code used signatures or heuristics. If a hostile bit of software was broken up properly, the signatures wouldn't match. And heuristics, which tried to guess at detecting suspicious functions within software, would be fooled entirely, since they weren't smart enough to look at the combined actions of multiple bits of software. This kind of attack would fool both easily. "Wow. I didn't think of it like that."

"Yeah, huh? That's some hella-cool work there. It's for a real uber-hack, something really huge. That's what I'm talking about…you go in, and you go in BIG, but in pieces."

"No shit. Wow." Reuben was starting to really understand how this could be nasty, even nastier than he'd imagined. "Is there a way to use that tactic defensively?"

"That's a problem…I don't think so. But attackers don't run IDS either. I mean in a sense you're doing that if you do what Sandia did, but it's really kind of different from that."

"Good point. Didn't think of it that way." Reuben suddenly remembered the beer he had been ignoring, taking a big slug of it. "Okay; here's a thought. Can you have one component deliver itself as an encrypted payload, and the other component as the decryptor?"

MadFast took a drink of his beer as well. "Hell yeah…that's a cool idea." He meditated on that one for a minute. "Without the decryptor, nobody would know what the payload was. You could get the payload everywhere first. Smart people would catch the attack and clean up, and you'd get nowhere after that on those networks, but you wouldn't tip your hand either. And the machines that stayed infected with the payload would be useful to you as soon as you hit everything with the second piece. Hella-leet!" MadFast smiled widely.

"Oh! I'm Reuben, by the way. I sometimes go by Tripwyre, but well…I guess I'm just more comfortable just under my normal name." He laughed, suddenly realizing that hadn't introduced himself prior to delving into deep conversation about potential attack vectors. Geeks had their priorities, after all. "I've always been clean, so I never really worried about it much."

"Ah, nice to meet you." MadFast smiled at him like he was thinking of something new. "Tell me, do you know what CC is?"

"CC? I'm guessing you don't mean in e-mail."

"Nope. Caezar's Challenge."

"Ah, no. What is it? Sounds like a puzzle."

"Sorta. Caezar is a hacker; every year at DefCon, he holds an event. It's invite-only, and open bar. Everyone gets together at midnight and at the start of the night, he throws out a challenge; it's huge, so big nobody wants

to try it, some kind of hacking or security problem to solve, but really really hard. And everyone drinks and talks and drinks, and by sunrise, they solve it."

"Oh, COOL! That sounds amazing!" Reuben shifted forward in his seat in anticipation.

MadFast pulled out a printed index-card shaped piece of paper and slid it over to Reuben. "CC IV," it stated in colorful letters. "Here ya go, it's tonight. Nobody knows where until an hour beforehand, so when it gets to be after 11, find one of us and show them the invite."

The problem was that Reuben didn't know who "us" meant. It didn't matter, anyway, as he had another idea. "How about this instead…are you hungry? I'll buy you dinner. I'm really into this conversation, and I want to keep talking, but I'm starving. And then I can help out, and not have to worry about missing CC?"

"Right on! Where? Not too far...I have to help out in a couple of hours."

"Alright, how about Hard Rock?"

"Right on, works for me." MadFast downed half the remaining beer as Reuben did likewise. The bar was filling up rapidly now as people started coming out of the last session of the day and began drinking in anticipation of the Black and White Ball.

Looks like I found my stride, finally! thought Reuben.

Chapter 3

The DoJ Project, Washington, DC, 2001

Washington, DC: Tuesday October 9th, 1:14 PM, 2001

"Alright, let me see if I understand you correctly. You've been burned in the past by consultants saying 'yeah, yeah, we know how to do that', and then after a few weeks of work they give you a deliverable that's big on words but doesn't really say much in terms of analysis; they don't boil it down and give you anything useful or coherent, right? And that's what you're afraid of this time?" Reuben talked calmly into the speaker phone in his boss' office at the Vigility Corporation.

The voice on the speakerphone piped back, "Exactly. We're on a tight schedule, so I can't afford to waste time on this." She called herself "Pam," and worked at the Department of Justice. A bigwig from Reuben's company had played golf with someone at DoJ over the previous weekend, and had learned that there was a need for some talent, in a hurry, for a project. Reuben's boss was instructed to make the call, and had Reuben with him for technical backup. The problem was, Pam hadn't been expecting the call, wasn't open to talking to vendors, and had someone in mind already. But she was also clearly not comfortable with what she had in the pipe; she was on a tight schedule and was afraid of spinning her wheels with someone who could claim to do the work better than they could deliver on it.

"Okay, good. That's what I thought, I've seen that myself." Reuben continued. "I'm not some sales guy, I'm just a geek. Bob has me in here because he wants someone watching over the technical things. I know how it is, how the salespeople offer things they don't really understand, but I'm not in that position, and I can't hide if I mislead you either. Bottom line, I'm the guy who'd be responsible for the geek work above anyone else, and I can tell you right now, we can give you what you want. If I'm wrong, it's my fault for lying to you outright, since I know what I can and can't do. Can I interest you in talking further?" He hoped this worked…

"Oh, definitely!" The woman at the other end seemed to do a total turnaround. Reuben's boss, Bobby "Bob" Marconi, had been about to acquiesce to her request to end the call when Reuben stopped him and interjected. Apparently it worked.

"All right. What do you want from us next, then? What should we do to move to the next step?" Bob asked.

"I'll get together a meeting…sometime in the next few days. I have to see when I can get everyone together, it'll be short notice. Can you be flexible?"

Bob and Reuben smiled at each other. Bob answered the question. "Sure, that's no problem. Just get back to us when you know, and we'll go forward from there. Look forward to hearing from you soon."

The call ended, and the two looked at each other. "I can't believe it…she was ready to hang up, and you turned her around!"

"Yeah, I don't know where that came from myself, but I'm glad I spoke up. I just knew what to say; I totally heard where she was coming from. I've seen so many companies promise this and that in security, and offer up shit, and get away with it because everyone expects it to be mumbo-jumbo anyways, so they don't know when they're getting bullshit."

Bob held his hands up. "All I know is, now we gotta get our act together so we can do this. Who do we have besides you to help out?"

Reuben smiled…this is what he did. "I can do this with Dan, and we need one more guy, from the outside. He's a specialist in cryptography; I met him at DefCon last year, and now we're good friends. He's in Seattle, and just plain brilliant." Frank was MadFast's real name, as Reuben had learned later on. In Reuben's mind, though, he'd always be MadFast.

Bob looked a little concerned. "We gotta do a background check on this guy. Are you sure he's okay? I mean, we can't have a risk on this…"

Reuben waved his hands. "Relax, Bob. You have to meet him to see what I mean, but he's fine. I trust him. Believe me, I have no illusions; I know it's my ass if I don't come through here. And we need this guy."

"Okay, I'm trusting you on this one. Do me a favor, ask him if he's got any criminal records. I don't care one way or the other, but we gotta do a background check, so let him know that."

"Don't worry, I'll ask. I'll be surprised if there's anything to worry about, though. You'll see." Reuben grinned as he hung half in, half out of the doorway on the way out, before going back to his cubicle to call MadFast.

Managers were always suspicious of security geeks, and with some reason. Many had less-than-innocent pasts with respect to their actions online, and some still crossed the line in their free time, despite making a good living working for the good guys. As pristine as he was, Reuben was still a bit distrusted early on, even though they recruited him. He wasn't worried though; MadFast was just as clean as he was, and at least as good-natured. Once they met the guy, they'd see that there was nothing to worry about.

Reuben had left DefCon with a renewed sense of purpose regarding his career. The conversations he had in the last 24 hours of the Con boosted his confidence in his own abilities, and brought him to leave LIS,

taking a position with a large corporation that was building a red team for commercial work. Unfortunately, shortly after that an even larger corporation purchased his new employer, and the commercial unit to which Reuben belonged was being looked upon as an unwanted stepchild. One person at a time, the members of the team were being moved elsewhere or laid off; the team was already at a point where it lacked the critical mass to accomplish many things with its own staff. Everyone kept telling Reuben how valuable he was, and he believed it, but that wasn't the point. As long as the team was unsupported, they weren't getting any new business, and weren't *doing* anything. And Reuben hated that. When he was hired on there was the promise of being busy, busy, busy, doing all sorts of things. Red teams are primarily used to simulate an attacker, and thus working for one usually involves everything from hacking into systems to actually breaking and entering into facilities to gain access. Reuben loved the challenges and constant change in work that such a job entailed, but now he was stuck with something else entirely different.

The person at the other end of that phone call was in need of a company to take a look at a VPN product that her department was about to implement. Apparently, a new bit of regulation in the federal government stated that such things now needed independent evaluation by an outside company to verify that they were secure; as a result, the rollout was imperiled pending such an examination. The best part was, Reuben really did know that he could put together the team to do it, if he could get MadFast. Dan, one of the other few remaining members of the red team, was an infrastructure guy, and would be helpful in setting up the test network and running certain tests, but MadFast had the crypto experience that was needed to really test it properly. Nobody on the red team, including Reuben, had any idea as to how to perform tests like entropy analysis and other mathematically-based attacks. And Reuben had never coded an exploit; if there *was* a problem with the software, it would probably be necessary to prove it. He pulled out his PDA and looked up the phone number, dialing with one hand as he held the PDA in the other. He needed to work fast to see if he could put this together. People's attention seemed to be scattered lately, after the recent bombings, and it wasn't

impossible that this could get lost in things if it didn't start to take on a life of its own in the next week or two.

Voicemail. "When you hear the beep, you know what to do."

"Hey, man! It's Reuben. Give me a call…I've got some work I want to pull you in for. It's sexy stuff, I think it'll be a blast. Talk to you soon!"

He hung up and took a deep breath. If MadFast couldn't come aboard for whatever reason, he had to go with "Plan B." The problem was that there wasn't one. *I am Plan A…there is no Plan B,* he thought. *Just remember that, and everything will be fine.* The hard part now was waiting…waiting for the client to come back with a meeting time, waiting for MadFast to call back…

The phone rang; Reuben rocketed around in his chair to suck the handset off the phone.

"Hello."

"Hey man! How've you been?" It was MadFast.

"Hey! Great to hear from you. I'm good! The weather's been really nice here, and I'm still driving around with the top down. How's life in Seattle?"

"Right on. Ah, same old, same old. So what's this work all about? I'm curious!"

"Oh, yes. okay, we don't have it for sure, but I think we'll get it. It's federal, but they're in a hurry. We need to look at a VPN and try and poke holes in it, see if it's really secure."

"Is it installed?"

"No, we're testing the product itself, as it's intended to be implemented. We'll stand up a lab here and work on it in a closed environment. Interested?"

"Hell ya! Sounds like fun! There's one problem; I'm kind of tied up here with a company right now."

"Can you get some unpaid leave? A sabbatical? Anything? We only need a couple of weeks, I think. And we'll pay for it, obviously, including travel."

"Yeaaaaah, I think I can get them to go for it. Let me talk to them and call you back. I definitely want to get in on this. They'll probably think I'm crazy, wanting to go to DC right now, but that's their problem."

"Thank God, because I have no *idea* who else I'd call! You're the only guy I know who'd be able to do what I need. Oh, another thing…I don't think it'll be an issue, but they have to run a background check. Anything to worry about?"

"Don't think so. Some parking tickets."

"Nah, that doesn't matter. I didn't think it'd be a problem. Cool. Go talk to them, and give me a call back, man. It's going to be great working together!"

"No doubt! Talk at ya later!"

Alright, that was one thing taken care of. At least he wanted in, that was the good thing. Without that, nothing would work out. He decided to assume that MadFast would succeed in getting the time free, and went down the hall to go tell Bob the good news.

Bobby Marconi, was definitely the most interesting person and best manager, he'd worked for. For one thing, he was a paradox of the tech world; a manager with no technical background who knew exactly how to manage geeks. He was the antithesis of the pointy-haired boss; he did not micromanage, he had fantastic common sense, and wonderful people skills. He had served in a major law enforcement agency for nearly his entire career, doing undercover work and decades of field work before deciding to become management, at which point he rocketed up in the ranks until retirement. After retirement, he had been recruited to work here.

Bob didn't need to understand the technology; he could clearly smell bullshit a mile away, and trusted certain geeks to give him simplified answers to the basic questions, based on their own technical analysis. Bob had no problem with being unable to geek with everyone; he knew what his skills were, and was entirely comfortable with his own proficiency. Reuben respected him deeply, and enjoyed being a part of decisions. Reuben had long since decided that geeks made bad managers, and Bob was the ultimate proof. It seemed that usually ex-geek managers didn't know that managing people was a skill, not just something added to a job. Even worse, they had trouble facing the twilight of their technical hands-on skills, which deteriorated while they spent time managing. It was hard for a geek to let go like that, and most seemed to resent it on some level. It helped not at all that they were expected to know how to manage auto-

matically, without actually being taught any of the fundamentals of management.

It didn't matter that Bob didn't know the finer details of what Reuben did; hell, Reuben had to help Bob with his e-mail from time to time. He trusted Reuben to accomplish the larger goals, and stay within the lines of what was acceptable. What mattered was that Bob had no fear of admitting when he didn't know something; he knew more about how to do his job than anyone else Reuben had ever known, and didn't feel like he had to know how to do anyone else's on top of it. It was a wonderful and refreshing change that made Reuben wonder why there weren't more people who "got it" when it came to management. It seemed so clear when you saw it like this. You found good people, you asked their advice, and you trusted their counsel. They maintained their particular areas of knowledge, and the manager saw to it that they had the resources they needed to do their job.

He arrived at Bob's office, leaning in the doorway. "Alright, I just got off the phone with Madfa...I mean Frank. He's interested, and he's working out taking leave from the company he's working for at the moment. And yes, I asked, he's clean, no problem with a background check."

"Good. Now, what else are you gonna need? Computers to install this on?"

"Yeah, I'm thinking about that now. I need to know what they're going to run it on first, as far as operating systems. We can get that at the meeting. I need to think about how many we'll need, but we've got time for that. Oh, we also need a room that we can lock, to use as a lab."

"Are you sure we can do this?" Bob was nervous, but in a rather amicable way.

"Trust me, Bob. We can do this. Watch…this is going to be amazing. ALL software has problems, and we're going to find some." He smiled broadly. "I can't wait until you meet Frank!"

"How much money is he going to need?"

"We can figure that out. From what I can tell, he's not making much right now, but I don't want to take advantage of him either. We really need him, and he's a nice guy."

"Okay, but remember, he'll cost more because of the travel issue."

"Yeah, I've been thinking about that. A hotel in the area is really expensive, but there's this bed and breakfast down the street, half a block from me, where he could stay; it'd be really cheap, and quite comfortable. Besides, he and I could spend more time together working and whatnot that way too. We need to know as soon as possible when he'll be here, so we can get the tickets cheaper, but that's alright because we need to know that anyways so he can get the time off."

Reuben knew all too well that he and MadFast would be working much the same way, interspersing work with rest and fun. It just made more sense for them to be close by each other during the engagement. The trick was going to be the timing; everything had to be planned out in advance, and the clock would be ticking once MadFast arrived.

"Good. Set it up."

Reuben was pumped. This was some meaty fun work, and he was driving the project. He felt dangerous and excited. But there were still at least half a dozen ways this could die before he even got to do his thing. *No sense worrying about what's out of my hands…just think positive. Better to be prepared for something that doesn't happen then to be unprepared when it actually happens*. Walking back to his cubicle, his mind swirled with of all the ways he could attack the VPN.

One problem that always bothered Reuben was how fast he thought at times like this; he'd have idea after idea flash through his mind, and all he could do to keep them organized was to type them out as quickly as possible so that he'd have a list to go back to. *It would be really great if only the thoughts weren't so fleeting.* He launched Notepad for simplicity and started capturing all of the ideas in his internal brainstorming session. The keys clacked away like a Geiger counter as he smiled widely, loving the flow of thought coming out of his mind. He broke the attacks up into groups, depending on how the client was going to implement the VPN system. If they were going to use VPN gateways to link entire networks, that limited the scope of the attacks to VPN gateways only, but if they planned to use it for remote access from laptops and the like, that also meant that the VPN client could be attacked and that it would have to prove secure even if the laptop were in the wrong hands.

As the time between each generated idea increased, it became time to find more information based on what others had done. Googling for data turned up nothing, however. Most of what came up were posts informing people that a VPN was going to be tested for functionality. Nobody seemed to be trying to poke holes in them. *That's so odd,* Reuben thought. *It seems like there are so many avenues of attack.* In his mind, he walked through the potential impact if a VPN went down, as connections tried to recover. If the VPN stayed down, the impact could be severe; it wouldn't be trivial to reconfigure networks to speak to each other in the clear, if you even wanted to take that risk. Some VPNs did things like bridge broadcast traffic, and that functionality would be lost as well - a huge issue for many Windows-based networks.

Alright, so it looks like we're going into fairly uncharted territory here. That's okay, Reuben pondered. He decided to Google some information on the Diffie-Hellman key exchange algorithm, so that he'd have a better idea of how things could be done wrong. He knew that many products on the market utilized algorithms that were secure, but implemented them incorrectly, making them insecure.

The problem now was Reuben's lack of background in the form of mathematics that he was currently looking at. In college, he'd attended business school rather than focusing on computer science; the math curriculum was composed of simpler things, alloyed with such idiotic notions as an equation to tell you how much of each product to produce to maximize your profit as a corporation. Making matters worse, the maddening uselessness of such exercises drove Reuben to essentially do the minimum amount of work necessary to pass those classes, and now he had even less to work with than he did back then, mathematically speaking. *Oh well, time to learn now, I guess,* he thought. *I've taught myself harder and less well-defined things. At least with math, you can check your own work before anyone else has to rely on it.* He clicked back and forth through some of the pages that he was looking for, picking a few to print out and take home to look over after dinner before shutting down. He was cooking tonight, and wanted to do something nice for Briana, his girlfriend.

He walked over to the printer, grabbed the printed pages and put them into order before walking back to his cubicle and dropping them into his

laptop case. Packing up his laptop and mouse, he looked around to see if there was anything else he needed. He still had time to get to Whole Foods and pick up something special for dinner, and to find nearby parking once he got home.

Tuesday, October 9th, 9:21 PM, 2001

The beef was truly excellent, and now Reuben was sipping wine while talking shop with Briana. "Yeah, so they need this work done, and fast. I think they're really nervous, I couldn't find anyone who'd ever done any research or work like this either. They were probably about to deploy the thing, but now they have this huge requirement for outside examination, and it might muck the whole
thing up."

"And you get to save the day. You must be loving this!" Briana smiled. She enjoyed it when Reuben talked shop. She herself was an IT worker, but not in the same field as Reuben; she'd started out with web design, moving on to build the intranet of the law firm where she worked. When that was done, she became more database-centric and now was in charge of a colossal document management system migration, all for the same large D.C. law firm. She loved listening to Reuben gush about what he was working on, which was part of what got her interested in him to begin with. "He talked nerdy to me," as she described the first interaction between the two. She was intrigued by his day's events.

"Well, let's see if we get the business, but I don't know who else they'll go to, frankly. And I think I got Pam's trust; there's nobody else they could possibly talk to who will be able to say what I did with regards to geeky personal responsibility for the work. At least, not without lying their ass off!"

"Now tell me, what exactly is a VPN? I think I know, but I want to hear your version."

"Well, it's fairly simple to describe, but hard to do. Let's say you're a big bank, and you have major offices in a lot of different places. Between all these offices you have to be able to communicate securely…you really don't want anyone to listen to your internal communications, right?

Okay…the normal way of doing this for a long time was to have private leased lines between the offices, but that's really expensive. At first, it wasn't so bad, because Internet connections were expensive too, and so it was simpler to do it that way."

"But the Internet got cheaper."

"Exactly. So now the best way to do it is to make use of the Internet connections, but you still have the privacy/security thing to worry about. So you use encryption on all the packets that travel between offices that way. It ends up being cheaper than leased lines, although you have to use bigger Internet links because of the added traffic."

"Okay, but what about remote users? Isn't there something about them?"

"Yeah, that's another thing you can do with a VPN. What I just described is when you have two gateways talking to each other; if you do it right, the two different office networks are joined transparently, as if they were one larger network. But you can also have a gateway that clients log into, and they can act like they're on the local network when they might really be in a hotel room quite some distance away."

"Like dialup?"

"Yes, but here's the thing. Dialing into an office has some problems. There have been security risks with such access in the past, the modems have always been a bit finicky as well as expensive, and you either have to pay horrendous long-distance charges or equally heinous 800-number costs. But if you can just dial into the local access number for some large ISP like Mindspring…"

"Oh! No long distance, and a connection to the Internet…use the VPN client to connect to the home office, and it's secure."

"Exactly, you got it! And that's the main thing they'll be using this for, as I understand it. At least that's the application we're examining. It actually raises a lot of risks for security if done wrong, though."

"Why's that?"

"Well, okay. In a perfect world, the guy whose laptop has the client only gets used by him. But what if it gets stolen? How do you make sure that it can't be used by anyone else?"

"Didn't think of that."

"Even worse, what if the computer at someone's home office has been hacked, and has a Trojan? Or if the software on the laptop or home computer stores credentials in some insecure fashion, so that they can be copied onto another system. That's one of the worst things that can happen, because then nobody knows that an attacker has gained access. At least if someone steals the laptop, the guy will know about it and the attacker can only have access until the laptop's owner calls in to report the theft."

"So what are you going to be doing to check the software?"

"Anything and everything. When MadFast gets here we'll work out a plan of attack, I don't know how to do some of the things he'll be trying. We'll set a small network up, install the software, and set up a VPN. Then we'll just try all kinds of things to break it. I haven't been able to find much about doing this kind of work, so I think we'll be figuring it out as we go along, a bit. It's okay though, I know we can do this. The important thing will be remembering not to believe anything that we're told. If you listened to the companies that made software, you'd think everything was secure…in truth very little is as secure as it could or should be."

"This sounds like great work! I'm so proud of you…"

Reuben waved his hand, smiling, "Hang on, we don't have it locked up yet. Well, I think we'll get it, but we can't be sure. A hundred things could still go wrong. They might not give the okay for me to bring MadFast over, or DoJ might take so long to drop the hammer on this project that Bob and Dan and myself will all be at other companies by then…"

"But I thought they were under the gun?"

"Yeah, but I've seen it before; in federal work, it's hurry up and wait, and sometimes the waiting happens for stupid reasons. Budgets, politics or God–knows-what other things can fuck it all up without warning. I really hope nothing like that goes down this time though. I really want to do this work. How do you like the shiraz?"

Briana looked at her glass and examined it a bit. "It's okay, but I'm not much of a red wine person."

"Yeah, I know. I just figured I'd at least get you to try a lot of different kinds anyway, in case you were just missing something you liked." Reuben

smiled. He loved food, and loved introducing others to it only slightly less. "It's a lot different from the other reds you've had, I was betting."

"That's true. It's kind of like berries, not as strong-tasting either."

"Right."

"I've got another question. How bad is it if someone can break into a VPN?"

"Well, it's really bad. VPNs carry stuff that's sensitive, obviously. But something that's sensitive enough to secure like that is also important in another way. It's not enough to keep the information secret, the connections need to stay up so that the information can be transmitted from end to end. It's not cheap or simple to set up a VPN correctly yet, so if someone's using one, you can be damned sure that whatever communication takes place over it is as important as the secrecy surrounding it. Make sense?"

"Yeah, I didn't think of that. Makes a lot of sense."

"So, someone doesn't need to be able to actually read the traffic to cause a lot of harm. If they can just do a DoS attack, they've inflicted significant harm. And since the functions of a VPN are more complex than those of just normal networking, theoretically it should be easier to knock them over than it would be to just DoS normal unencrypted links."

"Okay, I had you until about halfway through. Then you lost me."

"Alright, let me put it another way. Good encryption in something like this involves certain things. One of them is the notion of a session. Sessions exist in a lot of things; all TCP-based connections have them, which means that a session exists when you browse a website, send mail, and so on. But in a VPN, the 'session' I'm talking about happens on *top* of that TCP session, so it's an added level of things that can go wrong."

"Ah, okay. Got it."

"Now, an attacker might not be able to decrypt the VPN session, but he might just want to bust things up. All he needs to do is break either kind of session and he's succeeded in that task. The good news is that TCP sessions have gotten steadily more robust over the years, as hackers have developed different ways to attack them. The bad news is that VPN sessions are, I think, an uncharted territory, and probably a lot less hard to

screw with. They haven't undergone much of an evolutionary process yet to kill off the weaker ways of doing things."

"Wow. Why do you think that?"

"Well, for one thing, they're fairly new technology. They've been around a little while, but are not too widely used. And for another thing, I haven't been able to find much at all about how to attack them. So either everyone got it right the first time when they started making VPNs, or nobody's done too much research yet into how to break them. Take a guess which one is more likely?" Reuben laughed lightheartedly.

"Uh, yeah. I see your point. I love talking about this with you! This sounds like fun!" Briana was beaming at him, clearly proud of him for one reason or another. "And it makes a difference. Nobody seems to know what to do right now, so it's amazing to see you having a chance to make things more secure." Neither of them talked much about 9/11, having been so close to it. Reuben had stayed in the Marriott at the World Trade Center on several occasions on business, and while he'd been at home doing some research on his home network that day, he heard the impact at the Pentagon.

"That's what I think too." Reuben was a very lucky guy to have a girl like Briana. She didn't feel like she competed for his energy and attention when it came to his career and geeky interest, and supported him for what he was. *If only I could find women like this for my friends,* he thought. Speaking of which, "I can't wait for you to meet MadFast, too. He's got to be the smartest guy I've ever met. And coming from my family, you know that's saying something."

"Wow. I've never heard you say that about anyone before. He must be something else. How does he act?"

"That's the really incredible thing. He's a really nice, socially-adjusted guy. He's fun to talk to, and has lots of interests. Mind you, he's a true dyed-in-the-wool geek like me, so tech is always hanging around in conversation, but that's okay too. When he talks tech, if you don't understand something, he'll gladly explain it to you, and doesn't talk down in the slightest. Good thing too; I'd not have understood much at all of what he spoke about at DefCon otherwise."

"So, when will he be coming?"

"I don't know; that depends on the work, and when it happens. Just a heads up, we'll be playing host to him when he does come. I want to get him a room at the Adams Inn so that he'll be close by. That way he won't need a rental car, and we can all hang out together."

"Great! If he's anything like what you're saying, he sounds like fun to spend time with."

"Just to warn you, I think we'll be spending an inordinate amount of time working. But it'll be a short sprint, really, just a couple of weeks I think. But just the same, I really need all the time I can make use of during that period. Not that you've ever been jealous of my work, but I just wanted to warn you in advance."

"Alright. And thanks for letting me know. Is there anything you want me to do? Try to stay out of the apartment in the evening or something? I can spend some time with Michele a couple of nights; she's after me for a girls' night out…"

"Ah, I don't know yet. Can we play it by ear at first? I don't know when exactly this will happen, for how long it will be, or what it's like to work with him."

"Sure, I understand. Oh, I'm so proud of you!" She leaned in and wrapped her arms around him, hugging him awkwardly but enthusiastically on the sofa.

Reuben stretched his back a bit, hugging her back. "Thank you…I'm really happy about it." He smiled, just enjoying the moment.

"And you know how I love it when you talk nerdy to me, but you knew that," she added. She looked into his eyes, smiling demurely at him…

Wednesday, October 10th, 9:25 AM, 2001

"Good news," said Bob on the cell phone. Reuben was zipping along the George Washington Parkway, headed to the office in Tyson's Corner. "Pam just called, and it looks like the meeting will be later this week."

"Great! Do you need anything from me right now?"

"No, not yet. Right now it's just…it's only about money, and the bullshit of how to make the contract work out. They don't have time to bid it out, and there are some things you have to do in the government when you just give someone business like that, without putting it out for bidding. So we, I mean Pam and myself and Brenda from contracts and whoever else, will get with them to sort it out and see how to make it work."

"Alright. I'm about ten minutes out now. I'll do what I can to figure out what I'll need exactly in terms of the lab. At least then you'll know one aspect of the cost, if we need to buy anything."

"Good, do that. I'll see you when you get in."

Reuben closed the phone and put it back on his belt, downshifting to get onto Route 123. *This can work,* he thought. *I can feel it, it's really going to happen.* His mind methodically played out variables as he moved with the traffic past the entrance to the Central Intelligence Agency, noticing just how many cars turned off to enter the secured facility. He hated to wait to get information before trying to solve a problem; it was more interesting to play it like chess, and treat the information that came later as moved by an opponent, narrowing the options as they took him down one set of branches on the tree in his mind. *Three possibilities. Server to server, client to server only, and a combination of both.* He didn't know what the software was yet, so he didn't know what it ran on. That would come after everyone started signing Non-Disclosure Agreements, or NDAs as they were known.

As traffic started backing up, he slipped onto the Dulles Toll Road, rocketing along at 60 for about a mile, slowing as he approached the tollbooth. He flipped a quarter into the basket and sped off. Five minutes later he was pulling his laptop out of his car and walking into the building.

He was out of the elevator before the doors were half open, spinning abruptly to barely avoid crashing into some older fellow who probably had something to do with some large boring federal contract. He waved his ID at the plate next to the door and went in, stepping briskly to his cubicle and yanking out the laptop before he even put anything down.

Plugging in, he booted up, and started pulling his shoulder bag and laptop case off of his shoulders, stripping off the jacket and hanging it up. He took a moment to log in, and let everything start up as he got organized. He was hungry for some more work; it felt like being a dog on a

short chain, just barking and pulling and yanking back and forth. Now that something was happening, he felt himself barking louder inside, all the more eager for seeing something almost within reach.

He started up Outlook and let it start pulling down mail as he walked down the hallway to Bob's office. Leaning his head into the doorway, he saw Bob was on the phone, waved to him and let him be. Turning around, he went to go get some coffee and sit back down at his desk. Nothing too significant in his mail, just some continuations of discussions on various mailing lists, and a little bit of administrative stuff. He started going through his morning reading, opening up Slashdot first.

While many people read a newspaper, Reuben was like many geeks in that he read websites instead. He had his routine set of sites: Slashdot, the Internet Storm Center, Washingtonpost.com, and occasionally SatireWire or The Onion for some comic relief.

Bob came by. "Hey, I just got off the phone with Brenda. The money might be a problem; apparently the contract vehicle they use pays next to nothing. She's seeing if we can get onto another vehicle. The company that's rolling out the product might be able to sub something to us, and we can get on that way; they're seeing about it now."

Reuben was deeply glad not to be a contracts administrator. "Whatever you say. Makes you wonder why they can't just pay what's fair, doesn't it? You'd think the government could merely use its bargaining power to keep from getting screwed. It seems stupid that they can't even pay the right amount easily if they want to."

Bob laughed. "Oh, my friend, you have no idea." He loved how Reuben was so utterly un-federal, even to the point of naïveté about how things worked. Bob had been in the DEA his entire professional life up to a short while ago, so he knew it well and thought of such things as they were. Reuben, on the other hand, was idealistic and thought of things as they should have been. "You should see what it's like to get office supplies at some places, someday."

Reuben laughed. "No thanks! I'll stay here in the private sector, nice and comfy and well-supported. Which reminds me, I think I know how many systems we'll need for the lab. It depends a little bit on what configurations we'll have to test, but the number only really differs by one either

way, from that. The thing that really matters is what operating systems will be involved; can you ask them which ones they're planning on using? I figure they can tell us that without us having to sign an NDA. And do we have any servers lying around we can use for this?"

Bob thought for a second. "I'll ask…can't hurt to see. And I don't know what we've got lying around, but we may have to come up with something to set up the lab. I don't get the impression there's a lot we can call upon these days. And there's no way we can charge the client for buying machines."

Reuben nodded. "I've got an idea then. I think we can rent some systems, and it shouldn't cost us too much. We won't need them for long, and maybe we can even include that in the pricing."

"Good thinking. Call and get some idea of the cost. Figure on two weeks."

"Will do. I'll make sure the systems are clean before we give them back too. Odds are the company re-images them each time, so they won't mind if I do a little formatting."

"Ah, that's a good point. We need to be careful about who has access to what we find. Let me see about finding a room you can use for the lab. We've probably got something on the sixth floor. Do you need anything special?"

"No, just a phone, a working network drop, and power outlets. Oh, yeah, and one more thing. We need guns…lots of them."

Bob laughed in shock, "What??"

"Oh, sorry. Matrix quote." He smiled widely.

Bob chuckled, getting the joke…or at least getting that it was a joke…at that point. "Gotcha."

"One more thing. I've started looking ahead to plan how we'll approach this. Should I be logging my time spent on that? Can we retro-bill that kind of thing?"

"I'll ask. My feeling is no, so don't do all the work in advance. But keep track, just in case, and don't be afraid to be prepared. Besides, if you've got nothing else going on at that moment, it's not costing us anything."

"Good point. Okay. I'll call about rentals now."

Bob stepped away, and Reuben started looking on the web for computer rental options in the area.

Wednesday, October 10th, 8:21 PM, 2001

Reuben sat in Tryst, a coffee lounge in his neighborhood, alternating between attention to his coffee and his laptop. Larger than many restaurants in the Adams Morgan section of Washington, Tryst was an expansive space of chairs, lounges, and sofas, with a full bar, a small kitchen and the best coffee in the city, hands down. It was also extremely laptop-friendly, providing numerous power outlets and even analog phone jacks for local dialup connections.

It was where Reuben often did some of his best work when it came to the more mundane, writing-oriented parts of his job. It was at Tryst that he wrote scopes of work, deliverables for untold numbers of clients, and an entire marketing plan, not to mention the occasional small article to be published in one place or another.

In the dim light of the place, his face glowed white with the light of the document on the screen. Reuben was documenting the attack plan, as he could guess at it. He figured that it might change a bit, but then it could be changed; better to have something to start with anyway, since MadFast wouldn't be there long. Too much time spent doing things like this could cause a problem, since the whole thing would be a failure if they didn't cover enough ground in what time they had to work.

First they'd be looking over the documentation, approaching the whole thing blind. Learning the architecture of the system was probably the most important thing they'd need to know, and in the subtleties of suggested configurations one could find things that go wrong when a different setup was tried.

Next, obviously, would be installing the software. Looking for ways to screw up and leave things insecure was key; they'd go about it as blindly and in as much of a hurry as they could, then they'd go back and see if they missed anything. If there was any significant difference between the correct and actual configuration, they'd need to test things with the weaker

config before hardening it and having another go, in addition to documenting the mistakes that were easily made.

Then, they'd start using the software, doing network captures and trying to learn how to read the packets. Buffer overflows were definitely something that they'd try, and while Reuben was building packets to test data fields, MadFast could try entropy analysis on the encrypted data.

After that, they'd start assaulting the remote client, assuming that would be part of the intended configuration. They'd run RegMon and FileMon while starting up and using the client, and sift through the deluge of resulting data to see which registry keys and files were involved in it. File permissions on the client would be important; they'd also look for things like private keys and authentication information on the system, and settings that might be security-related. One possible goal would be to dumb-down the encryption; many applications that used encryption supported multiple versions, and could be forced to use weaker forms by an attacker. And they'd see if they could buffer-overflow the client as well, in case it opened up any weaknesses on the client machine.

Beyond that, it got rather fuzzy. Half of what they did would probably be determined by what they learned at some earlier step of the process; a whole set of tests could come to light based on the configuration, and other tests could be eliminated by the design of the software or how it would be used. But it helped a lot to think and plan ahead; at least now Reuben felt like there was a solid game plan, and that he'd save some time when the test happened.

Reuben realized he was about finished, and put down the coffee. He flagged down Kellee, one of his favorite people at Tryst, and ordered a beer. He had a feeling he'd be here a lot more over the next two or three days.

Friday, October 12th, 11:52 AM, 2001

"We've got a problem," Bob said.

Reuben looked up and over from his desk, turning around to face him. "Uh oh. What is it? The cost?"

"No…they're letting Dan go."

Reuben carefully considered this for a moment. "Well, hmm. I think we can still do this without him. I was truthfully bringing him in so that we could try and throw a bit more manpower at it, and set up more of a network, but the parts that really matter are at the ends. And as far as any infrastructure things go, I can handle that myself too. Remember, I was a networking guy before I went into security full-bore."

"Are you sure? We can do this with two people?"

"Yeah, we can. I know, you're worried that I'm overextending us because I want to do the work so bad. And yes, I really want it, I want it so bad I can taste it. But I'm not stupid, and I'm not going to get us into a nightmare situation. We really can do this. Wait until you meet Frank; you'll see what I mean. Remember how you once said you wished you had three or four of me?"

"You're saying he's like you."

"Yeah, except he's actually more like more than one of me. Just trust me on this."

"Okay. But just so you know, it's all in your hands now."

"That's how I've been looking at it all along. I won't let you down. How's everything else looking? Any news?"

"Yeah, we can get on with the other company, so that's all fixed. We'll get our rates covered, and can make some money on the work. I got a room for you guys, and there aren't any computers we can use…that's the bad news. The good news is that we can bill the client for the rental costs."

"Oh, good! So we've got our money for work and a lab. How about bringing Frank down?"

"Yeah, we got that approved to, but there's a catch."

"Uh oh. What's that?"

"He's got to clear a background check."

"Oh, that's no surprise. That's fine. Don't tell me you're still worried about that?"

"Yeah, I am. I'm just concerned. I mean, it's down to you and him, and without him we can't do it. So what if there's some unforeseen thing? I'm not saying he's lying to you, but how does he know what might be significant? If he's been charged with something, but then the charges were

dropped," Bob added, clearly worried that MadFast might have dabbled on the wrong side of the law, "then that's enough to make them cut him from the picture."

"Trust me, he doesn't have to know what is and isn't significant. There's nothing, there really is nothing out there. And nothing can't be significant. I mean, really, nothing. I'm sure of it."

"Are you sure? Remember where you met this guy."

"Yeah, but I was there too, and you know I'm not a bad guy. I just know some such people so that I'll know what's going on. Frank's fine, no problems, I'm sure of it. And he doesn't even look like a bad guy." Reuben smiled. "Just relax, he's not something we need to worry about. He's fine, he's going to be great. Do you want to talk to him on the phone? That way you can get a feel for what he's like, and I guarantee you'll feel a hundred percent better after."

"That's a good idea. Yeah, let's all talk about the project and make sure we're on the same page."

"That works. I need to call him anyway and see where he is at his end, on getting time off from work to do this. I'll set it up so we can call him from your office, and I'll introduce you. When's good for you?"

"He's in Seattle, you said? That's three hours back. How about three-thirty."

"Okay, I'll contact him and set it up."

They nodded to each other, and Bob went back to his office.

Reuben turned back around to his computer and reconsidered everything. He was sure that he could handle this, even with a third of the team eliminated. Well, he'd included Dan mostly to help Dan out, he realized; they were cutting people away here and there, and being allocated to something was helpful for survival. Too bad it didn't pay off in his case, but Reuben was sure that Dan would be able to find other work fast enough. He was plenty skilled and experienced, and he knew lots of people who could help him look for a new job. He picked up the phone and called MadFast, figuring he was probably in the office about now anyway. He got MadFast's voicemail.

"Hey, it's Reuben. I want to set up a phone conversation between you, Bob and myself. I was thinking three-thirty our time, so half past noon

yours. E-mail or call me back and let me know. Talk to you soon." He hung up.

He pushed away from the desk and closed his eyes a moment, thinking. He went down the list of all the aspects of the project, and everything that needed to be done, checking to make sure he had everything covered to the best of his ability. *So far, so good, despite all the surprises. I guess surprises are inevitable, and it's good luck that none of them have torpedoed this yet.*

Friday, October 12th, 3:33 PM, 2001

"Alright, now I'm finally going to be able to get the two of you to talk to each other. Bob, meet Frank. Frank, Bob." Reuben spoke into the speaker-phone, happy that this was finally happening. Things were probably going to start happening fast now, so for Bob and Frank to be able to talk directly would be a plus, and it would keep Reuben out of the middle when it came to things like compensation and organizational matters.

Frank responded first. "It's good to meet you. Alright, where are we now?"

"I'll let Bob give you the update on what's going on at this point. I think we're pretty far along, but I'm not the real authority on that."

Bob piped in. "Alright, here's where we stand. We've got the authorization to do the project, and to bring you in. We'll be setting up a lab, using rental computers, in a room downstairs. One thing, though. I need to put in for a background check on you, just to make sure there's no big problems or anything like that."

"That's fine, Reuben told me about that already. What do you need, my social security number and full name?"

"Yes. And your current address."

"Not a problem. You want them now, or in an e-mail?"

"Why don't you give them to me now, so that I can get it taken care of. Just in case there are any problems, it's better to know sooner so we can do something about it."

As MadFast gave his information over the phone, Reuben relaxed. He was a little worried that there'd be some offense taken at Bob's concern, but it seemed to be going alright. Reuben had always understood when

people were cautious, so maybe MadFast was the same way too. Whatever the reason, all seemed to be going fine.

Bob spoke up. "Okay, with that out of the way, why don't the two of you let me know how you're planning to go about doing this. I mean, I might get asked, and I don't want to be caught looking like I don't have an answer."

Reuben nodded. "I've been working up an attack plan. I need to e-mail that to you, Frank. It's not entirely done, but it's about as good as I can get it. I need you to tell me if I missed anything in it. I'm betting there are things you can do that I can't, too."

"Right on."

"Here's the gist of it. We set up the lab first, and then we go over all the documentation. I think there are things in there that we can find, clues as to what to look at. Then we set it up as haphazardly as we can. No point in setting this up like a kick-ass security guru, since that's not who's going to be installing that all the time. If it's easy to screw it up and make it unsafe, I want to find out."

"Right, right. Good idea."

"Then, we play around with it a bit, see if we can get an encrypted connection, that sort of thing, and we sniff the packets."

Bob looked confused. "Sniff?"

"Yeah. It's like eavesdropping on the network traffic, and we'll record what the systems say to each other, and look at the raw data."

"You can read that?"

"Depends, but usually yes. Some of it, at least. And that's the next thing I want to do. I want to see if I can figure out how the packets are built, what packets do what and how they are structured. If there's a buffer overflow in there somewhere, I want to find it, and that means we need to know the anatomy of the traffic."

Bob was impressed. "Wow. You guys scare me." He smiled.

Reuben continued. "After that, if they'll be using a remote client, I want to go after that. There's lots of fun I can think of there. Frank, how are you at reverse-engineering software?"

"I'm not bad. What are you thinking?"

"I'm thinking that this software might store credentials or whatnot in not-so-safe places on the local machine of the client. And I'd like to get at them, and do what we can with the information."

"Right on! I think we can do that." MadFast was audibly smiling at the other end.

"And aside from that, there's a lot of little things, but that's basically it."

"Sounds good to me," MadFast piped in.

"Alright, I think I have what I need," Bob answered. "Anything else you guys need?"

"I need to know when and for how long," MadFast answered.

"Yeah, me too. We need dates."

"Okay, I think we'll have those soon enough. Reuben will give me your e-mail address, Frank, so I can contact you when I have that."

"Right on."

"And I'll e-mail you the outline I made of the attack plan. There's more detail of attacks in there, things crypto-related."

"Okay," MadFast concurred.

Reuben finished up the call as he pretty much started it. "I guess that does it. One of us will be calling you soon, Frank. Be well."

"Talk to you guys later." And he was off the phone.

Reuben smiled at Bob. "What did you think?"

"He sounds fine, you're right. I got a good feeling about him."

"Exactly what I thought would happen. Wait until you meet him."

"Okay. I trust you now."

Chapter 4

The Arrival of MadFast

Baltimore, MD: Thursday, October 25th, 8:40 PM, 2001

Reuben waited patiently at the exit in Baltimore Washington International airport, watching for MadFast to emerge. Since September 11th, it was no longer so simple to pick people up. Everyone from all the different gates seemed to come out together. It was tough to search through such a crowd for one person he'd only seen once before in his life. But soon enough, the face he was looking for emerged, and saw him as well.

"Hey hey! Good to see you."

"Same here! How was the flight?"

"Security was a bitch! But I don't really mind. At least they're serious now. Had to lose my razor though. That seems a bit hardcore."

"Really? What kind of razor was it?"

"Just a normal disposable. I don't really know what someone could do with it. Even if they took the blade out, then what? It's not exactly strong or pointy."

"Beats me. But you know how it is. After something happens, everything changes too much, and gets more sensible later. And nobody around here knows what to do; they're all terrified. National Airport is still only flying certain flights now. I used to fly out of there all the time, and they may not reopen it now. And if you think the security people are paranoid, you ain't seen nothing yet. All sorts of people are spooked like crazy right now. If it's not the bombings, it's the anthrax scare. I talked to a guy the other day, he was going downtown, and was afraid of catching anthrax from someone. I had to point out to him that basically nobody had caught it, statistically speaking, and that it can't be transmitted from person to person like that. It's the damned news; they're pumping every bit of this for all its worth, for the ratings. They're scaring the hell out of the public by selectively reporting facts, and I hate it. Right now people need to know what is and isn't a real threat, not this whoring of fear that everyone seems to be into." Reuben had strong feelings about the subject, obviously.

"Wow. Tell me how you really feel, huh? But yeah, you're right. Well, let's go. This is creeping me out a bit."

They walked away and downstairs, to the baggage claim. "One good thing," MadFast noted. "Nobody's flying right now, so it's more comfortable. I hope my bags are OK though." Sure enough, the baggage claim area was relatively empty.

"Wow. It seemed like so many people at the exit to the terminal," Reuben noted. "I wonder what that will look like when people start flying again!"

"Yeah, no kidding. Ah, this looks like it." They walked up to a baggage carousel, and waited for bags to start coming out. Oddly enough, it didn't take long. MadFast grabbed his two bags off the conveyor.

"Here, let me get one," Reuben offered. He grabbed a duffel, and the pair walked out, Reuben leading. "I'm not parked too far away; there aren't too many cars in the parking lot either. I guess I should have known, eh?"

They stepped outside into the cooling fall air, and across to the parking garage. Going up a set of stairs, they went over to Reuben's black Honda. Disarming the alarm, Reuben opened up the back hatch and put the duffel in as MadFast followed suit before they both sat in the car.

As Reuben pulled out of the airport complex and onto the highway, he asked, "So, what kind of food are you up for? I was thinking tonight we'd eat out, whatever you want, my treat. I'm just so glad you could come, and I'm really looking forward to working together."

"Are you sure? It's my pleasure, you don't have to do that." MadFast smiled back.

"Yeah, I'm sure. Don't worry, I get paid well, but I'm not breaking the bank. And we'll be working hard the next couple of weeks, we need to have fun too."

"Right on. Well, how about something simple tonight, and a rain check? I'm a bit worn out from the flight."

"Ah, that's a good idea. We need to get you checked in too, I just realized."

"Right."

"Okay, simple it is. There's this great place for Chinese delivery, and we can all chill and watch TV at my place, and maybe talk some shop. Oh, and you can meet Briana."

"Right on."

Reuben pulled out his cell phone, and scrolled through phone numbers to find the one for home, and dialed. "Bri? It's Reuben. We're going to have dinner there, City Lights I was thinking. Yeah, he's here, safe and sound, and we're headed to the Inn to check him in first. So do me a favor, and straighten up a bit? Thanks. Love you too." He closed the phone. "All set," he reported, as he turned off onto 95 south toward Washington.

"Heh. You drive like I do," MadFast commented.

Reuben smiled. "How so?"

"Oh, pretty fast. And aggressive without being a dick about it. It's clear where you're going and what you're planning to do in traffic. Oh, and did I say you drive fast?" He smirked.

Reuben laughed a bit. "Well, traffic here fairly hauls. They've talked about making the limit 65 for this stretch, and they damned well should." He looked down at the speedometer, and noted that they, and everyone else around them, were going a solid 85 miles an hour. He had no problem with it; even though his car was used and not much to look at, the previous owner had done some suspension modifications to it that improved its handling quite a bit, although at the expense of comfort. The engine modifications were another matter, though; the car sounded faster than it really was. Still, it was nice how the car emanated a nice deep growl when under acceleration; it was extremely small, and sometimes other cars didn't see it as easily as they heard it.

In no time they were pulling onto the beltway, and Reuben was deciding which of several ways to go into the city. He chose the longer but more interesting route of the GW Parkway, which afforded MadFast a view of the lights in Georgetown across the Potomac River.

"Wow. Here it's all woods, and right there, the city."

"Yep. DC is a beautiful place to live. You'll see over the next couple of weeks. You know, it was designed to awe and intimidate visitors from other countries?"

"No way!"

"Yeah. It works too, I bet. I know that the first year I lived here, I'd just walk around and look at things. And I'd already been coming here every year for a long time before that, so it wasn't new to me. The White House pales in comparison to Versailles, but this city took a lot less time to build than Europe. A few other things you'll notice; there are no really tall buildings in DC. That's because there's an ordinance that states that nothing built can be taller than…I think it's the statue on the Capitol Building that is the height limit. Of course, the Washington Monument is taller, I think, but I think that's an exception for being a monument rather than a building."

MadFast nodded in acknowledgement. "Right on."

Reuben turned off onto the exit for the Key Bridge, braking as it curved sharply upwards. Turning onto the bridge, he shot across, thankful for the nearly-nonexistent traffic. "You'll like this…hang on." Braking abruptly, he shot to the right through a surprise turnoff on the bridge. Gaining acceleration down the ramp, he got onto the Whitehurst Freeway, a short elevated section of highway running through the bottom of Georgetown.

"What's that to the right?" MadFast asked, pointing at a brilliantly-lit rectangular white structure.

"That's the Kennedy Center. Arts and the like."

"You ever go?"

"Nope. Sign of a true Washingtonian, there are majestic and amazing things here I haven't taken advantage of. You'll see a lot of that too; the people who grow up here never see the monuments or museums except when they have visiting friends who want to see them. Funny, huh? Oh yeah, there's another thing you'll notice; nobody's from here. We all came here for a job, or to go to college, and stay. But it's one of the things that powers the city. We're dependent upon brainpower; there is no industrial base whatsoever in the DC area, so we need to constantly populate with smart people."

MadFast laughed, "What, you trying to recruit me?"

Reuben smiled at him for a moment before putting his eyes back to the road, which curved abruptly as the Freeway ended. "It wouldn't be a bad thing, that's for sure. But mostly I think I just love living here myself."

"I can see that."

"Okay, here's the part of the trip home that I love the most," Reuben said as he turned onto Rock Creek Parkway. "I can't believe there's road like this in the middle of a major city!" He gave the little car gas and shot down the relatively straight road, between a creek on the right side and a lush foliage-covered hill on the left. In an instant, there were no buildings, no stoplights, just like a trip in the country. Except that they were doing sixty.

"Amazing. You drive this often?"

"Every day." The road suddenly became more curvy, and the forces of turning slewed from side to side as Reuben worked the steering and

throttle to maintain a solid grip. If MadFast liked driving hard, then Reuben wanted to give him the full tour.

"Did you ever see that old Steve McQueen movie, 'Bullitt'?" MadFast inquired matter-of-factly.

"No, but I've heard of it. Big black car, movie from the '70s, right?"

"Yeah. You drive like that. You should see it, it's great."

"Uh, is that a good thing?" Reuben came off the gas a bit, feeling a bit embarrassed that perhaps he was showing off too much.

"Oh, yes! It's definitely a good thing."

Reuben relaxed. "Oh, good! Yeah, my driving scares some people. But I never drive beyond the ability of the car, or my ability to react. I can do this road faster, I think, except that if something was just around the corner, I wouldn't see it in time. I totally fail to understand motorcyclists who go well into triple-digits; there's no way anyone can see far enough ahead into the future to avoid an accident at that speed."

"Uh, yeah. Besides being out in the open like that! No seatbelt, no metal around you, no airbag…"

The lush greenery on either side of the road whipped past the car as they talked. "The best thing about this road is that it takes five minutes to cover it…but if we went through the city any other way, it'd have taken three or four times as long." The road curved more sharply still, and Reuben downshifted, getting to the right lane. "Almost there."

Under a tunnel they passed, and took the exit for the National Zoo, stopping at the light. "Now we're only about three blocks from my place, and about the same to where you'll be staying."

"Right on."

Reuben turned at a few intersections, and finally turned right onto Lanier Place, parking at the first available spot. They got out, and started pulling luggage out of the back. "Parking here can be a bit tight at night, so I'll just leave the car here. It's only a block that way," he pointed behind himself with his thumb, "to my place, so this is fine. The Inn is just a few doors up on the left."

Reuben helped carry the luggage up to the Adams Inn and to the door. "The office isn't open at this point, but I made an arrangement," he said as he reached into the mailbox. "Aha, here it is." He pulled out an

envelope with his name on it, and opened it, revealing a pair of keys. "Not the best security, but what the hell. One of these opens their front door, and the other opens your room. You'll notice the room number on the keychain; don't lose that key, obviously."

"These are not paranoid innkeepers, are they?"

"Yeah, apparently not. But it's comfortable, and they're really nice. When I lived in the suburbs, I used to come stay here every now and then when I wanted to spend a weekend in the city. We're two blocks from a whole ton of nightlife."

MadFast looked back and forth along the quiet street. "How many blocks?"

"Yeah, quiet here, isn't it? You'll see; this is very cool." He opened the front door and went inside, holding it open for MadFast. "Let's get you set up in the room and then get some food delivered at my place."

Washington, DC: Thursday, October 25th, 10:57 PM

The carnage of the meal was spread across the coffee table; various containers of Chinese food, the bags that carried them, and the usual accouterments of soy sauce, duck sauce, mustard and chopsticks. Briana, MadFast and Reuben hungrily tore into their plates of food, temporarily suspending serious conversation; they were starving. Putting down his food, Reuben got up from the sofa and stepped over Briana's legs. "I'm getting a beer. You want one, MadFast?"

"Sure, whatever you got."

"More water for you, Briana?" She drank water usually. A lot of it.

"Yes, thanks."

Reuben nodded and walked around the corner into the kitchen, grabbing a couple of Bass Ales and the pitcher of filtered water before returning. "Bass okay for you, man?" asked Reuben as he offered the open bottle.

MadFast looked up. "Oh, wow, right on. Yeah, it's great." He took it, putting his plate down and taking a swig from the bottle. "Mmm, good stuff."

"There's more in the fridge, help yourself. I'm assuming that you're like me, and you don't leave work behind when you leave the office. If that's the case, we're going to be working a lot here in the next couple of weeks, so *mi casa es su casa*, if I said that correctly. My Spanish sucks; I studied French in school."

"Right on. Say, do you have Unreal Tournament on your computer?"

"Sure do…you play, I take it?"

"Yeah, online."

"Ah, I haven't done much of that. I'd like to watch; I never got the hang of competing against human opponents. I can take the bots on in Godlike mode though, if I'm having a good day."

"I'll show you some tricks," smiled MadFast wickedly as he put the beer down and prepared to attack his food again. "Not to brag, but I'm a badass."

Reuben grinned back. "Cool, I'd love to learn." He sat back down and resumed devouring the rest of his food.

After dinner, MadFast and Reuben started comparing notes. "Okay, so you think the roadmap for this test works pretty well?"

"Yeah, as long as we don't stick to it too tightly. We may see things we never thought of, and we definitely want to go after them."

"Cool, that's what I had in mind too. I just figured that it'd be good to have a path to follow until times like that. Good then, I think we're set. Now, what are some of the things you want to try? Can we reverse-engineer this?" Reuben would love to take the software apart, but had no expertise in the matter.

"Yeah, I think so, but we gotta wait until we find something in particular to go after, like a function. A real reverse-engineering job like this takes a long time, longer than we've got."

"You're the man, I'll follow your lead on it. Tell me, do you think we'll find anything? Just your gut opinion."

"I don't know. Most software has flaws, but it's hard when it comes to VPNs and firewalls and things like that, or so everyone says."

"Yeah, that's what I was thinking too. I've only seen two kinds of firewalls, really. Rock solid secure ones and ones that are a joke. There hasn't been too much of a middle ground."

"Yep, me too. Who knows, maybe we'll get lucky, and it'll be like swiss cheese."

"Maybe!" Reuben didn't know how he'd write the deliverable if he found nothing. Ironically, that's probably what the client hoped to hear, but it would make for a lousy report. "Alright, you should get some rest; we've got the big meeting tomorrow. I haven't met any of these guys, so I don't know what to expect. Oh, and the systems for the lab should be in tomorrow morning, so we can set the lab up."

"What time's the meeting?"

"Not until two in the afternoon. Oh, and I should let you know, Bob's really cool. He knows we'll be working pretty much all the time, so it's okay if we get in late. Sleep is more important than punching the clock today, at least."

"Ah good. So, I'll come over here when I'm up and ready?"

"Sure. And I'll have good coffee made."

"Right on."

Washington, DC: Friday, October 26th, 2:16 PM

"Okay, so now that's out of the way, let's tell you guys what you're going to be doing for the next two weeks!" Vince said. Vince was the businesslike but quite amenable point of contact now, as Pam had gone away in some fashion. Sitting in his hands were the NDAs signed by Bob, MadFast and Reuben, basically stating that they wouldn't tell anyone anything about their work or findings unless they got permission from the Department of Justice first. The contractual details had been worked out, the price and costs agreed upon, and now it was up to MadFast and Reuben.

"We are at the start of a significant rollout of a software-based VPN product by the ZFon company. Are either of you familiar with their software?"

MadFast and Reuben looked at each other quizzically. Reuben spoke first. "No, I'm not, I don't think either of us is."

Vince didn't seem to mind. "No matter, you'll be familiar with it soon enough. As you may know, there's a new requirement that things like this be checked by an outside party prior to implementation, and this is why we need you. Your job will be to go over the software and make sure that it's secure."

Reuben had a question. "What kind of a configuration will you be using? Will it just be between networks, or will remote users have it installed on laptops or home computers?"

"Ah, excellent question. It will be used both as a gateway for net-to-net encryption and tunneling, and for remote users. And we do want you to go over both of them fully."

Reuben smiled. This is what he was hoping for; there'd be more opportunities to look for problems this way. He wanted to be thorough.

Vince continued, "We'll contact the vendor after this meeting, and they'll be providing you with the software. In fact, I wouldn't be surprised if they brought it by this afternoon. ZFon is based in Germantown, so they're local to the DC area. Contact them directly if you need them for anything. They've been asked to give their full cooperation."

Reuben responded, "That's good, we might need that. I have another question, though. If we find any vulnerabilities, what option will we have to disclose them, after the vendor addresses them of course."

"I don't think that'll be a problem. We understand completely that you'd like to take credit for anything you find, and the value of that to you. As long as you let the vendor respond, and give us a chance to patch, we won't have any issue with that. I'm guessing that you expect to find some vulnerabilities?"

"Well, that's what we're hoping, in truth. Nothing against you or the vendor, but to be honest, most software is vulnerable. And yes, it'd be better for our resumes if we found problems, rather than if none existed. The standards for disclosure you mentioned are perfectly reasonable, I think that'll be just fine. I wouldn't want to do it differently myself, really. There's no point in causing insecurity for people here, the whole point is to do the opposite. But what if the vendor doesn't respond to the issues found?"

"Well, in that case they'll lose a lot of money. We can't deploy without your blessing, gentlemen, and if they don't fix anything you find, they won't be able to keep the money they've been paid. The sale is contingent upon adherence to necessary standards, and your examination is one of those standards. So I think they'll be very responsive."

Reuben and MadFast smiled together at this. "Nice," MadFast interjected. He seemed as hungry as Reuben was to make an impact with this work. And everyone knew how many vendors hated to own up to flaws in their software, much less fix them in any timely fashion. Having this sort of leverage was a welcome twist to the situation.

Vince continued, "Okay, with that out of the way, let's take care of some minor annoying details. We're looking for a deliverable with the following parts…"

Forty-five minutes later, Vince walked out of the room together with Bob, Reuben and MadFast to see them out, reminding them to turn their visitor passes back over to security before leaving. "Gentlemen, I'm looking forward to seeing what you will do for us. I have a good feeling about this. There's one thing I want to tell you before you go. I don't know if I'm supposed to let you know this or not, but the NSA has already looked the ZFon software over and given its blessing. So I'm curious to see if you find anything. I know I'll be impressed if you do."

Reuben and MadFast looked at each other, not sure what to make of this bit of information. Neither knew exactly how talented the NSA was or wasn't at such things, but all indications they'd seen showed that NSA did know what they were doing. "Ah, I didn't know that," Reuben volunteered, not knowing what else to say. "Well, we'll probably be using a different methodology, so we'll see what happens. Did the NSA do source code review?"

"No, I don't believe they did. That would be for a system that's certified to a much higher standard than anything that would be connected to the Internet, so I doubt they did it. So it's entirely possible that they missed something."

"Well, it helps to know that." Reuben felt a bit of relief. Whatever he did or didn't know about the NSA, he doubted they followed unorthodox methods like he and MadFast would. He doubted there was much origi-

nality in the NSA playbook for something like this. "Maybe we can really show off, eh?" He grinned to Vince and Bob.

"Have a good afternoon, gentlemen, and I'll be looking forward to hearing from you shortly." Vince went back into the building.

Bob had only spoken up in the meeting to deal with administrative matters and fend off potential problems, leaving Reuben and MadFast to do most of the talking. Now he opened up to the two. "This is gonna be great, if you two can pull it off. I mean, I don't know, but from what I've read, everything has vulnerabilities in it, right? You just have to find them?"

MadFast looked like he wanted to answer this one. "Oh God yes, yeah. I mean, there are a *few* programs out there that are secure, but for the most part there's problems lurking in everything."

"So all you have to do is find it. Now, how hard is that?" he asked genuinely.

"Well, not everyone can do it. But I think we will."

Reuben didn't know why, but he felt the same. There was no logical basis for it, no factual foundation, but he just knew that the two of them would rock this project.

It wasn't long before they were back in the office, and sure enough, the vendor had called Reuben's cell phone to ask if they could drop off the software that afternoon.

Washington, DC: Friday, October 26th, 9:45 PM

Back at Reuben's place, Reuben and MadFast were going over the documentation that came with the software, gladly examining its feature set. "My God, they came up with a way around key escrow. It's clever, but incredibly stupid. Get this; they designed it specifically so you can re-create the keys to any past session." Reuben was beyond belief.

MadFast looked up from the computer. They'd been taking turns reading and playing games, mixing it up to make the work a bit more enjoyable. It was going to be a late night, they both knew, and there was no sense in not having fun during it. "Okay, I'm getting offline, I've got to see this. I don't even care that I'm the second-to-last man standing and

that I'll lose by forfeit." He disconnected the game session of Unreal Tournament and got up from the desk.

Reuben handed over the documentation. "It's all here, check it out."

MadFast read it over. "I'll be damned. Look at this…they did it so that law enforcement could come back to the people running the VPN with a court order and a network capture, and ask for the key. But the way they wrote it, you could replace 'administrator' with 'hacker' and it sounds like a kind of road map of how to compromise the traffic."

Reuben looked over his shoulder at the text again. "Shit, you're right! I guess that's something to go on our list, isn't it?" He grinned wickedly. They were having fun; ever since they got their hands on the software and documentation, the path ahead seemed quite clear. Things were no longer theoretical, and they could get their teeth into the work. Best of all, a very clear attack pattern was forming for them. Reuben felt much better for having done his original plan; it turned out to be quite helpful, as they modified it but nonetheless stuck to the basic roadmap it offered.

"That's going to require a reverse-engineering job, from the sounds of it. They have two-factor authentication protecting the software to do that," Reuben considered. "Unless we get really lucky and can break the authentication outright, you'll have to step through the software and find the functions that do that job."

"Yeah, that's what I was thinking, but hey, it's worth it. If it works like I think it works, there's no safety for the session if you can do that. You could generate the session key so fast that you'd be decrypting traffic before the session was over, and you'd be able to decrypt all of it."

"Good point. If we can do that, right there it's a game-over situation. Hell, even at this stage I'd say it's a safe bet, as we know what we'd have to do already. Doing it is just a matter of time. We should put it off, I think," Reuben added, "since we have so many other things to try first. Can you try just tracing DLL calls and maybe we'll get lucky and find all the functions in one DLL off by itself?"

"Yeah, good idea. And you're right, we won't get much else covered if we just go after that. Okay, so what's next?"

"We install it on Monday, and have at it. And see what else we can think of this weekend besides what we've done so far. But as far as I'm

concerned, we're off the clock now, so we can just chill. Want another beer? I've got some Trappist-style ale."

"What's that?"

Reuben smiled; he loved beer, good beer, and loved introducing others to it. "Okay, some background. In Europe, there are a handful of monasteries, mostly in Belgium I think, that make beer. Trappist monks, you see, produce some kind of product, so that the monastery can survive. Well, the beer that these monasteries make is particularly good, and tends to have a unique kind of character. Now some breweries are trying to copy the style, and some do a pretty decent job. It requires a careful balance of malt and hops like any good beer, but it also requires yeast with a particular character. Here, you'll see what I mean." He went into the kitchen, and returned a minute later with two glasses of golden beer, each with a substantial head. "Here you go."

MadFast took the beer, looking at it. "Looks good. How do you know so much about beer?"

"I homebrew…used to, that is. I got out of the habit for a while. I need to start again though, I miss it."

"Right on. How hard is it?"

"Not hard at all. It's like cooking, really. At first, you start out just following directions and use a kit that you buy. But then, as you get more into it, you read about how to improve your beer, and you learn a lot about beer in general. One thing though, after you do homebrewing, if you're any good at it at all, you won't be able to drink bad beer ever again. It's like losing your innocence, only in a good way."

MadFast took a sip of the beer. "Wow, it's…it's kind of sweet, almost."

"Yeah, that's the effect of the yeast. But it's not heavy, or too sweet; that's the hops and the alcohol. Speaking of which, this beer is a lot stronger than most. It's got quite a kick."

"Right on. So I guess we're done working for the night, huh?"

"Cheers!" The glasses clinked together.

Washington, DC: Monday, October 29th, 9:35 AM

Reuben put two cups of coffee on the coffee table. "Ready to kick some ass today?"

"Sure am." MadFast picked up the black coffee and took a sip. "Think it'll take long to install?"

"Nah, don't think so. Should be easy enough. It seems fairly idiot-proof too, so I don't think we'll run into misconfiguration issues. Whether the default normal config is secure enough though, that's another story."

"Yep."

They figured out who would be doing what during the day, and how to make best use of the time. They got into the car, and off the little Honda sped towards the Vigility office and their lab. They both marinated in their own thoughts as the car moved along, listening to a techno mix in the CD player and working through their own parts of the day's task in their heads.

Arriving at the building, they hustled in, eager to get started. Reuben went up to his cubicle on the seventh floor to grab his laptops while MadFast opened up the lab on the sixth floor.

The lab was a mish-mash of systems: two NT servers, a Windows 2000 workstation, and an NT workstation system. Between them ran Ethernet cables with a hub in the middle. The small room was a bit tricky to navigate, as the cables ran everywhere and tripping over them was a genuine risk. But it was a working lab, for their purposes, and it was all they needed.

Reuben arrived, handing MadFast the NT-based laptop; it was filled with vulnerability assessment tools and a copy of Visual Studio, plus some Windows-based exploits. "Thought you might want this. I set you up with an account on it already. Username, 'MadFast,' and password just 'password,' but you'll have to change it once you log in."

"Right on! Is this the one you were telling me about, with development tools?"

"Yeah, that's the one. You've got admin rights on it, so you should be set."

"Right on. I'll start on the packet injector, I have some code that I can reuse. Guess what it's from?"

"I give, what?"

"I wrote part of a system for online gaming. Just sort of a test, really, but it's the same basic concept. I wrote it to be flexible and variable, so I've got a basic structure already sorted out. I can set it up so that it'll establish a connection, and fire whatever payload we want at the target."

"Great! So that part's largely done?"

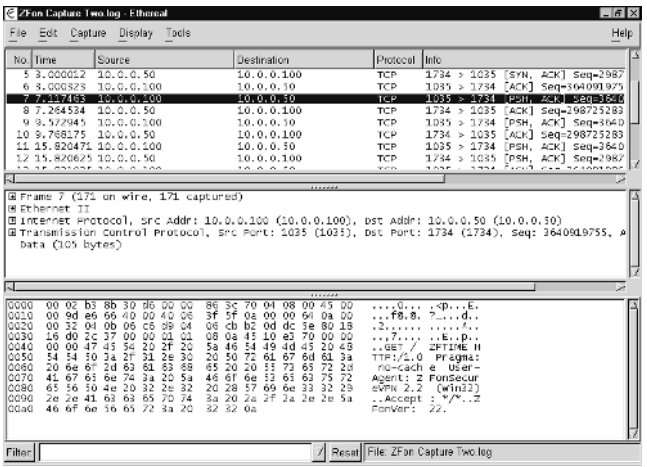
"Exactly."

"Cool. Let's finish installing this stuff, and then we can get some packet captures. I can handle that part while you finish the tool."

They got the software installed and intercommunicating properly. MadFast began setting up Visual Studio to his tastes and downloading code from his FTP server at home while Reuben set up a sniffer and did a few practice captures, setting the filter to ignore protocols like ARP and SMB, which were also being generated but had no direct bearing on the ZFon software. He then proceeded to do a series of six captures, three with one username and three with another. He pulled up the raw data in the sniffer and looked at the packets for some kind of pattern, some indication of their structure.

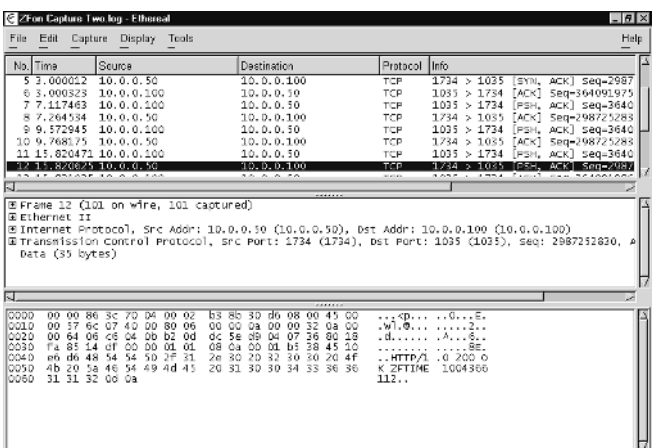
The ZFon software used only one port, TCP 1734. All traffic passed through this port at all phases of the connection. As normal, there was the standard three-way handshake needed to establish a TCP connection. A packet with the SYN flag set went from client to server, the packet with both SYN and ACK went to client from server, and the packet from the client to the server with the ACK flag set completed the connection. The next packet (and the first one containing data) went from the client to the server, requesting a VPN connection.

Packet One



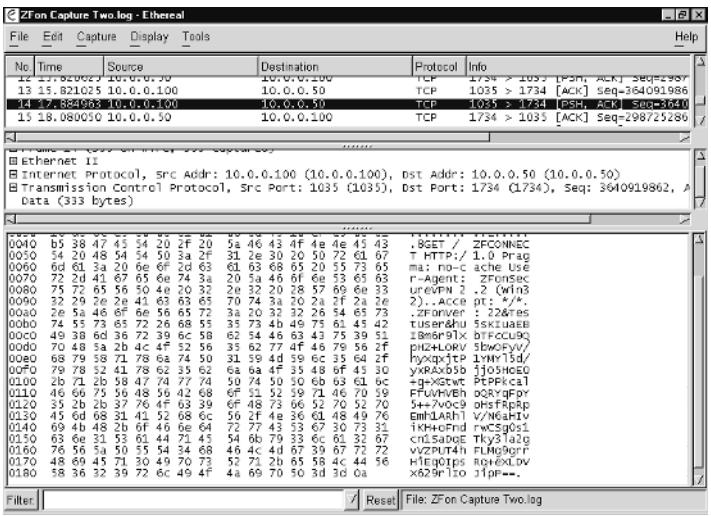
The first packet, which MadFast and Reuben promptly defined as "Packet One," was a time request, in fairly human-readable format. This was apparently to make sure that both ends of the connection were operating on the same time, as session keys would be set to expire after a certain period of time. It might have been up to the client to know when a new key was needed, and to request it; if it was operating off of the time of its hardware clock, and that clock was set even a few minutes later than the server, the key might expire before a new one was requested, breaking the connection.

Packet Two



"Packet Two," as it was called, was the time reply to the client. Not a lot of surprises there, and since everything was passing over TCP, spoofing options were probably limited. There wasn't much chance of a race condition either, since you couldn't flood the client or server with lots of false packets…at least not any that either end would accept as valid. And if you tried a large enough set of packets in hope of finding a match, odds were that the real packet would get through before anything fake that matched the right sequence number would. Even with predictable sequencing, you'd need more time to match up than you would have to work with. Two packets didn't take long to go back and forth.

Packet Three



"Packet Three" showed some real promise. There was a well-defined data structure containing version information, the user name, and some indeterminate data. The Field delimeter was apparently the & character, and it looked like there were two fields of the mystery data at the end of the packet. The odd thing about the data was that it was all characters; the bytes all used only the first seven bits. There were no values above 128, only upper and lowercase letters, numbers, slashes, plus signs and equal signs. The equal signs always came at the end though, as though they were padding of some form. Another interesting fact; the packets all looked like they were modified HTTP GET functions, including "pragma no-cache,"

which made sense since the ZFon documentation said their protocol was designed to work correctly through proxy servers. If the information was cached, it would only be correct for the first connection, after which connections would fail to work properly.

"All packets after Packet Three are encrypted; Packet Three must contain the authentication *and* the initial keying data from the client," Reuben told MadFast. "I think that's our target for now. I'll work on decoding the offsets in the packet; there are a few fields. When I'm done with that, I'll start building some payloads for your injector."

"Right on. Check this out; I'm building it to be like a rifle." Reuben stepped over to the laptop and took a look. Sure enough, the GUI was full of ballistic references. The "Send Packet" button had crosshairs on it, and the button that looked like it led to the dialog box for selecting a payload to send, was labeled: "Load Magazine."

He smiled at the irreverent nature of the whole thing. "Nice. Okay, I'll get back to making you some bullets to fire with this thing. Hey, can you do me a favor?"

"What's that?"

"Can you make it so that it'll strip off any carriage returns in the payload? That way, I can have every component of my payload on a separate line; it'll make them easier to read."

"Sure, but let me know whether you'll be using Notepad or Wordpad; they do the line breaks differently."

"I'll be using Notepad."

"Right on, I'll do it. There won't be any characters like that in the normal packets…you're sure about that?"

"Yeah, I'm pretty sure. It seems that it's all those characters I told you. Kind of funny, I haven't figured that one out yet."

"It might be good to know what that's all about. If the data is being transformed in some way, we'll need to un-transform it so I can do things like entropy checking."

"Ah, okay. I'll focus on that after I build the test payloads then." Reuben went back to his laptop and started designing packets. He figured there were four data fields in Packet Three, and so he started with four packets, one with each field set to be too large. Then he expanded on that

concept, developing different sizes and types; some of the larger fields just had random garbage, others had special characters to see what would happen if they were taken literally. And another set of packets had no data in one of the fields at all. All of them used data from captured packets when called for, so the data was probably at least somewhat valid. Reuben decided that once he knew what the unusual character set of the packets was all about, he would come up with another set of test data to send to the server.

"Are you getting hungry?" Reuben suggested.

"Yeah, actually. Let me finish cleaning up this function, and then we'll go get some food."

"Sounds like a plan." Reuben started writing down notes of where he was at this point in things, so that he wouldn't lose his place mentally. Still, he couldn't figure out what to do about how the session and encrypted data was transformed, or why. Every option that came to mind was instantly discounted. He vowed to put it out of his mind for a while as the two of them locked the door to the lab, and walked to the elevator.

As he unlocked the car, Reuben still couldn't get the thought out of his mind, the notion that the answer to the mystery was already in his head. As he got in, reached over to unlock the other door for MadFast, and started the engine, it hit him.

He sat for a minute, thinking about the data. *Lowercase characters, that's 26,* he counted. *Uppercase, another 26, that's 52. Add digits and that's 62, then the plus and slash, that's…64.* Something nagged at his mind; the solution was right there. He was close to understanding it. *It's like a number that uses 64 different digits to…wait. That's it…it's base-64 encoding! Proxies don't always like extended characters, so they use base-64 encoding to make sure that it's kosher!* "I have it…it's base-64 encoding!"

MadFast turned, for a moment not knowing what Reuben was talking about. Then, it dawned on him, and his head tilted back as the recognition struck. "Yeah, that makes sense. Right on! That way it works with proxy servers!"

"Exactly. Great…do you have anything to do base-64 encoding/decoding?"

"Nope, but I think we can figure something out when the time comes. At least now we know."

"Yeah, true enough. I'm almost ready with the packets too. This is going to be cool. I feel lucky too."

Reuben pulled out of the parking lot, waiting briefly at the light to turn onto Route 7, then pulled into the lunchtime traffic.

Washington, DC: Monday, October 29th, 1:52 PM, 2001

"While you look over the menu, can I bring you something to drink?" The waitress asked.

MadFast looked at Reuben, then decided to answer first. "Coffee and water would be great." He always drank those two, at every meal.

"Sugar and cream?"

"No thanks, just black is fine."

"And you, sir?"

"Iced tea for me," Reuben responded. The waitress walked off briskly, and the pair looked over the menus to pick among a choice of traditionally unhealthy chain restaurant food. The waitress returned with their drinks and took their order before cheerily heading to the back of the restaurant to put the orders in.

"So, how do you like it over here so far?" Reuben inquired.

"Oh, I'm happy. Dude, I really appreciate how you've been, making sure I'm comfortable and everything."

Reuben smiled as he poured sugar into his iced tea. "Don't mention it. I mean, we need you for this, and we really appreciate that you got some time off to come work with us. And besides, this is fun for me too. You're great to work with!"

"Right on. So, do you think we'll find anything?"

"Yeah, I do. I don't know why, but it's just a gut feeling. I can't help but think that with the way they deliberately decided to make it possible to reconstruct session keys, they really didn't make security the number one priority."

"I see your point."

The waitress reappeared with their food, lowering the plates in front of them carefully, before asking if they needed anything else and striding off sweetly to tend to other things. Judging from the speed of service here, they were still geared up for the lunch rush, even though the restaurant was nearly empty at this time in the afternoon. MadFast and Reuben started attacking their food, simultaneously realizing how hungry they were after working so diligently during the previous several hours.

MadFast asked, "So, what happens if we find this thing is so screwed up that they need to pick a different product?"

Reuben hastily worked to finish chewing the mouthful of food he was working on so that he could answer. In the end though, he didn't know why he was hurrying; he didn't know the answer nor did he want to consider the situation. "I don't really know, but I bet it'll be a hell of a mess. Your guess is as good as mine. But I get the impression that ZFon really needs this deal to go through. I've never heard of them before, have you?"

"Nope. So this must be a huge deal for them."

"Yeah. We need to watch our backs. Not that a vendor normally has any kind of incentive to play nice against guys like us, but here it might be even worse. We need to document everything, and double-check everything we come across. Our credibility has to be perfect all the way through, to armor us against any denials or God knows what else they might come up with. Come to think of it, I should tell Bob about some of the ramifications, just to make sure he understands. He's very savvy, but I don't know if he knows how the technical details play into it. I'll talk to him this afternoon and let him know what the likely scenarios are. He's really good at this kind of thing. He'll probably be able to warn us if we're about to do something politically stupid at some point."

MadFast smiled. "Right on. I don't think that will be hard. It isn't like we're critiquing art. We can prove what we find, easy as bits and bytes. It's not like they can deny we found a buffer overflow if we root the box."

"True enough. But just the same, whatever we do find, I want to be able to reproduce it easily in any environment. We need to keep track of how we set things up and make sure that we know if configuration plays a role in any vulnerabilities we uncover. If so, we need to know exactly

which configuration changes do what, so that they can't turn around and ask us for a 'demonstration' on a box that isn't going to be vulnerable."

"Good point. That shouldn't be hard either. It's not like there are too many configuration options that are within the planned configuration that DoJ will be rolling out."

"Yeah, true. And good to remember, too. But we might want to make sure that we know if even an unplanned config is or isn't vulnerable to a finding of ours. Kind of the flipside of the potential for a configuration error producing an issue, it could be that a configuration choice eliminates one. Then we can show some value to DoJ by telling them how to mitigate the risk by changing their planned standard config."

"Ahhhh…so instead of the vendor swooping in and raining on our parade, we get to be the heroes."

"Exactly!" Reuben was thinking proactively. At this point, the ball was entirely in their court, and they could either cover their bases or not. They had the benefit of knowing what they were going to be saying to everyone, and what their findings would be. It wasn't hard to guess what the motivations of the other players might be, so if there was going to be a problem, Reuben and MadFast had the edge. He returned back to his food, stuffing another frenchfry into his mouth. "How do you think we're doing, so far?"

"I think, pretty good. I know what I'm doing, and it looks like you know what your end is too. We've just gotten set up, but I think we're going to cover a lot of things. I don't feel like we're forgetting anything or just wandering around lost. The plan you laid out seems good."

"Ah, good. That's what it feels like for me too. So we're on the same page."

MadFast took another drink of his coffee, and the two of them resumed eating, like it was another aspect of their work. When they finished, Reuben paid the bill, leaving a hefty tip. He loved tipping well; it made him feel good that someone else would feel good from something he did. And usually the difference between a bad or unremarkable tip and one that got a genuine "Thank you!" from a waiter or waitress was only about a dollar or two. MadFast put on his jacket as Reuben put the receipt in his wallet to expense, and the two of them left.

Listening to techno again in the car for the short drive back, the two grooved to the music as Reuben moved semi-aggressively through Tyson's Corner lunch traffic. The air was thick with a sense of mission as they went back to the office to pick up where they left off, much as two commandos might feel as they started toward an objective in the night. They wanted so very badly to accomplish this objective, both for the glory and lust of the hunt and in service to their country and trade. If there was anything unsafe or insecure about this software, they would know about it before they were done.

Back in the lab, they stepped carefully over the network cables as they went back to their respective chairs, shrugged off their jackets and sat back down. They logged in and took a second to figure out where they left off, looking at their notes and contemplating.

MadFast looked over his code one last time. "I think I'm about ready here. This should compile fine, unless I made some small mistake somewhere. How are you with the 'ammunition'?"

Curiously, Reuben looked over Frank's shoulder and glanced at the code. The first part was displayed, and Reuben could kind of follow how it worked, at least at that point in the software.

```
#include <winsock2.h>
#include <iostream.h>
#include <stdio.h>
#include <conio.h>
#include <stdlib.h>

void mein()
{
        WSADATA wsaData;
        WSAStartup(MAKEWORD(2,0), &wsaData);
        int iResult = WSAStartup(0x101,&wsaData);
        if ( iResult != NO_ERROR )
        {
              printf("WSAStartup doesn't work, dude!\n" );
        }
        else
```

```
{
        printf( "Socket up, right on!\n" );
        SOCKET m_socket;
        sockaddr_in clientService;
```

Reuben smiled. "I've got a few fun things set up, and I'm almost done with the rest. Any preference or suggestion as to the characters to use for overflows?"

"Oh, right on! You're going to love this. Use the equivalent of hexadecimal 90 for every filler character. It's an instruction that raises havoc in assembly."

"Got it. Glad I asked!" Reuben fired up calc first, checking to make sure that 90 in hex was actually 144 in decimal. Seeing that it was, he then pulled up notepad, and typed **Alt** + **144** to cause the correct character, É, to appear. He copied this and went through each payload file one at a time, doing a search and replace of the original filler with the appropriate character. Each file had a different variable padded out to an extraordinary length with the letters. One set of the files had only an extra hundred letters in the proper place, and another set of them had several hundred. Sometimes a buffer overflow required a great deal of extra data to execute, and while Reuben figured they might save some time by just going with super-large values off the bat, he liked the idea of starting smaller and working upward.

MadFast started a build in Visual C++, watching for errors. "Ah, shit." The compile stopped on an error before completing. "Must have made a typo or something somewhere. I'll need a bit longer before I'm ready."

"Hey, don't sweat it. Nothing ever works right the first time. And hell, we've just gotten started. It's not like we're making bad time here."

"Yeah, I know. But it's sort of a pride thing." MadFast smiled at Reuben. "I always want my compiles to go smoothly the first time. Kind of a Zen thing, even though I know it's silly."

Reuben smiled back. "Ah, I understand. I'm always pushing myself too. Cool." He went back through the payload files, double-checking to see that he had named them all correctly so that he'd know which one attacked which data field, and that they all had the correct padding characters in them. "Hey, just for grins, we should try protocol attacks just for fun."

"Right on. I was thinking that too. Of course, we probably won't find anything other than what the operating system itself is vulnerable to. But who knows, they might have something that barfs even when Windows handles it without a problem."

"Even so, it's still something broken."

"Yeah, but it's something they already could know about. We're focusing on the app here, that's the thing we're supposed to check out."

"Yes, but we're supposed to check it in the planned configuration, and that includes this operating system. But it could go either way, really. I see your point. I'll get some clarification."

"Right on. While you're doing that, I'll find what I did wrong in my code and fix it."

Reuben got up and went out the door towards the elevator to go upstairs. Standing at the elevator, he realized how much he hated waiting to go up just a couple of floors. But as with most buildings, the doors between the stairs and each floor were locked so that once in the stairwell, you could only exit on the ground floor. Since almost nobody would have taken the stairs anyways, nobody seemed to care, but Reuben welcomed any chance for exercise that he could get. He used to be a lot more active, being an avid cyclist, but these days he spent all his mental energy at work, and thus had neither time nor motivation for exercise. He'd not gained weight, instead losing it, as he never really got fat. Instead, his muscle mass decreased, leaving him trim…a bit too much so for his liking.

The elevator arrived, its doors opening to reveal the empty interior. Reuben stepped inside, rotating and jabbing the button to go up. A brief interval later, the doors opened again, letting him out. He barged into the office area, walking down the nearly-silent corridor to look in on Bob's office.

Bob looked up from his desk, happy to see Reuben. "Hey! How's it going down there?" he asked congenially. He clearly wasn't worried, curious for the sake of his own curiosity rather than some anxiety that things weren't going well.

"Well, we're all up and running, we've got some idea of how the data looks going over the wire, and we're getting ready to start shooting garbage at the server to see what happens. Right now, MadFast is debugging… I mean, Frank, is debugging the code for a tool that we'll use to do the job."

"Great! So, what do you need? Or did you just want to get up and stretch your legs a bit?"

Reuben laughed lightly. "Well, there is one thing. We know we're supposed to test the planned configuration of the VPN, but that includes the operating system. But since there's already a lot of information about the weaknesses and strengths of Windows, we don't know if we're supposed to be testing that as well. We talked about it, and we could see it going either way."

Bob sat forward in his seat. "What's your opinion of the impact of one option versus another?"

"Well, we can be more thorough if we go over the whole thing, including Windows. But it also means it'll take longer, and we might miss more. Compared to an application, there's a lot more that can be right or wrong."

"What's your gut tell you?"

"I say we stick with just the ZFon software, and specify that they'll have to properly harden the host first. We'll test for possible issues of the two in combination, but we won't say anything about that testing unless we find something. That way we'll cover everything without duplicating the work of others."

"What kinds of things might be 'in combination'? And how would you know what to look for?"

"Well, I can think of only a few things. One is network behavior. It's a possibility that the software stands between the outside world and the operating system, in which case we might find something about it that doesn't act quite right. Or, perhaps it'll be even better. Either way it'll be interesting. And there's also the likelihood that some files or registry keys need to be well protected, like private keys or whatnot. Those two are about the only things I can imagine, really."

Bob smiled. "Okay, I understood about half of that, but the real answer, I guess, is that you know what to look for and what would be a waste of time. Okay, do it that way."

"Cool, will do. It's going really well. Frank's great to work with, and we're both on the same page. This is great; he knows a hell of a lot about certain things, and I know a good bit about other ones. Between us, we make one hell of a geek!"

Bob laughed. "Oh, God help us now! The two of you loose on the town!"

Reuben smiled back. "Oh, you have *no* idea. I have this really funny feeling that we're going to make some waves with this."

Bob smiled back. "You know something? I don't doubt it."

Reuben stepped a bit further into the office and pulled up a chair. "That brings to mind something else I thought I should bring up."

Slightly taken off guard by this, Bob's tone became a little more serious. "Alright, shoot. What's on your mind?"

"Well, we took the time to actually check out the background of ZFon itself, the company," Reuben explained, "and it looks like they aren't doing too well financially. Their stock isn't doing well at all, and I'm sure they're giving the employees options. And this is a really huge deal for them, probably the biggest sale they've ever made."

"So, in other words, you're worried about what they might do if you and Frank find the software is all screwed up?"

"Yep, you got it. There are a few things that software companies do when faced with a vulnerability. The one that we have to worry about the least is their doing the noble thing, and owning up to it, working with us, and fixing it. If they act that way, nothing else matters, life will be easy and everyone wins. But that's uncommon, I think. At the other end of the spectrum, ZFon might outright deny and try to bottle up information about the vulnerability. In cases like that, they might try to misrepresent things by throwing twists in, like claims that our findings were in a 'non-supported' configuration."

"Well, obviously that won't work. The configuration you're using is the one they told DoJ to use, and DoJ knows that. And I assume that if you find anything you'll be able to prove it, right?"

Reuben nodded. "Yes, exactly. But the whole point, as you probably know, is that they might not follow common sense, since they may feel backed into a corner by any of our findings. It's the desperation factor that concerns me. If everything plays out according to logic, we can handle it. But who knows how they might behave if they think the company might go under from this?"

Bob nodded. "We'll handle that if it comes up. You and Frank are pretty bright, and we've been playing it by the book for DoJ so far, and they're happy. So I think we'll be able to handle it just fine."

Reuben nodded back, smiling a bit. "Good, I think so too. I just wanted to let you know that it might be an issue later on." He got up, adding "I think he's probably done with the tool now, so I'll go get back to it. We'll keep you informed as to how things go."

"Good man. Go get 'em and I'll talk to you later." Bob smiled happily, and went back to his work as Reuben left the office to go back downstairs.

MadFast looked up and back as Reuben came in. "You won't *believe* what was wrong."

"Got the code working?"

"Yep. It was a stupid typo, right at the very beginning. I typed **void mein** instead of **void main** and didn't even catch it. You'd think I was hungry for Chinese food or something, with a typo like that!"

"Not where you were looking for a bug?" Reuben smiled at him. It had been years since he'd spent much time programming, and even then it was just a special project at one of his earlier jobs. He remembered how maddening it could be to have to search your own code for your own mistakes, though.

"Nope. It had to have been at the start because of the compile error I got, but I went over the code three times in full before I actually looked up at the very first part and saw it. That was a first for me, having a bug in the first line of code."

"Well, now it works. I'd say you built that in a hell of a short amount of time." Reuben clapped him on the back. "Let's get rocking and see if we can rip this thing a new ass." He sat in his chair. "Let me share this folder

out…ok, on my system, look for a share called 'ammo.' It has the payloads, in the order that I want to use them. Load the first one, and let's rip."

"Right on. Lock and load!" MadFast started up his program, and navigated to the shared folder on Reuben's laptop. Selecting the first file listed, he set the port and IP address of the VPN server, as Reuben walked over to the VPN server's console and started up Task Manager, picking the tab for running processes, also noting the total number of processes running. If they found a buffer overflow in the software, one or more of the processes would likely crash and disappear from the list.

The program was designed to be able to mimic nearly any network application that used TCP; it would establish a connection, and then fire the data payload selected by the user. The user would pre-define which data was to be sent to the target, and thus they had to know what the target would be expecting, but Reuben had done that part already. What they both had to do now was pay attention, to make sure that if one of these payloads *did* produce an undesired effect, they'd spot it. It wouldn't do to have the third payload crash the server, only to confuse them because they didn't notice it until they launched the sixth payload.

The payloads were all designed as illegitimate versions of "Packet X," since that was the unencrypted packet that showed the most promise. Reuben decided to make a set of variants with proper encoded data (borrowed from valid captured packets) and a set with just plain garbage. It would be interesting to see if there was any difference in the reaction. There was one last payload that would be used at the end, and it had encoded data that equaled nothing. It would be neat to see what impact that might have on the encryption, seeing that it wasn't designed to be non-repeatable. If they could force the encryption key to be the same each time, or at least remove one of the variables that went into its creation, it might be possible to derive the other components of the key, and thus obtain what was needed to break all past and future encryption on the same device. Obviously, this would be as bad a problem as a buffer overflow vulnerability, if not worse. At least you could detect when someone rooted your box; being able to detect that someone was intercepting, decrypting and reading your traffic was not so easy.

"Packet XA1 loaded," MadFast called out.

"Fire!" Reuben exclaimed comically.

MadFast clicked on the button labeled "Fire!" and the two watched the Process List on the server. No change, and when Reuben clicked on **Performance** to check processor utilization he saw nothing there either. "Nope, zero effect. Load Packet XA2."

MadFast clicked to select another payload, selecting the next one in the list. This one had a ridiculously long username. "Packet XA2 loaded," he announced.

"Fire."

They blinked, and leaned closer to the server. Suddenly, there was one process left.

"I don't fucking believe it."

MadFast reacted second. "Okay, you saw it too then?"

"Something crashed, right?" This was way too easy. They could *not* have found something so simple and so wrong so quickly. Could they?

"Wanna reboot it and see if we can do it again?"

"Hell yeah." Reuben closed Task Manager, and had the machine reboot. He was practically holding his breath. *My God, we found something. I can't believe we found something*. He went over everything in his mind, trying to come up with any kind of way to explain what could have caused the process termination aside from a crashed process. They'd checked to make sure that it was always on, the system wasn't running anything else, and the process had stayed up all this time, only to die when they hit it with another payload. *I believe in coincidences, I just don't trust them*, he thought. Maybe the combination of the first and second payloads together had a part? Reuben watched the system slowly reboot, cursing himself for not checking Event Viewer for an error, or the Services control panel to see if any services showed as stopped.

They watched the blue screen of NT breathlessly as it loaded system drivers, one dot at a time crawling across the top of the screen. It never seemed to take so long as it did now for the system to come back up. "Man, is it me or does it seem to take forever when you're eager to look at it?" Reuben quipped.

"No kidding. Are you thinking what I'm thinking?" MadFast responded.

"I don't know. I'm not sure what to think right now."

"I'm thinking the NSA missed something, *really bad*. Dude, we rocked this!"

Reuben was fighting hard enough to control his own enthusiasm, so that he'd keep a cool and scientifically accurate head throughout this. "We'll see, but I think you're right." He grinned.

The system came up, showing the typical "Press Ctrl-Alt-Delete to Logon" screen. MadFast looked like he wanted to log in himself if Reuben didn't do it first.

Reuben knew what he was thinking, but had an eye on the drive activity light, which was still showing bursts of activity as services started. "Wait, it's not fully up yet. We can log on now, but let's just wait until it's entirely set before we do anything. Patience, patience."

MadFast sat back in his chair and resolved to relax a bit. "So, what if we did find something? What then?"

Reuben stood back for a second thinking about that one. It had never occurred to him. "I guess we tell Bob, and play it from there. We definitely tell the client face-to-face, and without the vendor present. And I'm guessing we'll follow their guidance as to what to do next. But at the very least, if we did find something, we found a single-packet Denial of Service attack, and that's a showstopper. Considering what caused it, I'd suspect a buffer overflow is at hand and that is *definitely* a showstopper. I think the vendor is going to shit themselves over this."

MadFast smiled. "Booyah!"

The drive activity light hadn't flashed for over twenty seconds, and Reuben hit **Ctrl** + **Alt** + **Delete**, bringing up a login screen. He logged into the system, and took a quick look to make sure everything was right. "Okay. Everything is running, no stopped services…23 processes, as there should be. Alright. This time, let's just hit it with Packet XA2 off the start."

"Still loaded," MadFast reported back.

Reuben had a thought. "Shut down and restart the application. Let's make sure this is as clean as possible."

"Right on." He closed it, logged back off and back on again to flush out any weirdness that might have been floating around if he'd made a

mistake in the code, and started the app back up. He loaded the payload again. "Ready, Packet XA2."

"Fire."

The small panel in the lower left-hand corner of Task Manager went from saying "Processes: 23" to saying "Processes: 22."

"*Yes!*" they both yelled, as MadFast got up out of his chair and the two beamed mightily. They turned to look back at the running list, to see what was missing. "Yep, it's not there anymore." One of the processes that belonged to the ZFon VPN was gone.

Reuben could hardly contain himself. "Wow! Okay! Ah, alright. Let's go see Bob. This is amazing!" He knew they had a lot of work to do still to quantify things and see how bad this one problem was, but he knew Bob would want to know as soon as possible. Even though he wasn't a geek himself, Bob definitely understood the geek frame of mind, and shared in the joys and excitements that geeks loved. He deserved to be in on this as early as possible. There would be more time to check the other payloads while he set up the meeting with DoJ to give them the good (or bad, depending on how one looked at it) news.

The two triumphantly stomped out of the lab, locking the door behind them as they went to the elevators. Smiling slightly, they silently maintained the tension of holding their reactions in, save for the occasional "Booyah!" quietly said. Going down the hall to Bob's office, they stood just outside the doorway looking in.

Bob looked up, surprised by the second visit today. "Hey guys, what's up?" He could sense something was afoot, and his own curiosity piqued.

MadFast and Reuben looked at each other, wondering who would get to say it. "Go ahead, you tell him," prodded Reuben.

"Alright. We found something."

Bob's eyes widened, and he laughed out, "Wh-hat?" He grinned. "Already??"

MadFast and Reuben smiled back at him, looking like cats that had eaten an entire pet shop's worth of canaries. "Yep," Reuben continued, "we're not sure exactly what yet, but we can crash the VPN with a single packet. The key is sending it an unnaturally long username. The funny thing is, the packet is out-of-sequence; it should be preceded by some

other things. But no matter, the fact is the VPN dies instantly when you hit it with this."

Bob leaned back. "Wow! I gotta tell ya, Reuben, when you said you needed this guy, I wasn't so sure about this. But I gotta hand it to you two, you really pulled it off! We're gonna make history!" He was as infected with the sense of triumph and conquest as any of them.

Bob got a handle on himself and sorted out the next steps. "Alright. Here's what we need to do. I'm going to call the client and let them know. Is there anything you want me to tell them, or make sure? I mean, I want to make sure we do this right. I was thinking about what you said earlier, about the vendor, and we need to be careful."

MadFast stepped back a bit, comically, miming the notion that he wanted no part of these decisions and would leave his fate in the hands of Bob and Reuben. Reuben smiled at him, and turned to lean closer to Bob. "Well, we tell them no details over the phone. We tell them that face to face, without the vendor present. I want to be able to get the whole truth to them, and only to them, and to all of them at the same time. I'd like their decision to be made as to what to do next before the vendor has a chance to try and interject. I don't think we got so lucky as to find the only problem with this thing so easily and so quickly. I think this software is probably going to turn out to be a total piece of crap. So we have to make sure that the vendor can't spin this like it's nothing, because it's probably just a sign of more things to come."

Bob considered that. "I never thought of it that way, good point. Alright, I'll call them and set it up. In the meantime, you two go down there and document everything you're finding, get it all down on paper and clear. We need to do this right the first time, like you said, so that we don't have any problems later. That company is going to fight this tooth and nail, so we'll have to convince them too."

Reuben nodded sharply once. "No problem. We're on it. And we'll finish our checks for more problems after that, documenting as we go. It'll be good to show what does and what does not crash or break this thing."

Bob waved. "Have fun, you two. Keep me posted, and I'll let you know what's going on up here." The two nodded and spun, leaving the office and

hurrying back to the lab. They couldn't wait to get down there and start working again.

As they walked to the elevators, they felt a sense of release from having shared the news with someone else. Before entering the lab, Reuben had a thought. He dialed Brianna on his cell phone.

"Hello?" she answered.

"Bri? It's Reuben. We're having something nice for dinner tonight. I have some great news." He smiled into the phone as he told her the general details.

Tagig, The Philippines: Monday, October 29th, 5:25 PM, 2001

Lualhati didn't know what to do. There were so many of them, but they were just little kids!

"Go away, *Muslim!*" yelled one of them as he moved to the front of the pack, picking up more stones from the ground to pelt at Lualhati. "Why don't you go blow someone else up!"

It had gotten worse. Since 9/11, the normal background level of animosity against Muslims here had blossomed into a virulent and all-powerful hatred. The group of children continued throwing whatever they could pick up at Lualhati, their fear finding hatred as an easy outlet. Lualhati couldn't do anything except try to retreat; while he could easily have fought back, he was pretty sure that a Muslim beating up small children in the street wasn't likely to survive very long right now. He didn't know what hurt worse, the cut on the back of his throbbing head from a well-aimed rock, or the humiliation of being driven away by a pack of nine-year-olds. *Since when did everyone love the Americans so much?* he wondered. He could remember how happy everyone was to see Subic Bay close down, the American sailors and soldiers no longer around to support the rampant sex trade in the area. He also remembered the resentment at the Americans when the local economy sagged from the loss of trade provided by those same military personnel.

But for the past month, all anyone seemed to feel towards the Americans was sympathy for their loss. And all they felt towards Muslims was hatred like he had never seen before. For the first time, Lualhati actually wished he was

back in the squalor of Mindanao, as he ran away from the children and down the street, turning into a narrow alley.

He slowed down, having left the angry children behind. It seemed they only had enough hatred to attack him when he was nearby, not enough for the inconvenience needed to follow him and do more damage. Bending over, he caught his breath and tried to make sense of this nightmare. He wasn't able to go to school anymore, his mother had been fired, and their money was running low. He ached to get time to work on a computer, even to just play around with coding, but that was out of the question while his mother looked for another job. What had Lualhati done to any of these people to make them hate him so much?

Agpalo hadn't been surprised by any of it. "It's like this all over the world," he had said. "It's the Americans; they hate brown people, but they hate Muslims the worst. And they're getting the rest of the world to go along with them. I think they planned it, the bombing. I don't think there were any terrorists at all. I hear Bush was behind it, with the Israelis." He was getting increasingly angry, Lualhati thought, but maybe he was right.

Lualhati wondered where Agpalo had been going lately. He was worshipping more often now, but nowhere that Lualhati knew about; whenever he asked him Agpalo just kept his mouth shut. Where was he going, and what was the big secret? And why didn't the taunting seem to bother him the same way?

Agpalo had always been the angry one, always brash and irritated by their lot in life. And now he was calm, just as things had gotten so much worse. How could this be? It made no sense to Lualhati, and his mind flicked about trying to figure out the answer.

In another part of the city, Agpalo was doing the very thing that Lualhati was wondering about. He was listening. Weeks earlier, he had been approached by a stranger after worshipping at the mosque, and told about another place of worship. He was invited to attend, and stay a bit after to listen to what the Imam had to say. Taking the stranger up on the offer, he went the next day, to discover that he'd been invited to a meeting of Ibn Kelbeh. Ibn Kelbeh was the so-called "terrorist" group that operated in Mindanao; Agpalo had never expected to find any of them here. He'd never thought they'd be like this, they seemed so much nicer than was let

on by the government or the newspapers. They just wanted to be able to practice their faith in peace, it seemed, and only adopted violence because they had to, to defend their freedom. So what if they bombed places, what else could they do?

"Our brothers have shown the truth, that America is weak and vulnerable. Those youths who did what they did and destroyed America with their airplanes did a good deed. They have moved the battle into the heart of America. America must know that the battle will not leave its land, God willing, until America leaves the Holy Land, until it stops supporting Israel, until it stops the blockade against Iraq."

The young followers answered out, not entirely in sync, "Allah be praised." Agpalo listened attentively in the small windowless room, among the audience. His eyes sparkled with the hope borne of something to hold onto.

The speaker continued. "We must do our part here. We are far from America and the Holy Land, but we can still fight against the faithless powers of our own land that support the infidels in their crimes against Muslims. Their crimes against our brethren here, in Mindanao, and throughout this region may not go unpunished."

Agpalo listened quietly and with intense devotion, but without a sense of bearing. *What can I do about this?* he wondered. He wanted to act, he wanted so badly to do *something,* but what? All he knew how to do was to write code and worship. He wasn't strong, couldn't afford to go to Afghanistan to fight the infidel Americans, and certainly didn't have the desire to blow himself up. But he still simmered inside. He wanted to help, to hit back, to fight. *What can a computer geek do here to fight the Americans?*

Washington, DC: Monday, October 29th, 4:37 PM, 2001

"Alright, so it's the 'ZFon Listener' that bombs." Reuben was looking through the Services Control Panel on the VPN server, looking for clues. He opened up Event Viewer, looking through the Application logs first for any errors with their characteristic red circle with an 'x' in it. "That's

funny, no errors at all. Maybe in System?" He switched to the System logs, but again nothing.

"You'd think this was a healthy box, looking at this. But it's been owned twice over in the past thirty minutes," observed MadFast.

"Yeah, not good. So if this is a root compromise, you don't even have to clean up after yourself in the logs. By the way, is it possible to write the exploit so that it restarts the service?" Since no error message appeared anywhere on the system, determining whether the compromise was indeed bad enough to gain control of the system would require some sophisticated work. The method to use in this case would be to run something like Ollydbg or IDAPro on the server, and watch the process that was attacked. If they saw contents of the payload in certain registers in memory, they knew that they could make the system do whatever they wanted.

"Yeah, but only if you can restart the service. Try it."

Reuben clicked on **Start** on the Control Panel. A small dialog box popped up, with a progress bar, whose increments filled in slowly. "I don't think it's going to start," Reuben said. "It doesn't go this slowly and smoothly unless it's just marking time until it times out."

"What if you stop the other services?"

"Good idea." He waited until the attempt failed, and then stopped the other ZFon-related services. Then, one at a time, he started them back up, guessing at which had to come up first based on dependencies. He found that the ZFon Listener service needed to be in the middle of the group. "Ahh, that explains it." The service started, as did all the others. "Hey, let's try connecting to this normally now and see what it does."

MadFast went to the client machine, and opened the VPN client. He connected with it. "I think it works. Wow. Yeah, you can write an exploit for this, if you're good, that will stop all the services and restart them in the right order. This is really bad. If you can buffer overflow this and run your own code, you can own the box, and do it in such a way that nobody will ever notice that you did it. There won't be an error in the logs, there won't be a dead service, there's just you, owning the box, with a sweet little backdoor of your choosing running on it. Maybe, maybe someone won't be

able to log in for about thirty seconds, but that's all, and nobody would ever suspect anything based on that."

Reuben concurred. "Yeah. Now we need to sort out the rest of this. Let's go through the other packets. I want to reboot this server just in case, so we're clean. Let's do this by the numbers and get it finished, then call it a day." Reuben started rebooting the server.

"Right on." He loaded the third packet in the sequence, shaking his head at the fact that they were only at the third packet, having found an issue already. "Packet XB1 ready."

"Wait for it, it's not up yet." They patiently waited for the server to stop chunking its hard drive, and Reuben logged in again, repeating the process of launching Task Manager. "Fire."

They both looked closely. Nothing happened. "Want to reboot between every packet?"

Reuben considered that. "I don't think two packets that can do damage apart would fail to do anything when used one after the other. So I don't think so. If we find another weakness like that, we can go back and do a proper reboot to narrow it down. But for now, let's just go through them and see what happens. In the real world, an attacker won't be nice enough to let them reboot before attacks anyways, right?"

"Right on. Packet XB2 loaded."

Reuben checked Task Manager one last time. "Fire."

Nothing happened. Reuben indicated, "Alright, next packet." MadFast hit the button to browse and open the next payload.

Reuben's eyes widened. "What the *fuck?*"

MadFast turned around quickly. The little green square in the system tray that indicated processor utilization went solid bright green. The processor was suddenly maxed out. "Huh?" He turned to look at his own laptop, and verified that he hadn't even selected the next payload yet, much less fired it. He turned back and looked first at the server then at Reuben. "What did that?"

Reuben clicked on the **Performance** tab, and indeed, all of a sudden in the processor utilization graph, the line soared up to 100% and was still stuck there as a plateau, straight as an arrow. "I have *no* idea. But did we just find something else? And if so, what?"

"What was in that payload?"

"Uh, what was that…B2? Reuben flipped through his notes on the writing tablet. That was garbage encoded data, padded out with about half a K of the letter 'Z'."

MadFast sat silent for a second, considering. "Waaaitaminit." He turned back to his laptop, and opened the source code for the app he had written. He went through it, looking for a particular section. "Ah, right on, here it is. Yep, okay, I think I understand what's happening."

"Well, fill me in!" Reuben was dying to understand this.

"Um, okay, so it's like this. The application connects, and waits for us to feed it a payload. In that time the connection is still open, even after the payload. With me so far?"

"Yeah, keep going."

"Okay, but I knew that if we were to feed it multiple payloads as we tested things, we'd want to do it in separate connections, but I didn't want to leave them all open either. So I wrote it so that that when you closed the app or went to select a new payload, it would close the current connection so it could start fresh and new."

Reuben thought he was following, but he was missing something, he felt. "Okay, so when you went to open the next payload, it disconnected. How does that figure into this?"

"Simple. They've got a process that takes in that encoded data, but it doesn't check it at all. It just feeds it into a buffer, and waits until the connection closes to try and process it. And when it does, *boom!* It choked on what you gave it."

Reuben tilted his head back in understanding, his mouth opening. "Ohhhhhh! Wow. We found ANOTHER problem?" he commented incredulously. "I can barely believe it. This is nuts."

"Hey, you called it upstairs. You said that if we found one problem so fast there must be others. You were just right, that's all."

Reuben ran his hands roughly over his face. "Jeez, I don't think I can handle this much excitement in one day. Let's stop here, and write up what we've got. Then we'll go up and tell Bob, and call it a day. I need a break from this, I think, just to keep my head clear."

"Yeah, I feel what you mean. Me too, right on."

Reuben sat down and started jotting down rough notes before he forgot the thoughts. Writing on paper seemed better at times, for certain things. This was definitely one of those times. When he was done, he started typing into Word, putting things in order and making sense of it.

As it turned out, they didn't have to go see Bob. There was a knock on the lab door, and Bob poked his head in. "I just thought I'd take a look to see what kind of an operation you guys have running here. Mind if I come in?"

The pair smiled at each other before turning to face him again. "Come on in," Reuben invited. "We found something else."

"Wh-hat?" This was starting to form a routine now. "Another one?"

"Yeah, this one is different though. It maxes out utilization on the processor. Take a look; it's still maxed." Reuben pointed to the monitor.

Bob looked in at it. "This green line that's up at the 100 percent mark. That's what you're talking about? Processor utilization?"

"Yeah. Click on the **Start** button and see how slowly it pops up. That'll give you an idea how bad that is."

Bob tried it, and the Start Menu on the server opened, but very badly and with a jerky delay. "Like my machine at home sometimes. I should have that fixed, I guess. Okay, write this one up too."

"We're on it. Then we're calling it a day, this is just too surreal to handle any more of it today."

"Sounds good. Oh, by the way, we have a meeting at eleven tomorrow morning, at DoJ, where we met before. It's just like you wanted, there'll be representatives from DoJ only, no vendor. And they're eager to hear what you have to say. I didn't tell them anything, just that you wanted to talk to them, but I think…I think they know, at least on some level."

Reuben considered this. "That's fine. Even if ZFon gets wind that we're coming in and that we found something, they can't start trying to undercut it without knowing any details. So we're good, either way."

Bob was more serious this time, having worked off the distracting part of being so thrilled earlier. "Get some good sleep, guys. Tomorrow's a big meeting. And have a drink on me tonight, you did good." He smiled at them, opening his wallet and handing Reuben a twenty-dollar bill. "Anything else you need?"

Reuben looked at MadFast, who looked back at him, replying "I don't need anything, I'm good."

Reuben nodded and turned back to Bob. "Nope, we're all set. We'll just finish up our findings thus far, and we're out of here." He looked down at the cash in his hand. "Thanks, Bob. We'll all have to go out some night and celebrate, though. We couldn't do this kind of work without you making sure we have what we need, and making sure we don't have what we don't need, if you get my drift."

Bob waved his hand. "Ah, don't worry about it. You guys know what you're doing. My part is easy."

Reuben and MadFast both laughed at that. "So, why the hell doesn't anyone else do it right?" MadFast barely managed to exclaim in his chuckling.

Bob lightly laughed in return as he went to leave. "Have a good night, you two. Get some rest! And I'll see you tomorrow, here, before we go to the meeting?"

Reuben waved to him. "Yep, we'll be in by ten."

"Alright. Take care guys."

Washington, DC: Monday, October 29th, 10:11 PM, 2001

Reuben, MadFast and Brianna were all in Felix, a local hangout that Reuben particularly liked. Something about the décor, the fact that the club was fashioned around a James Bond motif made it interesting. And while some of the patrons could be a bit snotty, the manager and Reuben knew each other by this point, and Reuben always felt at home here. Being a Monday night, it was relatively quiet, which was how Reuben liked it. The bars and clubs in Adams Morgan were always such a nightmare on the weekends, what with all the weekenders coming in and filling the places. On top of that, a select but aggravating few always got entirely too wasted and copped a curious attitude. It was like they were trying to play urbanite hipster like it was some charade born of false bravado. None of that was going on tonight, since it was just locals, and sedate ones at that.

MadFast drank some of his beer, looking around at the various television monitors. The movie of the hour was "Thunderball," and it was on every screen. Sean Connery looked in on the club from several angles as he sought to forestall a nuclear disaster. "This place is hella cool. But why's it called Felix?"

Reuben smiled, turning on his bar stool. He pointed up at the Statue of Liberty cutout above the bar. "Felix Lighter, James Bond's equivalent in the CIA, who was from New York City." He grinned. "After all, we *are* in Washington, DC, not London, right?"

MadFast smiled, "Right on!"

Brianna smiled at the two. She'd been watching their antics back and forth all evening. They were still jacked up with excitement from the day's work, and she was just having fun watching them both. "What do you think is going to happen tomorrow?" she asked.

Reuben and MadFast looked at each other. Reuben put down his martini, slowly moving as he figured out the best way to answer this question. "Well, the client is going to be freaked, I hope. They should be, that's for sure. The vendor can either fix the software, deny the bug, or try some other unknown thing. But I doubt DoJ is going to use this crap as-is. And I don't know how the software can be debugged well enough in a short time, with all the stuff we're probably going to find."

MadFast interrupted a swig of his beer, cutting it short as he nodded vehemently. "Yeah. Some of these things can be a quick fix, but I'm betting the larger problem is that they're going about input handling all wrong. They assume everything will be given to them as it should be, but they need to specify what's right and reject everything else. It's not an easy thing to change, it's the kind of thing you have to start doing from the beginning, when you first start writing your code."

Brianna nodded, not entirely understanding what he was talking about. "So what happens to the company that makes the software if they can't fix it and the DoJ won't use it?"

Reuben shrugged. "They've got a problem, then. They might even go under. But what else can we do, recommend that the Department of Justice implement a large-scale VPN infrastructure that anyone could rip apart in a few minutes? I know this sounds callous, but they shouldn't have

gotten into the VPN business if they weren't planning on learning how to write secure code. It's kind of important that security-related products be secure themselves, even more so than with other software."

Brianna took a sip of her martini. She loved martinis, and they made such good ones here, of course. "I guess you're right. It's a shame though."

Reuben was sympathetic, but only so much. "Yeah, I know. But here's how I look at it. I've got a job to do, and I need to do it to the best of my ability. Here it comes down to the fact that I've got a clear duty, and I have to perform that duty. I do feel kind of bad for ZFon if they fold or even if they lose the deal but stay afloat. But that's not important, I still have my duty to perform. And if I forget that, I could be responsible for something really bad happening because people counted on me to do my job, and I failed them. I just have to detach from it a bit and focus on my job." He sipped at his martini again, smiling a bit to try and soothe her.

MadFast joined in gently. "Besides, he's right. They shouldn't have gotten into the business if they couldn't produce a safe product. That's how you have to think about it when it's at this level. It's not like when Windows 98 crashes while you're playing a game on it. This is serious, a problem with this would be exploited by criminals, terrorists, God knows who else. This isn't the kind of problem that just makes you pissed that you have to reboot before you can play again."

Brianna winced at that thought, realizing the stakes involved now. "I'm glad I don't have your jobs," she said.

Reuben and MadFast looked at each other, jointly realizing for the first time that it might not be entirely average that they loved their work so much.

Washington, DC: Tuesday, October 30th, 10:55 AM, 2001

The car pulled up to the building, with Bob, Reuben and MadFast inside. They calmly exited the vehicle into an unusually chilly morning for that time of year.

Reuben rubbed his arms, wishing he'd dug out a warmer jacket. "What happened to the weather today?"

MadFast smiled. "Feels fine to me."

Reuben smirked back at him as they started walking towards the building. "That's because it's not raining!"

Bob just smiled at the banter back and forth. "Alright, you guys ready?"

"We sure are," responded Reuben. "Right, Frank?"

"Booyah."

They walked into the building's lobby, and found a dour-faced security guard sitting behind a sorry-looking excuse for a desk. Reuben wondered for the second time if there was bulletproof material built into it. They went through the same routine as the previous week, producing their drivers licenses to sign in, filling in the blanks on the sign-in sheet, including the one marked "U.S. Citizen?" They were each issued visitor badges, and sat down to wait to be called in.

A blank, windowless door opened, and Vince appeared. "Come on in, gentlemen." He seemed cheery, and quite curious as to what could potentially come from the meeting.

Reuben, Bob and MadFast walked through the open door as Vince held it for them. "The same place as last time?" Bob inquired.

"Yes, sir, the conference room," replied Vince. They filed in and each took a seat, finding two other people from DoJ already there. "I have to go finish something up really quickly, so I'll let the five of you get started. I'll be in shortly to catch up." He walked back out and down the hall.

The three of them sat down, getting comfortable in their seats, and for a moment everyone looked at everyone else, wondering where to start.

Bob spoke up first. "I guess I'll start us off. Thanks for meeting with us on such short notice. We asked for this meeting because we have some preliminary findings to share with you, and felt we should discuss them before we went any further."

The two DoJ representatives leaned forward in their seats a bit. "What kind of findings?"

Bob smiled slightly, looking first at MadFast, then at Reuben. "Which one of you wants to tell them?" he asked.

Reuben sat forward and folded his hands on the table. "I'll take this one. We've found two vulnerabilities thus far, one of which we believe could potentially lead to a root compromise, and the other which defi-

nitely produces a denial of service on the system. Both vulnerabilities, when exploited, lead to total failure of the VPN until it is restarted."

Eyebrows were raised around the table. "You've only been working at it since…Friday?"

"That's right, and that's why we wanted this meeting. We've barely done anything in our testing, and have already found these problems. You might want to reconsider use of this project."

The two representatives must have feared something like this happening and exchanged worried glances; but they quickly composed themselves and leaned back into their seats. One of them responded. "Well, we'll have to consider what you've found so far and determine if it warrants any change in the scheduled deployment…"

MadFast stopped the man in mid-hedge. "What? We just told you that there are, at the *minimum,* two ways to knock this thing down. One of them might *also* give an attacker control over the system. And the crypto uses keys that can be retroactively recreated. What consideration is there? It's broken! You can't seriously be considering implementing it as-is? What is there to determine? This VPN is garbage, and if you rely on it you will be hacked."

The man who had been silent for the past few minutes slowly sat forward, placing his own hands on the table. "There are other aspects to this decision that you are not aware of. Trust that we'll be keeping your recommendations in mind, but that we must consider many factors in this. This is a large implementation, and in the current environm…"

The door opened, and everyone suddenly turned to see Vince calmly step in, a smile on his face, and take his seat at the head of the table. "So, gentleman, what did I miss?"

Everyone looked at each other, not sure how to bring him up to speed without further igniting the discussion. Reuben spoke up. "Well, we've found two vulnerabilities as of today; one cranks the processor up to one-hundred percent utilization and makes the box useless, while the other crashes the VPN Listener process. The second vulnerability is most likely exploitable to gain root access on the box, but we haven't been able to determine that yet."

Vince whistled. "Well, that's a showstopper."

The DoJ rep who had been speaking until Vince entered looked shocked. "What?"

"Well, obviously we can't use it like this. They've only been working at it a couple of days at most and already found these problems. Don't you think anyone else could too? We need to figure out a plan for dealing with this, and hopefully get things sorted out soon enough so we don't end up being too far off of our project timeline."

Reuben and MadFast both relaxed. Here was someone who at least knew what needed to be done, and who understood the importance of the issues found so far. Reuben continued, "We're obviously really concerned about the overall quality of the software. We found this without even trying, and the really frightening thing is that since the cryptographic keys are deliberately designed so that they can be re-created at a later date, compromise of the server can result in compromise of all present, past, and future communications. We think the worst-case scenario isn't if someone was to take and keep control of the server, but rather if they were to simply inject a process into memory to have the basis used for all keys sent to the attacker. Then the attacker could decrypt any and all traffic they intercepted.

"To be fair, I should say that they would have to do a few other things first. As you're probably aware, ZFon has a utility for re-creation of session keys. There are a few safeguards against abuse of the utility, including a two-factor authentication method. But the attacker could merely reverse-engineer the utility to get to the component that actually does the work, and build their own. This isn't a hard thing to do; teenagers do it every day to overcome copy-protection mechanisms on games and other pirated software."

Vince nodded. "I'm aware of that. And clearly such methods are not beyond the kinds of threats we worry about. What does your team advise?"

Reuben smiled. The sense of panic he had been feeling just two minutes ago entirely evaporated now. "Well, the ease with which we found these problems tells me there are larger issues with the code. I think DoJ should go back to the vendor and talk to them. They deserve a chance to fix things, obviously. But by the same token, unless we got very, *very* lucky

and found the only two problems inside of the first day we tried, this software is full of holes. Perhaps they could do code review and straighten it all out in time, but I have to doubt it."

Vince nodded. "Alright then, we'll do that. While we are in touch with the vendor, it doesn't make much sense for you to keep poking around at the software. If they do code review, they'll probably end up fixing lots of the things you find, and might introduce some new issues."

Reuben thought about that for a minute. "Hmm. Frank," he asked, turning to MadFast, "How likely do you think it is that we might miss something if it's in an area we've already covered in the software?"

MadFast got the point of this. "I see where you're going. We could find things that are broken now, but won't be in the next build of the software. And there may be things that are only broken in the new build, but that we might miss because we already checked for them. Ah, that's a hard thing to be sure about. On one hand, we've been documenting everything pretty well, but this work can get a bit repetitive and I can see that happening. But at the same time, we should go over the software more to be familiar with it. Perhaps we can refine our methods a bit, and save time down the road when the new build comes out. I'm only going to be here for so long."

Reuben nodded. "Got it. That makes sense to me too." He turned back to Vince. "Okay, we'll develop our methodology a bit more, but stop testing per se while the vendor decides what they want to do. I trust you won't accept the software in its current state?"

Vince shook his head. "Absolutely not! We're as eager as you are to have a secure implementation here. Oh, and the boys at ZFon will probably want to have a look at what you've found. I'd like it if you set up a meeting so they could drop in and see it first-hand.

"Okay. Let's handle it like this. I'll call ZFon personally and talk to them. Write up exactly what you've found so far, and send it to me. They may want to see it themselves first, but I'll make it clear to them that they have to fix it. You don't mind them coming by and taking a look, do you?"

Bob answered this one. "That won't be a problem. I understand that software vendors can sometimes suffer from a case of denial about problems in their work."

Vince nodded. "Exactly. Just be nice to them, and try to remember that we're all on the same team here. They'll fix the problems; they won't have a choice. We absolutely cannot use ZFon's product as it stands today."

Reuben nodded enthusiastically back. "Of course."

The meeting concluded after a few other points, and the same repetition took place as they all turned their badges in, and went back to the parking lot to get in the car.

"I think that went pretty well," offered Reuben once they pulled out of the parking lot.

Bob responded first. "What just happened?"

Reuben smiled. "Well, apparently the two guys without names didn't want to make a decision one way or another. I can't guess why. But thank God Vince came in and spoke his mind. Otherwise, they might be setting the damned thing up no matter how awful it might be."

MadFast exhaled sharply. "Yeah, no shit! I almost lost it. I mean honestly, just what the hell would need to be wrong with it for them to do something? What's the point of even testing the software if they won't care?"

"Maybe they didn't quite understand what we were talking about?" Reuben suggested.

"Or more likely they're on the hook for a deadline that they're going to miss because of this," said Bob.

"Hm. I hadn't thought of that," Reuben considered. "That might make things a bit tricky. It puts the objectives of ZFon in line with that of the client, potentially. How bad could it be if they miss a deadline or project milestone?"

Bob thought about it. "That depends. It could be that this is part of…what I mean is, from the way they were speaking, it sounded like the VPN was part of some bigger project. And it sounds like they need the VPN to finish the project, if I understand everything correctly. A lot of their traffic would be carried by this thing?"

Reuben responded, "Oh, I think that all traffic between remote sites would be on it. So all the field offices, including anything overseas, would depend on it for communications. But isn't that all the more reason to do it right? I mean, if all their traffic between dispersed geographic locations

would pass through the VPN they implement, why use an insecure one? Why put all of your eggs in the wrong basket?"

"That all depends on whether or not you realize just how wrong the basket is or isn't. We don't know what their backgrounds are. Maybe they don't understand." Bob was very good at pointing out that not everyone in the world was a computer geek. It was a very necessary thing from time to time.

"Well, whatever the reason, I'm just really glad that Vince showed up, and that he was able to set the tone differently. When do you think ZFon will want to come by?" Reuben was eager to move forward again.

"We'll see. I don't think they'll wait too long," Bob predicted.

Reuben suddenly realized something. "Hey man," he said as he prodded MadFast from the backseat. "You'd better come up with a slightly different version of the tool you wrote. We should use something that doesn't seem so sardonic."

"Right on."

Chapter 5

ZFon Vulnerability

Washington, DC: Friday, November 2nd, 2:47 PM, 2001

"Are you sure you set it up right?" John was one of the ZFon programmers, and already Reuben didn't like him. He tried to remember that this was a guy who was being told that his work wasn't good enough, and now his company either had to fix the mistakes or probably go out of business. But there was something more than that, some kind of arrogance behind it all that Reuben perceived. It wasn't just that he was on the defensive because of the situation, he actually seemed to think that he was the only person in the room with half a brain. *Boy, is he in for a rough time,* Reuben mused to himself as he smirked internally. "Well, why don't you take a look at it and let us know?" he suggested.

John sat down at the server and started looking over various configuration options. "It…it looks pretty standard. Did you harden the operating system?"

"Why would that have an impact on whether or not excessive data sent to the VPN server blows it up?" countered MadFast. He didn't seem to like John either.

John shrugged. "I dunno. Okay, let me see the problems."

"Let's reboot the server first, so it starts up clean," suggested Reuben. He triggered a restart, and they all waited in uncomfortable silence as the system restarted. The beep of the machine and subsequent grinding of its hard drive was the only sound in the room. *Why does it have to be like this?* Reuben wondered. *Why can't all programmers want their code to be secure, and welcome opportunities like this?* He wondered how to communicate to this man that they were not out to get him.

It had taken days for ZFon to send someone. It seemed that they were either in total disarray and paralyzed by the news or they were stalling. Either way, it had burned up a lot of time while MadFast, Bob and Reuben waited for them.

The server finally finished rebooting, and they watched the drive light flicker on and off as services started. When it finally stopped and it was clear that the dreaded error message about some drivers or services failing to start was not going to appear, Reuben hit **Control + Alt + Delete** and logged in. "Alright, I'm going to pull up Task Manager so you can see what's running in real-time." He brought up the process list, and then turned to MadFast. "Alright, hit the overflow first."

"Right on." MadFast fired up the exploit tool, and loaded the appropriate payload. "Ready."

Reuben nodded. "Watch the process list," he instructed John. "Alright, Frank, hit it."

MadFast hit the new and more politically-correct **Send** button on this version of the exploit tool. As expected, the number of processes dropped by one.

"Go on, look around the system. If there are any error logs we missed, we'd love to know. But nothing shows up in Event Viewer, even though the Listener service has totally died. Check it out."

John sat down, and looked at which services were running. "That's odd…this service isn't supposed to even run if that one isn't…hmm." He poked around a bit more, and then opened up Event Viewer. It was as though he didn't believe that it could be true. But sure enough, not a trace of an error existed. Reuben was glad he made sure that Windows was working perfectly on this server before they started work. "You're right."

"Is there some other logging somewhere else?"

"Ah, no. We rely on Event Viewer. That's what Microsoft directs."

MadFast piped up. "Yes, we know. We were just wondering if there was any trace of an error somewhere that we missed."

John didn't seem to be enjoying this. "Okay, show me the other one."

"Want to reboot the system again, or just restart all the ZFon services?"

John grumbled, and shut down the remaining running services, then restarted them in the proper order.

Reuben instructed MadFast, "Alright, you know what's next."

MadFast loaded the second payload. "Ready."

Reuben brought Task Manager again, but this time he set it with the **Performance** tab prominently displayed. "Okay, let it rip."

MadFast hit **Send** again. "Alright. Let me know when to disconnect."

"In just a minute." He turned to John, "Now you see, everything is fine right now. Watch this. Frank, disconnect."

Frank shut down the exploit tool. Instantly, processor utilization soared on the server, and stayed full-on at 100%.

"Isn't that the damndest thing?" asked Reuben.

John was fascinated. He leaned in, and got Task Manager switched over to the Process List. "Hmm, everything is still there."

"Yeah, but it's choking on the data. We think that what happens is it fills a buffer, and then tries to process it when the connection terminates properly, or improperly, as it turns out. But it's got bad data, so it just plain pukes on it. But the odd thing on this one is that it takes not only bad data, but a lot of it, too much. But the way it acts, I don't think it's an exploitable buffer overflow, not for gaining root."

John nodded, deep in thought. "Yes, that makes sense to me. I think I remember some of that code too." He was at least getting curious in that geek sort of way now, and that helped him find some common ground

with MadFast and Reuben. Reuben liked to believe that deep down all true geeks were driven by similar things, like a thirst for knowledge and desire to see how things work.

"Any other questions?"

"Ah, yes. Can I get a copy of those packets that you're sending?"

Reuben looked at MadFast, who shrugged, not having any idea. "I didn't think of that. Damn. The only thing I worry about is that we're essentially not supposed to tell anyone anything unless it's been cleared by DoJ. I don't know what they want us to do in regard to this. Let me call them and ask, and as long as they say it's okay, we'll e-mail them to you. It's kind of late in the day, so I don't know if we can get…here, hang on a sec." He pulled out his cell phone and called Bob upstairs.

"Hey, yeah it's Reuben. ZFon wants a copy of the two packets, but I'm not sure if that's covered by our NDA or not. Can you call Vince and get a go-ahead for us? Great, thanks." He closed the phone and put it away.

"We'll either have an answer right away, or tomorrow I think. Vince has been pretty good about responding, so far. I'm sorry, but I really want to make sure we do this by the book."

John didn't look happy about this, but didn't have much of a choice either. "Okay. I think I have everything I need."

"Cool. And hey, if you need anything else, or have questions, please call us. Even if we have to get permission first, we'll do anything we can to help. I know it seems uncooperative, but we have to abide by the NDA. Really sorry about that." Reuben could tell that this wasn't going to be credible, at least not at the outset.

John grunted, nodding his reluctant understanding and acceptance of the situation. "I'll talk to you later, I guess. Time to get back to the office."

Reuben walked John out, and returned to the lab. MadFast was playing around with some code.

"That went well, I think," he observed. "At least it didn't break down into an argument over whether or not it was borked at all."

Reuben nodded. "Well, what was he going to do, deny it? He saw it with his eyes, that it blew up. I'm betting that they want the payloads so that they can reproduce it on their own system and be sure. You know, I just don't get why it has to be so uncomfortable. I don't mind it so much

when people point out where I need to improve on something. Well, I mean, I mind it, sort of, but it's less painful to accept and work with than it is to just resist it. And I didn't get here by avoiding the truth, no matter what it meant."

"Well, it's a coder thing. It's your work, it's a part of you. So it becomes kind of personal when someone else pokes holes in it."

Reuben shrugged. "Oh well, we were as nice about it as I think we could be. I just hope we can get quick decisions from DoJ on things, so that he won't feel like we're freezing them out."

"Don't sweat it, man. Bob's a good guy, and so's Vince it seems. And John will see that nobody wants to freeze them out here, in time."

Reuben smiled back at MadFast. "Right on." He smirked.

MadFast laughed. "Hey, now you're stealing my lines…"

Washington, DC: Saturday, November 3rd, 1:24 PM, 2001

Reuben considered it his duty as a Washingtonian to make sure that MadFast saw the National Air and Space Museum before he left. As a child, he'd come to DC on many occasions when his father took business trips here for conferences, and he had pleasant memories of walking through the inside of Skylab, eating dehydrated ice cream, touching the sample of moon rock, and looking up at the Wright Brothers' airplane during those trips. Being a fellow geek, MadFast found the museum quite interesting as well.

"Wow. Look at this!" He was awed by the presence of actual air- and spacecraft that had made history. They stood before the heat-scarred underside of an Apollo re-entry vehicle, looking up at the honeycombed blackened surface that had been into space and back.

"It's kind of like looking at something holy, isn't it?" Reuben always felt a sense of being humbled by the achievements contained within the enormous building. It was one of the very few Washington museums that he still visited from time to time. The impact never seemed to wear off.

"Yeah, I see what you mean. To look at it, and know where it's been, to think of the history…wow."

"Oh, you haven't seen anything yet. This is just the start. They have an entire duplicate of Skylab here, and you can walk inside it."

"Really? Right on! Where's that?"

"It's behind us, and to our right. Oh, how into planes are you? Do you know who Burt Rutan is?"

"Ah, no. Should I?"

"Probably not. I'm a big fan because growing up I read about some of his planes in National Geographic. Well, he designed and built a plane that flew around the world without landing or refueling once, called Voyager. The plane is here now."

"Right on! Where's that?"

Reuben smiled. "Turn around."

Reuben, Brianna and MadFast swiveled around, and looked further into the museum. At the far end of the chamber they stood in, they saw a long wing stretch from one side to the other, suspending a thin triple-fuselage between. The middle fuselage, which clearly held the cabin, had propellers both at the front and back of its cigar-shaped body.

As they walked toward it, the true wingspan of the craft became clear, and they could even make out scratches from flying debris, and the scraped ends of the wings. A few wires still stuck out of a hole at the end of one.

"What did that?" asked Brianna. As a native Washingtonian, she had only been to the museum once before, years earlier. One of the peculiarities of the city was that for all its monuments, museums and other spectacles, most native residents only saw the sights when they had guests.

Reuben grinned; he knew this plane well. "Well you see, the plane is made of composites. Rutan is into composites in his designs. Anyways, the plane, as you can see, is flexible. During takeoff, the wings actually drooped so low that the tips were dragging on the runway. The wings are supposed to have wingtips to catch the turbulence coming off the underside and getting a bit more lift, but one of them came off during takeoff, and the other one was damaged. During the flight, they performed a maneuver to snap the damaged one free, so that the plane would have more even trim."

They turned, looking along the underside of the plane. "Amazing," commented Brianna.

"Come on, let's see some more things," prompted Reuben. "Ready?"

The other two nodded, and they followed Reuben down the long wide hallway (if you could call such a huge space a hallway) towards some of the exhibits.

Reuben was still thinking of work as they walked. "MadFast…how long do you think it might take to write an exploit for the buffer overflow we found?"

"I don't know. Not too long, I've practiced them before. I also coded a few during CTF. Why?"

"Just in case ZFon tries to deny that it's exploitable. We'll have to prove it. I'm not thinking of releasing the exploit itself though."

"Right on."

Brianna jumped in. "What exactly is a buffer overflow? I know they're bad, but exactly how do they work? I never knew, and nobody could explain it to me."

Reuben had always tried to come up with a good way to explain how an overflow worked, but never succeeded. He guessed it was time to try again, however.

"Alright, I'll take a shot at it. First off, some basic ground rules of life inside a computer. Imagine that we're bits of code inside a computer's memory, right now. This building is the memory, and everything has to fit inside it. With me so far?"

"Sure."

"Alright. Inside a computer, however, things don't get pushed out of the way. In reality, two objects cannot occupy the same space at the same time, obviously. This is because they have mass. But you know what? Data has no mass. If one of us walked into the other, one of us would overwrite the other. If you drop a ten-ton weight, it doesn't squish what it lands on, it replaces it. This is the hard thing to keep in mind, but it's the key to how an overflow works. Follow me?"

"I think so. Go on."

Reuben continued. "Okay. Let's say that that security guard over there is a trusted process." Reuben pointed at the guard by an x-ray machine. "And of course, when someone comes in with a package, a large bag, whatever, they have to hand it to him so that he can examine it. Now

remember, the security guard isn't just a bit of software, he's a bit of software with more rights than most of us walking around. And all things in here are data. People are programs, and the things we hold are like raw informational data, like word processing documents or e-mail."

"Okay, got it."

"Keeping in mind that data doesn't push other data out of the way, but rather just replaces it. What happens if the next guy to come through that door doesn't hand the security guard a normal-sized briefcase, but instead drops a ten-ton weight that he's carrying with him?"

"It'll erase him, and there'll be a big weight standing there?"

"Right. In that case, the guard is gone now; the software stops functioning. But what if it's not a ten-ton weight, but another person?"

Brianna smiled, catching the connection. "Oh! He'll replace the guard."

"Exactly. Now here's where it breaks down a bit. Basically he'd have all the rights of the security guard, despite the fact that as I described it, all the things that give the guard power would be destroyed along with him. Software doesn't have things like badges or ID cards for running processes, not in most systems. So it is more based on where the guard is standing with relation to the x-ray machine. So in that case, the person who just came in has gained access equivalent to that of a trusted process.

"So, to wrap it all up, there was a program there, the guard, who accepts input. Get it to accept too much input and it overwrites things. Do it the right way, and you'll overwrite something that has a lot of power, so you can assume that power for yourself. That's a buffer overflow."

MadFast smiled. "Nice."

"But why's it called a buffer overflow?" asked Brianna.

"Simple. The data that comes in goes into a little space of memory set aside for it. That space is called a 'buffer'. When you put more data in than the buffer can accept, it overflows over the boundaries of the buffer and overwrites memory next to it."

"Ohhh, I see. That makes sense. Now, you two are talking like it's an even worse thing than normal that there's a problem like this in the software you're looking at. Why is that?"

MadFast answered this one. "Well, ya see, there are a few reasons. Or a couple, I haven't listed them yet, and whoever said programmers could

count…anyways, reason number one is that the application will always be accessible from the outside. It's bad enough when there's some vulnerability in a piece of software that would typically be inaccessible to the outside world because of a properly configured firewall, but in this case you can't hide it behind a firewall for safety. It has to be visible and accessible, since that's largely the point; it's meant to allow remote users access the network securely, no matter where they may be. Another problem is that it's security software that is designed to both keep secrets secret, and enable privileged access from the outside. There's a lot of trust in that, and if someone can break it you have to face all sorts of threats above and beyond someone just taking control of the box and using it to probe deeper into your own network. Also, since it's a VPN, it will have more access to things on the network. A web server on the DMZ won't necessarily be allowed to talk to many devices on the private network behind the firewall, but the VPN server *has to.* Otherwise, the users of the VPN can't get to the resources they need. And last but not least, the client has a rather large number of enemies, ranging from script kiddies to huge drug cartels. There isn't anyone in the world who wouldn't try to break in and fuck their shit up."

Brianna nodded. "That makes sense. Wow." She smiled at Reuben. "I don't know how you handle it. You two just seem so cool about the whole thing. Aren't you nervous or stressed about this? You know the stakes, but it doesn't seem to bother you?"

Reuben shrugged. "What choice do we have? The way I think about it, it's the same work and the same issues regardless of who will be using the software. I focus on the tech of it and don't dwell on the other stuff until it's time for the meetings. All it does is take everything else I do and magnify it, but it doesn't change what I have to do, or how I have to do it."

Brianna grinned at him. "My little super-geek! I'm so proud of you."

The three of them had come to a stop, distracted by the conversation. MadFast suddenly looked up, and his eyes widened. "Whoa! It's huge!"

Reuben smiled, remembering that he reacted like that too once. "Ah, MadFast, meet Skylab. Let's go in!"

The three of them grinned and started towards the stairs to get up to the entry point of the space station.

Tagig, The Philippines: Sunday, November 4th, 7:05 AM, 2001

Agpalo was very serious, but in a strange sort of way. It was intense, but profoundly calm at the same time. Lualhati was dying to know what he wanted to talk about, and what had gotten into him. Why had his angry demeanor softened, and where had he been spending his time? What had changed? It made no sense to Lualhati that as Muslims became even more despised and persecuted, he would become calmer. Did he have some new outlet for his frustration? Lualhati was about to find out.

"We have been friends a long, long time now. We stuck with each other when nobody would talk to us. When nobody could be trusted. You know that, right?" asked Agpalo.

"Yes, I remember. What is going on? It's as though there's a distance between us now, and I don't know why. What's happened to you?"

Agpalo smiled. "Yes, I know, I've been keeping a secret from you. And I am sorry for it. But that is about to change. I wanted to wait to be sure for myself before I told you about it. I didn't want to put you at risk until I was sure it was worth it. I am deeply sorry, and only ask that you understand why I did so, and forgive me."

Lualhati was starting to worry a bit now. *Protect me from what? What is all this?* His mind reeled with all this, and he wished that it would be over. "Of course, of course, but what is it you're going to tell me? I cannot stand this talking around the subject. Just say it already. What's going on?"

Agpalo nodded. "I have found something wonderful, and I want you to be a part of it too. I have been asked to join Ibn Kelbeh! And I have told them about you, that you can be trusted. And I want you to join with me."

Lualhati's eyes widened. This was far from what he had expected. *He's been meeting with them?* It did explain some things, perhaps. Agpalo always wanted to be part of something, but nothing ever seemed to want him. It seemed to be good for him, but Lualhati wasn't so sure about the whole

thing just the same. Could it be that perhaps they weren't so bad as the government said? "I…I don't know what to say. What are they like?"

Agpalo smiled softly. "They're not sadistic terrorists like the newspapers say. They're just Muslims who want freedom to be Muslim, to follow the teachings of the Prophet, and practice Islam. They've been forced to do the things they have done. They are freedom fighters, not murderers."

Lualhati took a moment to absorb this. Agpalo had indeed been his friend. Perhaps he was a bit hot-tempered at times, yes, but always there for him. And he'd never done anything to hurt him, nor had he ever really been wrong about things. Here it was again, how he looked into this group, withholding the knowledge of it from Lualhati until he was sure it was the right thing to do. Agpalo was looking after Lualhati once again. *I should trust him,* he thought. This was a lot to deal with, but Agpalo had always watched over his shy friend.

"You do seem much happier. Calmer, maybe. How is that?"

"Ah, yes. I know what you mean. I have found peace. Ibn Kelbeh, they know the true word of Allah. And in this truth I have found new hope."

Lualhati ached for some semblance of peace. Some certainty, some hope, some thing to look forward to, or at least cherish. This locked it in for him. "Then I will trust you, my friend. My answer is yes."

Washington, DC: Sunday, November 4th, 6:07 PM, 2001

"So, what shall we have for dinner tonight?" asked Reuben.

"Hey man, whatever is fine with me. Everything has been great, I trust you. Just nothing *too* weird. Brianna's told me about your love of dangerous sushi."

Reuben chuckled. "Ah yes, the fugu. Fear not, I don't think it's even in season right now. There are only a few weeks a year when it shows up on the menu." Reuben was adventurous with regard to food. It was perhaps more accurate to say that he was extreme, being willing to try almost anything once. He'd eaten fugu, also known as blowfish, on more than one occasion. The thing about it was that if it was prepared incorrectly, the neurotoxins contained in much of the fish would contaminate the edible

parts, and the diner would not survive to the end of the meal. The flavor was subtle, and something he enjoyed quite a bit. He knew Kenji-san, the owner of the restaurant, and that if he was still alive and kicking, the fugu was still being prepared correctly. There was no doubt in his mind that Kenji-san looked forward to the arrival of fugu each year more than Reuben did.

"Well, we haven't had Chinese food in over a week. How does that sound to everyone?" Brianna suggested.

Reuben looked at MadFast, who looked back. "Sounds good to me," MadFast said in reply to the unspoken question.

"Okay, let me grab the menu!" Brianna cheerily went off into the kitchen to look in the cache of delivery food menus for the right one.

MadFast and Reuben looked at each other, both thinking about the same thing…work. "Do you think we'll get anything to go on tomorrow?" asked MadFast.

"I don't really know. I hope so. I want to finish this project. Who knows what's going on right now? But I don't know what else to do but wait. Maybe they've been working on it over the weekend."

MadFast snorted. "I damned well hope so! They've got a buttload of work to do if they want to fix that thing and keep the sale. It won't happen overnight."

"Might it not happen in time no matter what?"

"Maybe. But there's no way we can tell one way or the other."

Reuben pondered what might be going on at ZFon at that moment. "Hmm. And if they don't have our payloads to test, they might not be able to tell exactly what's broken. So they either have to fix everything they can find in that section of the code, or they might miss what we found. If they come back to us with another build and it's still broken, then they're probably screwed."

MadFast drew the connection. "And that's why DoJ didn't want us to give them the payloads. Clever. I didn't catch that before now."

"I'm thinking Vince is even cleverer than we thought. Which is good, since it seems he likes us and how we're doing. I don't think I'd want to be on the other side of that coin though. But I wish he hadn't put us in the position of telling them no when they wanted to see what we used to

bork their software. I felt like such a schmuck having to tell John. You just know they think we're trying to screw them."

"Yeah, no shit. But what can you do, huh? I mean, it's the client's wishes. And it does make sense, in a way."

"True enough. But I also wonder what the deal is with that. Do they not trust ZFon to fix it? If so, why are they even considering their product anymore? What's the deal with that?"

MadFast shrugged. "Maybe it's too late for them to choose someone else at this point. Who knows? It's that whole thing the guy was talking about before, about a 'bigger picture'. I can't guess what makes sense about using an insecure product, but whatever."

They noticed that Brianna had long since returned with the Chinese restaurant's menu. She'd been standing there, quietly listening to them talk, fascinated. "Should you guys be talking about this now?"

MadFast looked at Reuben for an answer. Reuben replied, "We can trust her." He looked back to Brianna. "But are you comfortable with being trusted?"

Brianna fidgeted a bit. "That's a good question. I love hearing you talk about this stuff, but I worry if you say too much in public. I don't want you to get in trouble."

Reuben weighed this in his head. He liked exposing her to new things He liked the notion that in being open about his work, or at least the concepts within it, he helped expand her professional knowledge and broadened her horizons. He felt a profound sense of gratitude toward all those who, in sharing their knowledge with him, gave him the tools with which he built his mind and his career. And nearly deified amongst these was Mr. Donegal, who started it all those twenty-one years ago.

"Man, this is hard. I really want to share with you. But I don't want to make you uncomfortable. How about this: we'll make our discussion a bit more hypothetical to make it easier for you to bear, and you let me know if you're uncomfortable. But one thing you must remember is that even as we strip off the details, what we talk about is to be kept secret. Once let out, information cannot be put back."

Brianna thought about this, nodding as she considered it. "Okay, I think that will work."

MadFast relaxed, glad that this moment had passed. He hated to feel like an intruder, and felt like he was intruding just now. Reuben smiled. "Good, then. Let's order dinner."

Washington, DC: Monday, November 5th, 9:45 AM, 2001

Reuben brought both cups of coffee into the living room. "Here ya go, man," he said as he slid one of them over to Frank. It was the standard morning for both of them now before starting work; MadFast came over and they discussed their plans for the day while having coffee. After that, they'd get into the car and jet over to the office.

"So, what are we going to do today if DoJ hasn't got any news for us, and ZFon hasn't got a new build or software patch yet?" Reuben was keeping an eye on the calendar, and the time that MadFast had available to work on this was ticking away. He was nervous about the past couple of business days having been spent without any significant work being done. "I want to work on an alternate plan. I don't think ZFon is going to have anything for us this week, and I don't think that Vince will either. So we're basically billing DoJ for our 'sitting around waiting', and then when we do have to resume, we'll be out of time. You'll have to go back to Seattle and catch up on your project work there. And I know I've said this before, but we really need you here to finish this. So how can we work this out so that everyone gets everything they need?"

MadFast sat back, sipping the hot coffee. "I think I can get some of my project work done this week while we have downtime. How about we don't bill DoJ for that time, and I'll be billable to my regular client instead?"

"That's a start, but what about the expenses? DoJ will still be paying per diem and lodging."

"True. But I'm also sitting put without anything else to do because they want me to. This way they can have what they want without putting me in a bind. And it'll be cheaper for them than what they're getting now."

Reuben thought about that. "That makes sense. Why don't you talk to Bob and we'll see how they feel about it? From what little I've seen, it looks to me like government contracting is full of crazy details and regulations, and I want him to make sure there's nothing wrong with trying to work it out that way. I'm glad I haven't had to get involved in those details, to be honest."

"Right on. I don't blame you. That stuff looks like a total nightmare. Your tax bucks at work, man!"

"Yeah, I do wonder if it ever reaches the point where the cost of the effort of keeping the costs down ends up costing too much. At what point does it become self-defeating?"

MadFast laughed lightly. "It's not like we'll ever know. No sense trying to figure it out. It's just how it is."

They downed the rest of their coffee and grabbed their stuff. Minutes later they were listening to music in the car as Reuben worked them out of the city.

"What do you think of this?" asked Reuben, referring to the music that was playing.

"I like Linkin Park. It's kind of like a little bit of hip-hop, a little bit of metal, and a bit of electronica. It's nice to hear something different getting airplay for a change. I'm sick of the skate-punk music that's been barfed up by every station."

"That's a good way to put it. Yeah, I like the eclectic nature of it too." He shut up and continued listening to the album.

Several tracks later, they pulled into the parking lot and parked. Well-used to the routine, they were upstairs with their gear in no time flat without even thinking about it. They started to boot everything in the lab, then went upstairs to see Bob and check in.

"Hey Bob, we're here. Hear anything yet?"

Bob looked up at the pair. "No, not yet. Eager to get back at it?"

"Hell yeah," answered MadFast.

Reuben took over. "We came up with an idea. While we're waiting, DoJ is paying for both of us to just sit around, on top of Frank's expenses. And the clock is ticking down, because he has another commitment on hold while he's here. What if we could take them off the hook for his

hourly rate while he's here, and he works on the prior commitment? That way he's on hand when they're ready for us to resume, and he can buy some time to be useful when that time comes."

Bob sat back. "That's not a bad idea. I'll have to get them to go for the expenses while he's here, but I think they'll go for that. It beats paying for him to do nothing, and it wouldn't be any more than they'd pay for expenses. Hell, they'll save on the overall tab. It means we might get paid less, but it lessens the risk that we'll run out of time and end up underserving the client."

The pair nodded back to Bob. "That's pretty much what we thought," replied Reuben. How do we go from here?"

"Well, since we're just on hold, why don't you just start today? I mean, I need to call Vince first and get them to sign off on it, but why don't you work on your other project, Frank, and if they go for it we'll make it effective as of today. If they don't, then you get to do a few hours of work anyway and I won't tell."

Reuben smiled at MadFast. "Great, now what am I going to do while you're busy again?"

MadFast laughed. "Practice management skills?"

Reuben laughed back, play-punching him in the shoulder. "Shut up!" He turned back to Bob. "Alright, so we'll work like that, and let us know what Vince says. Talk to you later."

Bob nodded and picked up the phone, dialing as the pair left.

Tagig, The Philippines: Friday, November 9th, 10:32 AM, 2001

"Don't you see, friend? There is so much we *can* do to help," said Lualhati.

Agpalo smiled, remembering yet another reason why he wanted Lualhati to join him at Ibn Kelbeh. "You were always smarter than me about such things. I never see the larger picture like you do. You're right. We can hit the Americans very hard from here. But we need to be careful, and not get caught. And I don't know how we can do that yet."

Lualhati smiled back. "It won't be so hard. The Internet cafés are everywhere; we can use them. I'm sure our brothers would help us with this if they knew what we could do for Islam."

Lualhati, although hesitant and nervous at first, had fully committed himself to Ibn Kelbeh after the initial contact. The degree to which he simply seemed to let go and place his fate in Allah's hands surprised Agpalo. It was good to see him being so much more comfortable now, less timid. Perhaps all he had needed was a place that felt safe. And already he had a fantastic idea.

"The hard part," he continued, "will be figuring out how to hurt them. This will not be simple. And we will need to prepare very carefully. We must not exploit anything we find until we can *truly* exploit it. We must not expose ourselves or our plans before they are ready."

Agpalo nodded. "Of course, for our own safety."

"Yes, but also so that they do not see the attack coming until it is too late. We can always hide our tracks in various ways, but if they realize they have a weakness before we take advantage of it we may fail."

"How can we hide our tracks? Besides the cafés, I mean."

"Well, that is simple. We don't attack directly. We hack other systems, and use them. It will take planning, and a lot of work, but such is the way of the holy, no? And we can enter paradise after living long happy lives. First, we must practice. We will start small, in small ways. And we will learn. Once we learn, we will teach others."

"Teach others?" Agpalo didn't know how he felt about that. He thought of this as something just for him and Lualhati alone.

"Yes, brother. We must have some help. You and I will direct everything, but this will be a hard job to do by ourselves. America is not weak, nor is it stupid. Two boys from Mindanao cannot do so much harm just by themselves. We must be smarter than that."

Agpalo nodded. "So how do we start, exactly?"

"Do you remember when we wrote that virus? We must get better at it. And we must learn how to break into systems."

Agpalo sensed more than just a start in Lualhati's mind. "Then what?"

"Ah, you're in a hurry. You must relax. First, we must get approval and know that we will have help. We will need people we can trust, and a

small amount of money, for the cafés. It is not enough to be safe later. We must be safe and careful from the very beginning, and so we will start using shops with Internet access, and only with the help of our brothers. You must remember that large success later is better than little or none at all now."

Agpalo nodded, taking a breath. Lualhati had always been the quiet one, and patience must have been a part of that. "Of course, you are right. I just want to know where this will lead. What do you have in mind?"

"Very well. I understand that websites are easy to break into, so that is where we will begin. Nothing large, and certainly nothing in this country. I will show you how to find web servers that are not part of a large group, but just belong to small companies. You see, brother, you learned how to program better, but I learned more of the networking. It is simple, you will see. The small companies we hack won't be able to do much to find us, so we will be safe. It is only when we move on to larger prey that we must be more careful. But by then we will be more skilled as well. We must make our first mistakes in small places, and in small ways. But there is one thing left I have not yet figured out. I do not know exactly where we will focus our efforts. We need to choose a target more specific than just America. Though, I do not know exactly what we will target."

Washington, DC: Friday, November 9th, 11:23 AM, 2001

"Wow, this was really quick to set up. Are we really done?" asked Tom. He logged out from the system and started straightening up.

Tom was a contractor, one of many that worked on DoJ's IT infrastructure. He'd never set up one of the ZFon systems before, and was learning on the job from Jane, who had been trained on it the week before. "Yeah, wasn't that easy? I told you it was a cakewalk. I see why they chose it. A monkey could do it," replied Jane.

Tom laughed. "Isn't that what we contractors are? Just scumbag contractor monkeys?"

Jane giggled. "Yeah, but we get paid more, don't we? I wonder why *that* is."

"Oh, maybe because we're here to do the things that the real federal employees can't accomplish?" he countered sweetly.

Tom and Jane were a bit of an item in the office at the DoJ. While both of them were excellent at their jobs, they paired up in a flirtatious sort of way practically the first day they worked together. Nothing ever really happened between them but coy sparring and genuine friendship, but among the dry atmosphere where they worked their style wasn't exactly in harmony with the surrounding culture. But they were also talented and necessary, and watched each others' backs, so in time they came to be accepted as necessary, if risqué. Neither of them seemed to hold the skills of federal IT employees in much esteem, which both increased the friction and helped facilitate their "them versus us" mindset, which helped them bond together to survive the office politics. Contracting for the Federal government was often a situation where people did not want to listen to the truth, and you could get fired for the most asinine things.

"So they're setting these up everywhere I hear," mentioned Jane. "There was some kind of big stink about it too. I think the deal was that this is way past due or something. There's some kind of huge row that broke out over it."

"Really? I didn't hear about it."

"Yeah, it was something way high up, I heard. That's why nothing of it happened around here. It didn't involve us in the trenches here, just the big brass. Oh well, not our problem, and at least it's getting set up now. These VPNs will connect all the field offices, plus liaisons with all sorts of other organizations. It's pretty wild, really."

"And all those connections end here?" Tom wasn't thinking entirely of work at the moment. In his mind, this task was done, and so his focus went out the window.

"Well, this one will handle the people in the field, with laptops. There's another one we'll be doing tomorrow…jeez, don't you read your e-mail? The one tomorrow will connect to the field offices. And there's another one after that for other agencies, so they can link to us." She playfully batted at him. "I swear, I don't know what to do with you sometimes. What would you do without me?"

He laughed. "Oh, probably go into consulting only to commercial clients. But I'd be bored!"

Jane grinned at him. "Only *you* would say that you'd be more bored doing commercial work. Did you know that?"

Washington, DC: Monday, November 12th, 10:56 AM, 2001

"What!?" Reuben was so shocked, it didn't even sound like a question.

"Yeah, I know. Didn't make sense to me either, Reuben. But it's what they said," Bob explained. "I have no idea why, or who is behind it, but they basically said that you two are to check the new build for one of the vulnerabilities, and then if it's gone, then you're done. The other one will be fixed sometime next month. Beyond that, I don't know what else to say."

This was an entirely unexpected turn of events. "This is bullshit," protested MadFast.

Reuben nodded, but figured that they still had a job to do, and the client determined that job. "So when do we get the new build?"

"Later today, they think. You're supposed to look for the Denial of Service; they said the overflow is something they've found, but they need a bit more time to make sure they fix it right. They promised DoJ they'd have it done within thirty days, so that satisfied their requirements."

"But don't they know that we're not even close to being done at looking for more problems?"

"I told them that, but they didn't seem to care. I gotta tell ya, something isn't right here. I mean, obviously something isn't right, but what I'm saying is that either someone high up is tied to the vendor in some way, or someone has some kind of pull who doesn't know the whole story here. But hey, we have to take care of the client, and maybe after all this we can get it sorted out and have another go at it. But for now, I think if we resist this we won't get anywhere."

Reuben and MadFast looked at Bob, then each other. They raised their eyebrows, realizing he was right. "Okay, so we wait for the new build, and test it," Reuben conceded. It felt like some kind of defeat.

"Was there anything we did wrong?" asked MadFast.

Bob shook his head. "No, I really don't think so, and here's why. Vince was very careful to let me know that you two shouldn't think this reflects on you. I mean, he wasn't overdoing it, he wasn't so careful that I think he was hiding something, but he wanted to make it known that everyone was really happy with the work so far. This is something else altogether, so don't worry, it's not that."

MadFast had another question. "When should I go back on the clock?"

Bob didn't hesitate. "Screw it, go on the clock as of today. You guys have some stuff to do to get ready, anyways, yeah? Like uninstalling the old version? Make sure there aren't any traces left of it, so that you get a good test."

The pair nodded. "Will do," replied Reuben. "But this really sucks. I hate how they're going to have insecure software. Is there anything we can do if nothing more comes of all this?"

"Like what?" asked Bob.

"I have no idea. But something. This is a disaster waiting to happen, and there has to be some way to change it."

"Well, if you think of something let me know. For now, I don't have any ideas, except to see where things go and hope for the best. Anything else won't change their mind, I don't think."

Reuben nodded once. "Okay. We'll get to work, then. No sense getting sloppy now." And with that, the pair turned and trudged off to prepare the lab for testing the new build.

Tagig, The Philippines: Tuesday, November 13th, 7:31 AM, 2001

"Allah be praised, what you are planning is good indeed." Lualhati and Agpalo knew him only as 'Al-Hakim', which they now knew meant "the learned one" in Arabic. "And you are wise beyond what I expected to desire such caution. Wise indeed." He twisted his beard, thinking carefully. Beside him, a hot cup of coffee sat untouched.

"Thank you, Al-Hakim," replied Lualhati deferentially. "I have great plans, but know that we cannot do this alone."

"Indeed, you probably cannot, Lualhati, but you need not try, either. Allah has sent both of you to us, and us to both of you. Together, we will all work and, Allah willing, accomplish the end result of your plan. And this is a sign from Allah, who most of all has sent you to me." His hand went to the side, lifting the coffee to his lips. He sipped the thick sweet liquid, pondering his next words.

Almost nobody knew much about Al-Hakim, and he carried with him a certain aura of mystique. He was a former oil worker who had truly learned to discover and love Islam while working on the Saudi Peninsula. An engineer, but of Palestinian descent rather than a Saudi citizen, he was among the vast class of immigrant workers mostly responsible for the operation of a tiny country's vast petroleum production. Such people, denied citizenship, were not able to share in the wealth, however. While fortunate not to have been cast out as so many were after the Gulf War, he saw how many were not so lucky, and truly grasped the exploitation of his kind. The less lucky ones were unceremoniously driven out after Arafat backed Saddam Hussein, and were cast from a life of some stability to seek a new life elsewhere.

Agpalo and Lualhati tried to figure out what Al-Hakim was getting at.

The cup of coffee went back down, and the man folded his hands together before speaking. "You see, young students, I think that we all together have the knowledge to put together a great plan. You do not know my past; nobody here does. I used to work in the Mid-East, on the oil fields. My profession was in building and maintaining control systems for large tanks, groups of them."

The two young men glance at each other again, now even more confused. Why was he telling them this, and where was it going? They barely knew this wise, respected man, and now he was confiding in them like he had never done with anyone else, apparently.

"You see, these tanks are grouped together in large clusters, often called tank farms. They store diesel, petrol, kerosene, aviation fuel…all sorts of things. They are very, very important."

The pair started to become uneasy, and almost uninterested by this. "Al-Hakim," Agpalo offered, "I mean no disrespect, but why are you telling

us these things? We have no use for this here." Lualhati just kept his mouth shut, as he always did when he felt uncomfortable.

Al-Hakim smiled. "Ah, but you do have use for it. Listen to me. Did you know that the Americans use more oil than any other single country? And that they depend on it so much that their economy can falter if the price goes up too high?"

They shook their heads, still clueless as to the point of this, but at least reassured that it connected in some form to something they cared about. "No, but what does their need of Muslim oil have to do with us? Oil does not come from here."

Al-Hakim smiled, and nodded. "You are correct, Agpalo. But remember, you are hoping to strike at the Americans. What do you think would hurt them the most? What can you take from them that would hurt them so badly that they would not ever forget the lesson?"

"Oil?"

"Yes. But how?"

"I don't know."

"Exactly. But I know. And I'm going to tell you. But I can't do it myself; I need you to do it for me. I don't know computers as you do, and you don't know petroleum facility operations as I do. These tank farms are extremely important. At refineries, they hold the oil and petrol before it goes in tankers. And near cities, the same tankers fill the tank farms, where the petroleum is stored before it is distributed to petrol stations, airports, and similar places. They are a very important link in the supply chain that feeds the infidels of America.

"These places are large, and full of gauges and valves. They are complicated, and difficult to control. If you fill a tank too full, the fuel spills, and creates a problem. Fumes can build up in some of the tanks, and explode if things are not handled correctly. From the outside they look simple, but it takes a great deal of effort, and many people to operate them safely.

"It used to be true that people had to walk around, taking measurements and controlling things. They used radios to talk to each other. But in recent years, computers have taken the place of people with radios. Valves are controlled from afar, and gauges are now computer instruments that sit in a single control room. It is all done with computers."

Lualhati smiled, and Agpalo did a moment later as he too understood where this was leading. "You know what to choose as a target, Al-Hakim…yes?" inquired Lualhati, wanting to be sure.

"Exactly, young student. If we can somehow go after these computers, we can stop the flow of oil to the American infidels. There are problems with my idea, but we are only at the very beginning. Allah will guide us. But as you have said, we must be very cautious, and start in small ways. Of course Ibn Kelbeh will support you. Tell me what you need."

Chapter 6

Scanning the System, 2003

Washington, DC: Tuesday, October 21st, 9:13 AM, 2003

Looking at the front page of the Internet Storm Center was a daily routine, like looking outside to see what the weather was like before going outside or choosing what to wear. From time to time there were interesting things, like a sudden spike in scanning for a service that might indicate that there's a new vulnerability. But this time, it was different. "Upward Scanning Trends: TCP port 1734, unknown." It was the same port as used by the ZFon software.

The Internet Storm Center operated as a free service of SANS, a respected computer security organization and educator. It operated by making available a software client that volunteering companies and organizations could use to submit their logs from IDS and firewalls; these logs contained data on port scans and attempted attacks. By collating the sum of these daily reports from hundreds of volunteers, it could piece together an overall view of what was happening on the Internet. When one company was scanned, it could examine the ISC's data and see if they were being targeted specifically, or if it might be part of a larger effort underway that encompassed the entire Internet.

"Hmm." Reuben clicked on the item, bringing up a chart detailing the activity trend over the past month, listing the sources and total targets of probes. Toward the left, a flat line indicated nearly zero scans, until three days ago, when the number abruptly peaked up to over fifty thousand targets per day, and a few thousand sources. The activity formed a sudden plateau that continued through to the end of the graph, only fluctuating slightly.

What was particularly interesting was that the number of scans wasn't quite high enough to gather much attention in and of itself; it was dwarfed by the scans for certain other ports, for example, and the site's default graph of probes didn't even show it. But the fact that there was any scanning, for an application with no publicly known vulnerabilities, was extremely significant. It meant that someone knew that it was vulnerable, and that they were looking for targets. And what was really scary was that since the volunteers submitting data to the ISC were a definite minority, the amount of scanning going on was at least two orders of magnitude worse than the numbers shown on the graph.

"Dear God."

Someone out there knew, and they were getting ready to attack. They were scanning to find the vulnerable systems. And with so many already-compromised systems from which to scan, they'd find nearly all of them. Hackers, good ones at least, never attacked major systems directly from their own machines. They hacked other systems, like home computers on DSL or cable modem lines, and used those machines to forward attacks for them. Thus, they covered their tracks, as such systems were either properly

secured (and thus not usable by the hacker) or entirely wide open with no logging of any sort. Even tracing back the attacks to these systems resulted in a dead end, since there was no way to figure out where the attack originated. And some hackers with a purpose set up hundreds or even thousands of such systems to use at their disposal for large-scale attacks.

He stared at the screen for a minute, not sure how freaked out to be. *We both knew this might happen, get a grip*, he thought. *This isn't the end of the world, this happens to all sorts of applications and the sun keeps coming up.* He tried to reassure himself, but the truth was, for all the times he'd known of this scenario occurring, it had never happened to him. Then he decided that he was *seriously* freaked out.

Reuben found himself in the midst of a huge dilemma; if he kept his mouth shut, he'd wittingly be complicit in whatever hacking was about to take place. But if he spoke up, he'd probably end up sacrificing himself for the greater good as the DoJ went after him for violating his NDA. And even if he did raise the alarm, the attacker, whoever he was, would still have culled a long list of vulnerable systems; as soon as word got out that there was a weakness, his hand would be forced and the attacks would commence almost instantly. *Goddamnit! This is what we tried to prevent in the first place! Why didn't they just listen to us?*

His hand slowly went for the phone; maybe MadFast had a better idea. He looked up the phone number, dialing it in; he and MadFast almost never spoke voice, instead preferring the asynchronous convenience of e-mail. But in this case, Reuben felt it best not to leave some kind of trail in the wake of their conversation.

"Hello, Frank here."

"Hey man, it's Reuben. We've got a problem, man. Look at ISC's front page."

"'K. Hang on."

Reuben heard the phone shift around on MadFast's shoulder and the rapid tapping of keystrokes, followed by a few seconds of silence. Some clicking of a mouse followed, and Reuben knew that MadFast was most likely following the same steps he did.

MadFast took a deep breath, and exhaled. "Shit. What you're calling about is obvious, I assume?"

"Yeah. Unless there's some other vulnerable app we both worked on that I've forgotten about. I don't know what to do…any ideas?"

"Uh, no. Not right yet."

"Okay, me neither. What the fuck are we supposed to do? If we talk, we get sued big time. And it might not even help! But if we keep quiet, it's partly our fault, whatever happens."

"Yeah, but…yeah. I didn't get into this kind of work to just let shit happen like this."

"The only thing I can think of is to talk to Vince. He's the one guy who's been cool about this, maybe he has an idea. Hell, maybe they'll LET us release now. You think?"

"Ah, right on! There's an idea. At least it won't hurt to talk to him. You want to do it or should I do it?"

"Let me. I've got a bit more insight into where he's coming from at his end. As you've seen, the federal world is kind of surreal. I've got some people here to guide me through it, but you might make some mistake if you try anything, since you don't have any help."

"No shit. Okay, sounds like a plan. Let me know? And don't let him screw us like he did last time."

"Are you kidding? Of course I'll keep you in the loop. And remember, he didn't screw us, he was as much of a pawn in it all as we were." Reuben heard MadFast shrug on the other end.

"Yeah, I know. It just pisses me off. This sucks, we tried to prevent this, and they screwed themselves on it."

"Yes, they did, but now we can help again. Look at it that way, and hang tight. In the meantime, I'm going to try and think of a way to work around the vulns…any thoughts?"

"No fricking way man, there's just no way. You know how it works; it only uses one port. You can't shut that off without making the thing useless. And every service it runs is part of normal operation."

"Okay, that's what I was thinking too. Worth a try at least. I'll call Vince now, and talk to you in a bit. No e-mail on this or anything, okay?"

"Right. Talk to you soon man. Good luck."

As he got off the phone, Reuben felt a bit better. At least he wasn't in this alone. And it always felt better to be doing something instead of just sitting idly while events progressed.

Back in 2001, as it turned out, ZFon had indeed addressed the lower-impact of the two bugs found. And they addressed the buffer overflow as well, only it took them a bit longer than a month. By that point, the software was being widely deployed throughout DoJ, and thoughts of the next version got sidelined in favor of a smooth and extremely overdue implementation. As it turned out, someone's job was on the line for how delayed the VPN project had become, and in an act of personal survival they declared the product secure enough after just the small bit of work Reuben and MadFast had accomplished. They were firmly reminded of their NDA, and not permitted to even disclose their findings after a fix was available for both issues. And the vulnerable version stayed in place at DoJ, liberally distributed throughout their network.

And even worse, after some time MadFast went a bit deeper when he returned home, using a copy of the install files they'd kept for themselves. The buffer overflow turned out to be a root exploit after all, and there was a second one that one of Reuben's untested payloads also triggered. The software was lousy with issues, and they couldn't get anyone in DoJ to return their calls. Shortly after that, Vigility dropped the hatchet on the rest of Reuben's unit, and Reuben just barely got a job working somewhere else in time to keep paying the bills. And over time, he felt more comfortable that nobody else would ever stumble across any of the problems they knew about, and that their worrying would all have been over nothing.

Well, so much for that hope, thought Reuben. Rather than call Vince right away, he decided to stretch his legs a bit and collect his thoughts. He got up and stepped out of his office, going down the hallway to the vending machines. He got a Coke, and stood there for a minute, his mind flipping over the motivating forces at play in DoJ and how Vince might react.

The federal government was notoriously uncooperative with private industry when it came to computer security. On more than one occasion, some kind of organization, task force, or group was created to help

industry, only to ask for information from private companies and not give any back in return. *This could be tricky. I don't think they'll want to play nicely and let anyone else know,* he thought. *Boy, do I wish I could threaten to go to Congress and spill the beans.* One of the nightmares of living in Washington, DC was that for all intents and purposes, you had zero representation in either the Senate or the House of Representatives. Reuben had done lobbying in his college years, and knew how easy it could be to alert a lawmaker to a serious issue, but only if you were one of their constituents.

No, that's not the right way to go about this. If I get confrontational, we lose, just like that. Reuben tried to relax and not react before the fact. *Maybe it won't be so bad, maybe Vince can get it cleared for us to release so we can force ZFon to fix their software. This could turn out to be a good thing.* Reuben felt hollow…no way could this be good. Even if everything followed a best-case scenario from this point forward, thousands of systems would be hacked and their privileged communications violated, at the very least.

Reuben had always hoped that things would work out a bit differently here, and that nobody would ever notice any remaining weaknesses in the ZFon software. It looked like his hopes were not to be, though.

"Hey, you alright?" asked a coworker in mid-purchase of a soda.

"Huh, what? Oh, yeah, I'm fine. Just thinking about something."

"Okay…you looked kind of in your own world for a second, that's all. Sure you're okay?"

"Yeah, just trying to figure out how to handle a client situation, that's all. No big deal," Reuben lied. "Just walking through the options in my mind."

"Okay." The man smiled back. "Gonna finish opening that Coke?"

Reuben looked down He was holding the can in one hand, and had the tab half-lifted with the other, and must have just stopped in that position as his thoughts drifted. Usually, when he was this into his work he was in heaven. Today it was the opposite. "Ah, heh. You know how I get." He finished opening the can and took a hungry pull of the drink.

The coworker nodded and finished his own purchase, waving as he walked off.

Reuben walked back to his office, and closed the door, locking it. He stared at the phone, and decided he'd just call Vince and figure out what he'd say on the fly. This was the kind of thing that could go terribly wrong if one thought about it too much. He sat down and looked up Vince's number in Outlook, dialing the number nervously.

"Vince here."

"Hey, it's Reuben. How are you?"

"Hey! Good to hear from you! What's new? Where you working these days? I hear where you used to be got hammered."

"Ah, I got out from Vigility just before they dropped the bomb on everyone. When I left, they were all saying what a mistake I was making, but a month later I was getting calls asking if there were jobs open where I was. I've got to ask your help on something, though, and it's important."

"Sure. What can I do?" Vince was a nice guy, and easy to deal with.

"Remember how MadFas…I mean, Frank and I warned how ZFon wasn't quite secure still?"

"Yes…" Vince sounded a bit concerned.

"Someone's scanning pretty much the entire world looking for running instances of it." Reuben waited to see how long it might take for the implication to sink in.

It didn't take long at all. "Oh, boy. Hmm. Let me make some calls and see what needs to be done first. I want to be careful so that the wrong feathers don't get ruffled over this, so that we're free to address the situation properly." He was clearly as interested in dealing with this as Reuben was, thank God.

Reuben relaxed, feeling better now that there was a clear road to walk from here. "This can't be a good thing. Whoever is scanning is doing it from a lot of different hosts, which means they've already got control of a lot of systems. If they are looking around like this, they have something large in mind."

"Why don't you think it's more than one person scanning, then?"

"Because what are the odds of hundreds or thousands of hackers simultaneously developing interest in the ZFon VPN on the exact same day?" Reuben had already thought of this.

"Good point. All right, I'll see what the next step is. If anyone asks you anything, play dumb, okay?"

"Will do. Thanks, Vince."

"Don't thank me yet, this could be a mess."

"Yeah, but at least you're trying to help out. I feel safer knowing you're involved, and I know that Frank does too. You're more politically savvy about these things, *and* you're connected in ways that neither of us is."

"Well, if not for you two, we'd have been a lot worse off. I don't see how I could just leave you twisting in the wind."

"And that is exactly why I'm grateful." Reuben smiled into the phone.

"I see, okay. I'll give you a call when I know a bit more. Hang tight."

"Cool, will do. Talk to you soon." He hung up and leaned back in his chair. *I think we're handling this well, come to think of it,* he mused. *Maybe this will be alright after all.* He debated calling MadFast and telling him where things stood. He grabbed the phone and dialed him up.

"Hey hey."

"It's Reuben. I just got off the phone with Vince; he's helping us out. He's calling around and figuring the best way to handle it, and he'll call me back when he knows. He's fully on board, I think, and will help us avoid causing any political complications. Until then, play dumb if any questions come up, okay?"

"Right on. Anything you want me to do?"

"No, just sit tight. We need to see what Vince comes back with, and in the meantime, I've got our backs. I'll let you know when I know more."

"Right on. Talk to you soon."

"Yep."

Reuben hung up and sat back, trying to think if there was anything he'd missed. *Yeah*, he thought. *I miss the days when I was just a geek and it didn't affect anything besides the systems I was directly responsible for.*

Tagig, The Philippines: Tuesday, October 21st, 5:19 PM, 2003

"How's it proceeding, brother? Are we finding anything yet?" asked Lualhati. Agpalo had just returned from one of numerous Internet cafés the pair was using.

"Surprisingly well, actually. We've lost relatively few of the zombie systems. The first set of scans are in progress, and are moving along. We have found a number of vulnerable systems, and it looks like each zombie is only doing a very small number of scans total per day, as planned."

"Good, that way none of them will make enough noise to give themselves away too easily." Lualhati had studied worms, zombies, and bots that had become widespread. He sought to learn what had been done incorrectly, and many times it was merely that the compromised systems started sending outbound scans with such ferocity that otherwise ignorant administrators couldn't help but notice the sudden flood on their networks. Generally, the more savvy the administrator, the less noise the system had to make to be noticed, and the most savvy ones ran IDS and therefore noticed most kinds of scans, if not the original attack itself. This last group of systems is what Lualhati had the least use for.

The plan he had worked out was clever, and rather unusual. Rather than attacking things once and leaving them be, they attacked them twice. The first time a box was rooted, it was set up to do fairly straightforward scans for other vulnerable systems. The vulnerability, whatever it may have been, that made it possible for them to take control of the system was fixed to ensure that nobody else came along to take control of the system away from them. After a while, if the system was not cleaned up or taken offline, it was deemed fit to use and the real zombie was installed. This way, they managed to keep many well-trained administrators from discovering the software that could give away some of their true targets. It had happened before, that an exploit found in the wild became the disclosure of a previously unknown vulnerability, and resulted in the hole being patched. And in this case, they would probably not get a second shot at their targets.

The first target was a large software suite that performed the role of *SCADA Master* in a petrochemical storage facility. The facilities differed

from each other only slightly, and as such were typically created with similar designs and systems. The PetroilSoft SCADACommand application was an industry leader, having been implemented in the overwhelming majority of such facilities in the United States. Unfortunately, it also happened to be fantastically insecure, containing a plethora of remotely exploitable vulnerabilities. It happened to be that Al-Hakim was quite familiar with it, having implemented it several times in the Mid-East.

SCADA stood for Supervisory Control And Data Acquisition, and essentially referred to a broad category of applications and equipment that make industrial systems network-capable. Instead of various controls and readouts dispersed throughout a plant, a master control panel of information and controls can be put in one room, cutting the costs needed to run the plant, and allowing it to run more efficiently in most cases.

Remote units, such as a control servo at a valve or a digital sensor that detected the temperature inside a pipe, were attached to Remote Terminal Units, or RTUs. These boxes in turn were connected to a central network, where the SCADA Master resided. The SCADA Master was the central server-based application that did all the functions of turning raw data into human-readable displays, handling scheduled events, sending alerts when certain values were outside of predefined limits, and so on. It was the brains of the outfit, simply put, and with it, the managers of a plant could control and supervise everything.

The only problem was that very few SCADA systems were ever designed to work in a secure fashion from a standpoint of computer security. This problem largely originated with the psychology behind the things that SCADA controlled; since a large chemical plant, for example, had strong physical security, you didn't need a lock on every valve to make sure nobody could just walk up to it and open it at the wrong time. And many developers of SCADA software moved forward with the assumption that the networks they designed and built would never be connected to anything else.

But the Internet changed all that, as it went from something handy to something utterly essential. More and more industrial plants developed their own computer networks in addition to the SCADA networks, and since both used the same protocols, invariably in many plants, the two

networks ended up being connected together. The same control room workstations that interacted with the SCADA Master also had to be able to browse the web and handle e-mail, and thus the two networks became one. And for the first time, someone could turn that valve at the wrong time without having to come anywhere near the plant.

And since a SCADA Master wasn't the kind of thing that you found on many networks, not many security geeks had looked at them for problems. Those who had found problems on a large scale still had difficulty getting them fixed. Since an industrial plant was typically in use all day, every day, nonstop, the SCADA Master couldn't be updated easily. And again, awareness of network and computer security was the exception rather than the rule in these facilities, so why bother? These facilities didn't advertise their presence online with web servers or the like, so how would an attacker find them? And even if they did, why would they bother? Unfortunately, that question was about to be answered soon enough.

The first challenge was to target only installations in North America. Fortunately, Lualhati had long since figured out that only certain allocation ranges would be applicable. The list of IP addresses available for use is broken down first by region. APNIC, for example, controls IP allocation within the Asian Pacific region. Other ranges were allocated to companies that had merited their own class-A range. Lualhati focused only on ranges allocated to ARIN and other groups known to be associated with the United States, so as to limit impact on any Muslim-controlled infrastructure.

The pair had developed a relatively clever two-stage attack. Their main target was the petrochemical infrastructure, but they realized that they needed to create a secondary effect that would in some way slow the reaction to the first attack. Working backwards, they recognized that targeting national law enforcement capabilities would be the best solution. From there, they did some varying research, mostly looking for software vendors who claimed significant installations with agencies like the FBI and Department of Justice. They settled upon ZFon as the target of choice, given the breadth and criticality of its deployment within the federal law enforcement community.

What truly delighted them was the discovery of just how easy it was to break into ZFon's software. While the newer version had less issues, they were able to get a copy of an older one, the same version that the DoJ servers were running, and it was riddled with bugs. It took the excited young men only a week to discern how to root the gateways and develop shellcode that would accomplish their aims. What remained was the scanning, which was already in progress.

One thing on their side was the relatively static nature of their targets. VPN servers rarely changed, and SCADA systems almost never changed. As a result, they could complete their scans and then take some time to prepare the attack; the data would not get stale very quickly. What was important was that they hit every target in both phases of the attack as simultaneously as possible. Hopefully, they would disrupt the distribution of gasoline and other such fuels entirely, while fracturing the ability of federal law enforcement to communicate widely with computers, thus hindering their efforts to assess and counter the damage. And since American companies were so untrusting of each other, without an organization with the power of the FBI to step in and intercede, it might take precious days or even weeks before they started to cooperate with each other to resolve the problem.

"How much longer until the ZFon scans are done, brother?"

Agpalo smiled. "Only another week, I would say. Scanning one port every thirty seconds covers more ground than I would have imagined."

Lualhati grinned back. "It helps that we need only scan one port for each attack, per system. Scanning takes much longer if you need an overall view of what is running, but in this case it is far simpler than that. And since we're able to take our time, I doubt anyone is seeing the scans at either end. Even so, since the Americans expect everyone to speak English, there won't be much hope of their having our zombies taken offline."

Lualhati had determined long before that concentrating their hacking efforts on systems within the APNIC IP address range would be their best bet. South Korea, for example, had a tremendous number of home users with broadband connections, but no security. When they hacked one of these systems, they secured it themselves, and thus kept it for their

own use. And if a security admin in the United States noticed a scan from one of them and reported it, the English-only report typically fell upon deaf Korean ears, either due to language barriers or perhaps just the unwillingness of Korean ISPs to meddle in the affairs of their subscribers. In either case, what really mattered was that the police in one country couldn't start looking for evidence in the other, so none of the reports really went anywhere. Some of the zombies were indeed shut down and replaced with more secure systems, but this was to be expected; the point was that most of them stayed intact, and it appeared that nobody had noticed their plan yet.

"Good. When we are done with this phase, the next should be simpler. And while the second scan runs, we can allocate which systems will be attacked by which zombies. It is all moving along like clockwork now, and we are starting to see the results of our labor. Insh'Allah, we will be victorious!"

The plan was to knock out as many of the VPN servers as they could simultaneously. The catch was that they didn't know which ones belonged to whom, so they had to take them all down. Fortunately, they knew which version was being used by law enforcement, thanks to reverse DNS lookups, and that helped limit the list they had to hit.

Later that evening, they met with Al-Hakim to discuss their progress. "Everything is proceeding as we had hoped, Al-Hakim," Lualhati stated pleasantly. "We have started the first set of scans, and the second set will finish as we prepare our first attack. The first set is going well, and the second should be no different."

Al-Hakim smiled, offering them food. They declined the coffee he always seemed to be drinking. It was always so sweet and heavy! "Good, good. It pleases me to hear that you have come so far in this. And I am sure that Allah is also pleased by your works. So, you are sure you can cause the software at the storage facilities to fail?"

Agpalo smiled; this was his department. "Oh yes, I am quite sure. We could not have done it without your help. Even had we known of the systems, without your assistance in acquiring a copy of the software for testing…we would have been helpless. And the machines to run it for testing were also important. But we have done all we can to make sure

that the intended effects will take place. They may differ, based upon the type of RTU in use, but very few will escape our actions unharmed." He had written the shellcode and tested its effect. He was deeply proud of his accomplishment in that respect.

"How long will the attack require, brethren?" inquired Al-Hakim. He had been careful to remain hands-off up to this point, merely asking what was needed of him and providing it. The less anyone knew of what anyone else did, the better. These two were clearly capable of carrying out Allah's work in any case, he felt.

"A very short time. A day or two, per attack. The zombies will overlap in their attacks, to be thorough. I would say that in three days it will be over," reported Lualhati.

"And how long until you can begin the attack?"

Lualhati checked his own math one last time, mentally, before replying.

"About two weeks."

Al-Hakim smiled. "Allah be praised."

Washington, DC: Wednesday, October 22nd, 10:42 AM, 2003

The phone was answered after the second ring, "Bob here."

"Hey, it's Reuben. How've you been?"

Bob's face brightened. "Hey! How the hell are you? Haven't heard from you in a while. Keeping busy?"

"Busy enough. You know how I am. If they don't feed me enough work, my feet start to go to sleep." Reuben felt much better talking to Bob, even if he didn't like the prospect of what Bob might get pulled into because of the work they all did two years ago. Bob had always been straight with Reuben, and Reuben never worried about things with respect to Bob. At times like this, just that kind of certainty and trust was beyond all measures of value.

"Looking for work? We might be needing someone in the near future."

"Ah, no. Not calling about that. It's something else. Remember the problems that Frank and I told you weren't quite fixed, in you-know-what?"

"Yeah, why?" Bob didn't seem to see this coming.

"We think there's a bad guy out there who knows about them too, now. And he's scanning for them."

Now, Bob certainly knew why he was getting a call at this point. "You're kidding. How? Neither of you said anything, right?"

Reuben almost laughed. "Are you kidding? After trying so hard to get the problems fixed? The last thing I'd do is blab about them and cause something like this to happen. Frank's the same way. No, someone figured this out on their own. And whoever they are, they're good. There's a botnet scanning, rather than just one guy, so whoever is behind it has done this sort of thing before. It's no script kiddie, this guy is trouble."

"Okay, what the hell is a botnet?" asked Bob. Sometimes Reuben forgot that for all his understanding of what made geeks tick, Bob wasn't a geek.

"Sorry, I'm a bit flustered. A botnet is basically a large group of compromised systems that are used in concert by a hacker to accomplish a goal. Let's say I want to attack a lot of systems and I need more than one machine to pull the attack off. I first hack a bunch of home computers that are hooked up to DSL or cable modems, and then I use *those* systems in my attack. The group of systems is called a botnet."

"So what do you want to do about it?"

"Well, I've called Vince, and he's feeling around to see what our options might be. After that, I really have no idea."

Bob took his standard role as the guy with the big-picture view. "What exactly do you think you can accomplish? I mean, if some bad guy out there is attacking, what can be done about it now? The genie's out of the bottle."

"Ah, I see what you mean, but the attack itself hasn't really started yet. What's happening right now is scanning."

"So how do you know there's going to be an attack? I don't understand."

"Well, it's simple. You don't line your sights up on something unless you know there's some point in shooting at it, right? No sniper ever takes his time to line his crosshairs up on the armored side of a tank. You don't scan for a single application unless you already know how to crack it. It's the same idea."

"Oh, so what you're saying is, there isn't an attack in progress *yet*, but there will be any day now."

"Exactly. Now, what can I do about it? I don't know. If the latest version of ZFon's VPN addresses the issues, then the thing to do is patch or upgrade, whichever is easier or possible. If not, nothing can be done, as I see it, at least not fast enough to matter. But at least they can be warned to watch out."

"Okay. You want my advice?"

"That's why I'm calling, yeah."

"Right. If you're *sure* an attack really is coming, and you're willing to bet it'll be really soon, make as much noise as you can about this. That way, even if anyone decides to get upset with you, they won't be able to hurt you. I mean, they won't be able to get around to doing anything before the attack comes, and they'll end up looking really dumb. But know this, if you're wrong, man, they'll probably crucify you. You gotta ask yourself how sure you are, and how much this means to you. I mean, they took the pass on doing it right, not you. I know you, you're probably beating yourself up over this, but it's not your fault. You don't owe anyone anything. But if you want to do the right thing, making a big stink is what I'd do."

Reuben exhaled, relaxing a bit. Bob always had such a clear view of things, right down to the shades of grey. It was so rare to find someone in DC who could suggest both sides of an argument for the sake of objectivity rather than hedging. "Thanks, Bob. This helps. I guess I need to do some thinking about this."

"Yeah, take a day to think it over. But don't take *too* long, because if what you said is true, I mean if this attack is coming, you won't have long to act. Good luck, and let me know what you decide. Maybe I can help bend some ears in your direction. If you're so set on this that you'll put your own ass on the line, I'll put my ass out there along with it."

"Thanks, Bob. That means a lot to me. I'll give it some thought and call you tomorrow."

The rest of the day passed uneventfully. Reuben tried to focus on his work, but his heart just wasn't in it. Making matters worse was the fact that it was policy work, which he was good at, but hated. It bored him to no end to take proper procedure and write it down with all the details that were relevant to a particular environment or organization. He was good at it, though, so from time to time he ended up being stuck with the job, and consoled himself in the knowledge that he was at least making a contribution by doing it. Resisting the urge to call anyone to see if there were any developments, he reluctantly started to power down in preparation to leave the office. He decided to give Brianna a call before he got in the car.

"Brianna here."

"Hey, it's me. Can you take care of yourself for dinner tonight?"

"Sure, hon. What's wrong?"

"Ah, I just need some time to myself tonight. I need to make a hard decision. Remember that ticking bomb I hoped would never go off? From a couple of years ago?"

"Uh oh. The VPN thing?"

"Yeah. I talked to Bob today, and he had some good insight for me. But I need to make a choice, and it's a big one. So I figured I'd just wander by myself a bit and think it through."

"Is there anything I can do?"

"I wish there was, but not really. Just give me some room when I need it, and I'll find my own way. And I'll let you know if there is any way you can actively help me, okay?" He didn't want her feeling helpless; he already felt that way, and hated it. There was no point in more people sharing in the misery.

"Okay. You promise?"

Reuben smiled a bit. "I promise."

He felt a little better. At least now he had some freedom to just do whatever he wanted while he thought things through. He only wanted to give himself one night to make this decision, for fear that otherwise he'd never decide.

Grabbing his gear, he left the office and got into his car. Over the past few years, he'd been quite successful, enough to have bought himself the car he'd been wanting. His Miata was more than just a car to him; it was a personal project. He'd made many changes to it, but kept it understated for the sake of good taste. He hated the sight of import vehicles with loud exhausts, numerous stickers for various "performance" products, and spoilers that looked like painted bookcases. As such, there were few outwardly visible clues as to just how altered his car really was.

With the top down, one clue was the stout four-point rollbar that was among the first modifications. While the Miata was extremely crashworthy, very few convertibles did well if some force flipped them over, but the SCCA-approved Hard Dog rollbar fixed that problem, and then some. Reuben smiled at the nice weather, and disarmed the alarm. Having left the top down, he just tossed his bag onto the passenger's seat, and turned the ignition. For a moment, he forgot everything else as the engine growled to life. The last set of modifications involved a complete turbo system sold by a company called "Flyin' Miata," which essentially doubled the horsepower of the small car.

He pulled out of his space, moving out of the parking lot. Ahead of him was a twisty set of roads to get home, and since traffic seemed light it looked like it would be a fun drive. *I have nothing else to do right now but go home,* he reminded himself. He preferred to focus when driving, and hated those on the road who were always on their cell phones, or doing God knows what else besides paying attention.

Moving smoothly with traffic down Route 7, he turned off onto Georgetown Pike and took the slightly longer but more enjoyable route home, letting the sharp curves in the road hold his attention for a while. It was nice to feel in control of something, even if it was only his car.

Washington, DC: Wednesday, October 22nd, 11:21 PM, 2003

"Another DeKonnick?" asked Brian.

Reuben nodded. A second beer would probably help him worry a little less about what he'd decided. "Thanks."

Brian was one of the co-owners of the place, known as "The Reef," which had opened a year and a half earlier. He bore a startling resemblance to Vin Diesel, but apparently was not fond of having this fact pointed out. Reef was a fairly new place, started by several people who had worked together at another bar elsewhere in Adams Morgan. They had promptly done everything right, and the place was an overnight success. Reuben loved it because of its comfortable atmosphere. They never let it fill entirely to capacity, and as a result, even on the busiest of nights it was still sane and civilized inside.

Reuben rotated on his stool and looked out the second-story window that overlooked 18th Street. On either side of him, large salt-water aquariums throughout the bar calmly displayed the life contained inside as Reuben tried to put his mind at ease. *What if I'm wrong? I'll be screwed.*

"Here you go, bro." Brian placed the chalice-shaped glass of beer on the bar.

"Thanks. Quiet tonight, huh? Even for a weeknight."

"Yeah, you know how it is, sometimes it's dead, sometimes it's slammed. It all works out."

"True enough." Reuben spun back to face the bar squarely and took a sip from the glass. Reef had one of the best selections of beer in the city, certainly second only to the Brickskeller, who was probably untouchable in that regard. Reef only carried beer on tap, and only good beer at that. They did reluctantly end up adding one bad beer, simply because so many of the weekend tourist crowd asked for some kind of awful light beer. But they didn't show it any respect on their beer list, describing it as, "It's light. It's wet. Some call it beer."

Reuben picked up his glass and walked to the tank in the center. He loved looking at the fish here, and loved the story behind them. A broad collection of aquatic life including shrimp, a rock lobster, a brightly-colored sea cucumber, and even a lionfish, the contents of the tanks had all belonged to the bar's owners beforehand. Their common love for the ocean and its life was the inspiration for the concept behind the bar, and when they opened, the bar's tanks became the new home for their aquatic collections. There was something very soothing about watching everything move around.

He wondered if maybe he was making too much of a big deal of all of this. After all, computers had been hacked before, and everything had always been okay. The world kept turning, even after the nastiest worms struck. As messy as Slammer, Code Red, Nimda, or Blaster were, life still went on. So the systems might be more important in this case, but the FBI was notoriously hackable for years and it didn't seem like anything too horrible had ever come of it. Just a frequently defaced website and a slew of Denial of Service attacks. He'd make his noise, the hack would come, he'd turn out to be right, and after the dust settled maybe things would just be a bit more secure. Perhaps it took a big mess to get them to clean house in the first place. Reuben walked back to his seat at the bar.

"Whatcha thinking about, bro?" Brian had been noticing his malaise.

"It's hard to explain. I need to make a tough decision at work."

"What kind?"

"Well, I'm not really allowed to talk about it, but it's like this. I can keep my mouth shut, and let something really bad happen, or I can speak up and get in trouble."

"Whoa. That sounds like a tough choice. What're you gonna do?"

"The right thing. I'm going to raise hell, and hope I don't get fried for it. If the 'something awful' that I fear actually does happen, I might help lessen it, and being right should save my ass. If not, though, I'm screwed. So I kind of hope it does happen, but not too badly, if that makes sense."

"Yeah, I hear ya. Doing the right thing is hard. I guess that's why it's a catch phrase, ya know? But at the end of the day, I don't think anyone really ever regrets doing the right thing. Not really, bro. Even if you get screwed, you'll get over it. But for the rest of your life, you'll never look back on it with regret."

Reuben smiled. Brian had a good point there. "Thanks, man. That helps, thinking about it like that. I had already made up my mind, but that really locked it in!" He took a deep drink of his beer, and enjoyed it for the first time that evening. "God, I love the beers you guys carry."

"Oh, bro, wait until a few weeks from now! We're going to have a few new ones in. There are some amazing brews we can get in winter, you've got to try them."

"Dude, you have some amazing brews here all the time." Reuben finished off the beer and put the glass down.

"Another one, bro?"

"Sure, what the hell. Now that I'm not freaking out anymore, I can finally taste the beer."

"Right on. This one's on me, bro. For doing the right thing."

"Hey, Brian…you aren't originally from Seattle by any chance, are you?"

Washington, DC: Tuesday, October 23rd, 9:14 AM, 2003

"Vince, I don't care. Listen to me. There isn't a lot of time for this. Time is *not on our side.*" Reuben was adamant, but very calm. "I don't care what backlash there is, I'll take the risk. But it has to be made clear that something bad *is* coming, and it's not far away."

Vince had been helpful during the original evaluation of the ZFon software back in 2001, but over time it had become apparent that he served political expediency more than anything else. Reuben had kept in touch with him, but didn't entirely trust him anymore. In fact, to this day Reuben was still trying to figure out how he felt about the man. But at this point, Vince was the best point of contact Reuben could think of.

Vince sighed. "Yes, but you might be wrong, you said so yourself."

"Yes, I know I might be wrong. But I doubt that I am, and I'm willing to accept the risk."

"But what about other people? If I have any part of this, I'm taking on that risk too."

"Vince, you don't realize how determined I am to make all the noise I need to make to bring attention to this. I could just call one of my Senators…"

"Okay, okay, I get your point. But you understand the position this puts me in, don't you?"

"Yes, I do, and I know it sucks. But I'm putting myself in an even worse one. And why aren't you even considering the possibility that I'm right? Don't you care what might happen?"

"I don't really know what might happen. But I don't think you understand what it is you're going to try to do here."

"You know what? You're absolutely right. I don't understand. But I'm going to learn as I go, because I don't have time to understand. And just because I'm doing it for the first time doesn't mean I'll be doing it wrong. I don't care if I don't understand. And maybe, just maybe I'm the only one who does understand, and everyone else is doing it wrong? I tried it the other way, and look where we are now. Forget it, I'm going to go with my own instinct now."

Vince signed again. "Okay. So what do you need me to do?"

"Names and numbers. Introductions when necessary. All I need to do is talk to as many people as possible. I just want to get some awareness out there. Even if nobody cares, they'll remember as soon as they see the signs of the attack, and they'll at least be a little bit warned. I don't have time to finesse and schmooze, I am going for the warning equivalent of cold-calling here."

"Alright. I'll see what I can do."

"I want a call back before three. I'm tired of waiting. If I don't hear from you by then, I find another way."

"Okay."

"I'm serious. I've been patient long enough."

"Are you threatening me?"

Reuben didn't have to consider the answer to that question for even a moment. "Yes, I am. I think you may have been stringing me along, and if I think it for another day, not only will I be noisy and disruptive, I'll Velcro your name to every bit of it. I have to risk my own ass doing this as it is, and it won't cost me a thing to drag you along for the ride."

Vince was clearly not expecting such courage or conviction. He folded, his last card played out. "Okay. Talk to you in a few hours."

"Right." Reuben hung up. He felt surprisingly good, and yet almost a bit queasy. *Well, I've really gone and done it now! I hope this works…*

He picked up the phone and dialed it again, this time looking at the number on a business card from years before. Reuben prayed silently that it was still the same number, and the same guy.

"John here." It was. Reuben recognized the voice. John was still at ZFon.

"Hey, it's a blast from the past. It's Reuben. How are you?"

John didn't take more than a moment to remember. "Ah, hi. Wow, it's been a while. I'm good…what's up?" He wasn't as upbeat as Reuben was.

"Well, I just thought you might like a heads-up. Someone is scanning pretty much the entire 'Net for your product. It's coming from an organized group of compromised systems, so it's undoubtedly in preparation for a large-scale attack of some sort. So if you've been bored lately, you're about to get very, very busy. That's all." He smiled into the phone wickedly as he described the purpose for the call, feeling the sense of vindication that he was right all along.

"Uh…what?" John was expecting Reuben to want something, not hit him with this. "Wait, start over. What're you talking about?"

Reuben was starting to develop a real case of schadenfreude. He was beginning to enjoy seeing these people squirm, far more than he expected to. "Okay. Someone out there knows about the vulnerabilities in ZFon's VPN. With me so far?"

"How do you know this?"

"Simple. They're scanning the world for it right now, as we speak. Days ago, all at once, several hosts started scanning for port 1734. So either thousands of people got curious in the same random way all at the same time, *or* some hacker is using a network of compromised systems to scan for him, in anticipation of a large mass-hack. Got it? It's a pattern that has been happened before. When there was a vulnerability in OpenSSH, for example, which nobody knew about except for one bad guy, this is how it all started. A lot of scanning, then a lot of properly maintained boxes getting hacked."

The phone went silent after Reuben stopped talking. He decided to let the silence last as long as it had to. What he heard next was a deep breath in, then a deep breath out.

"Okay. What do you want us to do?"

"Oh, that's up to you. I just thought you'd like to know. By the way, a mass hack of the Justice Department will make headlines, in case you didn't figure that out already. Have a nice day!"

Reuben hung up the phone. *That was a success,* he thought. Keeping it short and simple probably had a lot more impact than any other method he could have come up with. He had no doubt that at this moment, John was talking to at least one manager over at ZFon, and that further discussions would take place throughout the day. *Perhaps they might even pick up the phone and call me back,* he mused. *Maybe they'll accuse me of having some part in it. Boy, wouldn't that be amusing?*

He decided to call Frank and let him know what was going on; it had entirely slipped his mind. Reuben's plan was to keep Frank out of it as much as possible. Frank probably couldn't make much more noise than Reuben would make already, and there was no point in both of them taking the risk. And Reuben had a gut feeling that keeping Frank clean of all this might come in handy later.

"Hey, man, what's up? Hear anything yet?"

"Yes and no. Okay, let me tell you what's going on. I don't think that playing this the nice way will get us very far. So I've decided to play hardball. I'm making as much noise as I can. I'm hoping to draw some attention to the problem now, so that there's a chance of limiting the impact if a hack occurs. And if it does occur, it might just save me from any trouble I'd get in for making noise."

"Right on. But what if it doesn't happen, man? You're screwed."

"Yeah, probably. But I don't think that's too likely. But it's the reason I want you to stay out of it, at least for now. It doesn't do for both of us to risk it."

"Are you sure? Isn't there anything I could do to help?"

"Not really, I don't think. My job now is to be a local pain in the ass to everyone, so that they can't help but remember what I'm talking about. I think that one of us, oddly enough, might be more memorable than two. I'm not sure why I think that, but I just do."

"Okay, if you think so. I'll trust you. But be careful man, alright?"

"I think the best way to be safe is not to be careful. If something bad is going to happen, the more visible I am prior to it, the better. If everyone knows me as the guy who was yelling about the warning, nobody could dare to touch me afterwards."

"But only if you're right."

"Yeah, there is that. But honestly, how likely do you think it is that the scanning isn't preparation for an attack? And why would they bother if they didn't have an exploit ready?"

"True, true. Okay. Keep me up to date, and good luck."

"Thanks. I know I'll need it."

Chapter 7

Zero Day

Tagig, The Philippines: Friday, November 7th, 9:02 AM, 2003

"It is time, brother." Lualhati and Agpalo looked at each other before they separated and went in different directions down the street. This morning, they would walk into different Internet cafés, log in, and start issuing the commands that would trigger the first attack.

"Insh'Allah, this will be the beginning. May our works be like the armies of Saladin."

They nodded to each other, and started walking. Each arrived, as planned, at their destinations, and started scripts on several zombie master systems, each of which then issued commands to other zombies. The orders went out to initiate attacks on any systems that they had found, and the zombies completed the first phase of their purpose. As they finished, each of them fired back the list of IP addresses attacked, uploading the data in a burst to the zombie masters. This data went in turn back to Lualhati and Agpalo, who saved the lists to floppies they carried with them. Amidst the groups of people checking e-mail, trying to pick up girls, and playing games, nobody paid either of them a moment's notice.

Thousands of miles and eight time zones away, ZFon VPN gateways throughout North America received short bursts of data from the zombie systems. At the J. Edgar Hoover building in Washington, DC, the attacks happened just as people were leaving for the weekend.

The main ZFon gateway came up early on the list of targets, and accepted the malformed stream of data willingly. The ZFon Listener service failed instantly, and the shellcode that the attack contained ran with full administrative rights, just like all the other systems on the attack lists. Across the world, gateways followed the example of this one at the FBI and ran the exploit shellcode.

The shellcode was insidious, causing a restart of all ZFon services upon completion. Nobody noticed the seconds-long interruptions of the gateways. Even those who were carefully monitoring their gateways with management tools saw only a brief flap of the services and attributed it to some quirk, dismissing it as inconsequential.

The purpose of the restart was the thing of true concern. Each gateway had its core software patched with a minor addition, and upon restarting, the modified software was loaded to replace the old that had been running in memory. Each VPN gateway thus affected was now at the disposal of the pair of young men from Tagig. Aside from that, they were left unchanged, for now.

Washington, DC: Monday, November 10th, 4:22 PM, 2003

Reuben could taste the bitter, metallic taste of adrenaline in his mouth. He was looking at the ISC again, at the summary for scanning activity related to port 1734, as he had done every day for weeks now. Every day, it had shown pretty much the same thing: a constant and relatively steady amount of activity. His calls to Vince sounded like progress was being made toward getting the DoJ to address the impending attack, but over time, nothing had changed. And every day, more scanning was happening, the activity was solid and steady in the ISC's logs.

That activity had now entirely ceased.

Reuben had noted the change on Saturday, which showed as a dramatic drop, but wasn't entirely concerned. Many organizations seemed not to submit logs of activity from the weekends, as there was a steep drop in all activity during those days. But on this day, no such factor was at play. After the whole day, there was still no scanning.

This confirmed one thing: the theory that one person or group was behind all the scanning. The only way that the scanning would have stopped as quickly as it began would be if there was a single entity controlling it. Unfortunately, it indicated that this entity now had what it wanted and was done scanning. An attack was going to start any minute, if it had not already begun. The ISC didn't show attacks against running applications, just attempted connections where they should not be directed.

He had noticed the difference in the morning, but didn't want to believe what he saw. And, being the morning of the first business day of the month, he could dismiss it as nothing more than the lag before people submitted their logs. But this late in the day, there was only one explanation for what he saw. And he hated to admit that to himself.

He picked up the phone, dialing Vince's number from memory.

"It's Reuben. Where are things now?"

"Well, good afternoon."

"No, it isn't."

"I was being sarcastic."

"I wasn't. Guess what just stopped?"

There was a pause. Reuben wasn't happy with taking people off guard just now. In fact, he was fairly sick of being the first one to figure everything out, and stuck with the job of trying to get them to catch up.

Reuben gave up waiting for the guess. "*The scanning.* They've stopped scanning."

"Oh! So that's good news, they've stopped! So they gave up?"

Reuben couldn't take it anymore. He threw the handset of the phone against the desk, standing in his chair in ultimate exasperation. He felt more exasperated and angry than he had in his entire life, more so than even his worst days sitting at a desk doing helpdesk work. Looking around for some desperate outlet for his anger, he scooped up his empty coffee mug and hurled it against the wall. It predictably and cathartically fragmented into shards of glazed white ceramic.

Reuben picked up the phone, almost beyond caring if Vince was still there. "Okay. Let's try again, *shall we?*"

Vince was more serious now. "What does it mean, then?"

"It means they've found what they're looking for. And what do you do once you've found all the things you want to attack?"

"Ohhh. Yes, I see. You attack them."

"Yes, now you get it. We're out of time."

"So it's started already?"

"I can't tell for sure. The best way to figure it out is to look at some of the VPN servers."

"How did you know they were scanning in the first place, then?"

"Simple. The hackers look for running servers by probing a range of IP addresses. Most of what they scan, however, isn't running what they're looking for, so the probes show up in logs as being strange traffic. A probe to an actual server, on the other hand, looks pretty much like a normal connection, so it does not show up as being anything of interest. And now that they know where the servers actually are, they can connect to them without raising flags."

"What about intrusion detection?"

"Well, that's a bit trickier. Since it's an exploit that nobody knows about yet, there won't be a specific signature for it. That said, if we get

lucky, they may have written it in such a way that an IDS can detect with a more generic alert. If it has a big NOP sled, for example, or it uses shellcode from another exploit, then maybe some intrusion detection systems will fire an alert when the attack hits. But if they did something even remotely clever, I wouldn't count on it. And even then, that only applies to networks that have IDS in the first place. How many do you think there are, at all the remote sites? The FBI field offices, the embassies, and so on."

"Uh, yeah. I see your point. So how do we find out if there's been an attack?"

"I need to get my hands on a gateway that's been running, and look around. I don't know what they're doing to the systems, so I don't know exactly what to look for. But I know where to look, and I think I'll know it when I see it. I need you to get me access to a system."

"Okay, I'll see what I can do. You sold me."

"Good. And the sooner I can look for the attack the better, so we can learn what exactly their intentions are with respect to the gateways. Because I don't know what we can do besides damage control at this point, and we need to learn how to assess the harm that they do."

Tagig, The Philippines: Tuesday, November 11th, 5:00 PM, 2003

The pair met with Al-Hakim to give him a status update on their efforts. The room was silent, everyone else having been directed to go elsewhere for a short time. "Everything is moving forward as hoped, Al-Hakim. This far, we could not have hoped for more," reported Lualhati.

Al-Hakim took another sip of his coffee. "Excellent. So the first attack took place as hoped?"

"Indeed, Al-Hakim. It is concluded, and the systems await our commands now. The scans for the main thrust are proceeding as well as the first did, and should be done in approximately a week and a half. When this is complete, we will move to strike the infidel Americans in their own homeland."

Al-Hakim smiled. "It will be entertaining to watch their society stumble and fall without Muslim oil to keep it running. Do you require more assistance of your brethren?" He was eager to see the attack proceed.

Agpalo answered. "That will not be necessary, but we thank you, Al-Hakim. Now the burden of the effort rests upon the shoulders of the computers we are using. All that is left for us to do is wait, and plan. The worst of the work is well behind us."

"Good. Allah smiles upon you, my young students. You are doing His work."

Washington, DC: Thursday, November 13th, 3:17 PM, 2003

For days, Vince had worked to bring this meeting about. It was a frustrating process, as he worked to convince one person, only to have someone else step in and raise concerns. "Reuben wasn't cleared for this kind of access." "Reuben had no concrete proof of an actual attack," were the answers he received. One person even went so far as to claim that this was an elaborate ruse involving him, for the purpose of getting access to trusted systems by hackers. And this was all compounded by the occasional bureaucrat who, not understanding exactly what was being described, felt it safer to do nothing rather than risk screwing up.

Repeatedly, Reuben had been asked to tell them what to look for, and at first he humored the request, asking to speak with the engineer who would do the looking. Initially, this request was declined, and things went back and forth for hours until Reuben relented and decided to use a bit of logical judo to resolve the deadlock. He began to explain, at length, all the things that needed examination, and explained in equal totality the possible signs of a compromise. The relatively non-technical manager to whom he spoke quickly realized the uselessness of this, and finally caved in.

The manager had put Reuben in touch with a contractor named Jane, who was perfectly willing to listen and learn, but in the end she too felt that it would be best that Reuben look with his own eyes. She suggested that she accompany him, so that she herself could validate his efforts and assure the DoJ that nothing untoward was taking place.

But in the end, it had come to this compromise, with Reuben and Jane sitting side by side at the monitor, with Vince, the two unnamed people from past meetings with DoJ from years ago, and two other managerial types in attendance. The two new faces had clearly never been in a server room before, shocked as they were at how cold and loud it was in the sterile rack-filled space. They were also the only ones not to bring their jackets with them, and were clearly not having much luck keeping warm. Nobody looked happy about this whole situation, and it was clear that at any moment Reuben could be asked to leave.

Reuben tried as best he could to focus, given the pressure of the situation and the myriad sets of eyes upon him. "Now, the vulnerability doesn't throw a specific error in the Event logs, unfortunately. You don't even get a message box popping up to let you know that something went wrong. I don't think there was anything in Dr. Watson's logs, either," he added, referring to a specific diagnostic log that Windows used to sort out software failures. "The service just dies. What we did see is that restarting the service provides the normal event in the Application Event Log."

He opened Event Viewer, and looked first to see how far back the logs went. By default, the Event Logs only kept half a megabyte of events, and overwrote the oldest events as newer ones were recorded. Half a megabyte was not a hell of a lot of data to store, and the logs only went back five days. Reuben had included in his report to DoJ that any system set up to act as a ZFon gateway needed to be built in accordance with basic standards for securing Windows properly; apparently this was ignored, or never made it into the procedure for building the gateways.

"Dammit!"

"What?" asked Jane.

"There's only half a Goddamned meg allocated for the Application Log! Unless the attack happened in the past…uh…five days, it looks like we won't see the restart event of the service. Who built this system? I put in my report that all gateways needed to be properly secured and built before they even got the ZFon software to begin with!"

Jane's face flushed. She didn't want to say in front of everyone there that she was the one who basically built the system. She was angry at him for potentially making her look bad, but she was angrier at herself. She was

so distracted going over the process with her colleague Tom, she overlooked the step about hardening the operating system first. She knew better, but nobody ever expected their own systems to get hacked until it was too late.

Reuben sat back and rubbed his forehead, trying to get a grip. He was already frustrated; it was so discouraging to see that what little advice he was able to give wasn't followed properly. He thought for a minute about what to look for next. "Well, maybe the exploit leaves more of a trail than our testing did. Let me look at Dr. Watson's logs." Opening Explorer, he went to the file in the C:\WINNT directory and opened it. He spent a few minutes looking at some of the things that had blown up in the lifetime of the system, but saw nothing with any relevance. He exhaled a long breath of the cold server-room air.

Jane was watching, and could feel his frustration. Blaming herself for the logging problem, she tried to come up with options. "Is there a log that resides within ZFon itself?"

"No, it uses the Application Event Log for everything. Microsoft standard. Let me check, just to make sure, though."

Behind the pair, impatience grew among the observing managers. Reuben sensed that his time was running out. "Okay, let me think. Here's where having an honest-to-goodness bad guy here would be helpful. There are various ways this box could be rooted, but the most common is to run a rootkit on it. There should be a listening port somewhere on the system."

Jane's face lit up. "Oh good, just run netstat then?" she suggested, referring to the command-line utility that showed the state of network connections on the system.

Reuben shook his head. "Nope. The first thing they do is modify netstat so that it doesn't show certain things, for that very reason. We need someone to run a portscan against the gateway. That way we can spot any listening ports that shouldn't be there, without having to trust any of the binaries on the gateway itself. There are just too many ways to hide the listener otherwise. Do you guys happen to have a Linux box around somewhere so we can run Nmap?"

"Uh, no. We don't use Linux here. We've moved strictly to Windows-based systems."

"Ah, great, and they wouldn't let me bring my own laptop in. Okay. Do we have a system we can install Linux on, then? All I need is some bandwidth, a desktop or laptop computer, and a CD burner with a few blank CDs. It'll take a couple of hours to get everything set up, but then we'll be good to go to run a few tests."

Jane looked back at the five silent managers behind her. "What do you think?" She was afraid of running afoul of them; this was serious business, politically speaking.

They all looked at each other, and the one who clearly held rank spoke up. "What do you think of all this, Vince?"

Vince was hoping not to have to say a word during the meeting. He knew that if he upset Reuben, Reuben would work hard to discredit him or worse, but he also stood to lose a good bit if he went too far the other way. "I think we should give it a shot. Jane…it's Jane, right? You trust him to do this without causing any harm?"

Jane nodded. "So far, everything he's done makes sense. He hasn't been poking around anywhere strange, and hasn't looked around in any random way that makes me think he doesn't know what he's looking for. I say let him try it."

The big cheese nodded. "Okay then, get to work. Jane, get him everything he needs and call us when he's ready. Keep the computer he sets up off the network until then."

Reuben hated being distrusted so much. He felt insulted. *Hmph. Here I am, trying to save these assholes from their own Goddamned dumb-ass selves, and they're thinking I'm the problem! How dare they?* He held his temper in check, and directed it toward finding the server compromise so he could have the last word when he turned out to be right.

Jane and Reuben stood up, logging out of the server, as everyone filed out of the room. Jane motioned for Reuben to follow her, and led him out of the server room and down the hall toward the cubes where contractors worked.

Tom was waiting there for her, hoping to hear the gossip on what transpired. He seemed to consider Reuben's appearance as something of a

bonus in that regard. "Hey, you must be Reuben. How'd it go?" He smiled expectantly, eager for the scoop.

Jane frowned. "Not so good so far. I fucked up." She turned to Reuben. "I'm the one who built the system. I'm sorry, I totally passed over the hardening. It was just a single line in the procedure, and I was trying to get to the install of ZFon itself, so I guess I just missed it that time. It's my fault."

Tom frowned at her. "I noticed that, but didn't say anything. I figured you must have hardened it beforehand. Oh well, I guess I should have spoken up. But what does that have to do with it?"

Jane explained. "There was only 512 KB allocated for the Application Event Log. Reuben says the attack probably happened seven or eight days ago, but the logs only go back five days. So that's one piece of evidence that's lost forever."

Tom tilted his head back in understanding. "Oh man. Sorry about that."

Reuben looked at both of them, trying to figure out how he felt about their admission. "Well, I guess it's an honest mistake. Sorry I erupted like that in the server room, Jane. I had this mental image of a total shithead as the person who set it up. All through this thing, I've been banging my head against people who haven't got enough brain cells to outwit a chair, it seems. I'm just so tired of having to jump through so many hoops just to do the right thing, and to be treated like the enemy the whole time."

Jane smiled at Reuben slightly as she handed him a stack of blank CDs. "Welcome to the fun world of government contracting, friend. Let's get you set up so you can do that voodoo that you do so well, eh? Tom, could you get that spare laptop we have in the storage room?"

Washington, DC: Thursday, November 13th, 5:28 PM, 2003

Reuben was finally set to start working. He had installed Linux and Nmap on the laptop, which was made somewhat easier by it being a 2002 model. Everyone reconvened in the server room, where the laptop was now plugged into the network and was ready to begin scanning.

Reuben inwardly crossed his fingers as he inhaled and exhaled deeply, calming himself. "Let me check that IP address again." Jane held out her notebook for him, with the address of the VPN gateway's outward-facing interface scribbled on it.

Reuben typed the command into Nmap to scan all ports, both TCP and UDP. He set it to do so fairly aggressively, figuring that since he was connected to it with a fast connection, it would be best to make use of the speed available to him. He set it to do full connects for TCP scans, to make sure he didn't hose the machine with a SYN flood accidentally. He also set Nmap to operate in "verbose" mode, reporting on each action it was taking as it operated:

```
root@testbox: nmap -sT -sU -T Aggressive -p 1-65535 -v -n -oN nmapscan.log
192.168.10.216
```

He stood back, watching the scanner work.

Nmap was the most widely used port scanner known, a command-line program that did port scanning and *fingerprinting*. Fingerprinting was the act of guessing which kind of operating system was running on a machine by the peculiarities of its reactions to network traffic. Each operating system had its own particular behavioral traits when it came to TCP/IP traffic, much as people from different regions of the same country speak with different accents. They could all talk to each other, but if you knew how to tell the accents apart, you could tell what parts of the country they were from. But what Nmap did best was detect open ports, reliably and quickly. And, quite often, it could do so without detection by using certain methods of scanning where it refused to follow the rules of how a normally operating network application should behave.

"This might take a while. The UDP scan alone can be a lengthy process, since UDP doesn't use sessions," reported Reuben. He stood back from the laptop to resist the urge to touch anything. It was very hard to remain patient at a time like this, but he had a great deal to lose by being impatient.

The big cheese spoke up, taking advantage of the lull in activity. "So what exactly is it looking for?"

Reuben was grateful for a chance to educate the managers as to what was happening. In his mind, any questions they had that he could answer was a good thing. It gave him a chance to demonstrate that he did know what he was talking about, and it might just help them to understand how important all of this was right now. "I'm going to assume you don't know networking very well, so if I say something you already know, just bear with me. Computers are like big sets of sockets. When one computer connects to another to talk, it's like a wire is plugged into a socket in one computer, and into another socket in the other computer. Each system has about 64,000 sockets that can be used, and each one can either send the connection or accept one, but not both at the same time. With me so far?"

The man nodded. Reuben noticed that this time he'd worn a jacket; he was learning in more ways than one today.

"Okay. Each socket can only have one program using it at the same time too, so the question becomes that of 'which socket is the program I want to connect to using?' The solution to this is simple; certain sockets are reserved for certain types of programs. Web servers, for example, use socket…or, as we call it, port…80. So if you want to talk to a web server, you connect to port 80 of a machine that's running one."

"Got it. Go on."

"Well, in this case, I suspect that there's a program on the VPN gateway that was installed by the hacker or hackers, that listens for a connection. I don't know what port it would be on, though, so I'm scanning all of them. There are certain ports that are used by Windows, another that is used by ZFon, and maybe a few others if you have some kind of management software running on the server. But anything beyond those is suspect, and probably bad news."

"How can you tell what should and should not be there?"

"That's actually pretty easy. For one, we can compare what Nmap tells us to what the server itself says it's running. You see, hacked machines are altered so that you can't see the bad process or the port it listens on. So if we see something that shows up in Nmap, but does not show up when we ask the server what it's running, that's a dead giveaway right there. What was a way to hide something from us becomes a way to discover it."

"Ahh, I see. It's like someone's alibi turning out to be false. That way you know they're hiding something. It doesn't directly point to them being guilty, but it's an indicator for other reasons."

"Exactly, you've got it. The reason it's taking so long is that I have to scan every possible port…and there are a lot of them…because I don't know where it might be. Every hacker puts them somewhere different, to make them harder to find like this. And there are two kinds of ports too, so I have to scan both kinds, and the second kind takes longer."

Jane nodded in confirmation. She and Tom had gotten a chance to get a good feel for what Reuben was like, and what motivated him, while he set up the laptop. They were both impressed with him, and now Jane wanted to help him in any way she could. He was clearly someone on the good side, and he wasn't stupid. After Reuben had explained it all to her, she too was convinced that something awful was happening. It didn't take a genius to connect the dots, so she didn't understand any better than Reuben why it was so hard to get the DoJ to cooperate. She wondered how much of it had to do with the political battles over getting it deployed in the first place.

Reuben glanced at the screen, but the scan wasn't finished yet. "God, I wish I had some idea how long an intensive single-system scan like this took. It's always so hard to wait for it to finish, not knowing when to expect it to be done."

The others shifted on their feet, and smiled in acknowledgement. Reuben had finally found some kind of common ground at least. He looked back at them all. "What would you do if I did find something, if I may ask? I don't know if ZFon has ever fixed their software completely. What never made it into my report was that afterward, we looked more closely at it, and easily found at least one other issue not described in the deliverable you got. And since ZFon didn't get that information either, I'm thinking there isn't a version they make that can't be hacked or knocked offline. So where does that leave you guys? It sounds to me like this software is a key component of your wide area networking now, and that without it you basically can't communicate securely with any of your field offices or other facilities."

Reuben seemed to have hit sensitive territory. Everyone but the big cheese seemed to shrink a bit, not wanting one bit of the question, its answer, or the responsibility inherent in dealing with either. "Why don't we cross that bridge when we come to it, shall we?" suggested the big cheese somewhat coldly.

Reuben didn't push the point, and stood there for a minute trying to think of something to say to change the mood back.

Jane tapped him on the shoulder. "Hey, I think it's done."

Reuben turned, stepping up to the laptop to examine the output:

```
# nmap (V. 3.00) scan initiated Thu Nov  13 17:39:51 2003 as: nmap -sT -sU
-T Aggressive -p 1-65535 -v -n -oN nmapscan.log 192.168.10.216
Interesting ports on  (192.168.10.216):
(The 131057 ports scanned but not shown below are in state: closed)
Port        State        Service
135/tcp     open         loc-srv
135/udp     open         loc-srv
137/udp     open         netbios-ns
138/udp     open         netbios-dgm
139/tcp     open         netbios-ssn
445/tcp     open         microsoft-ds
445/udp     open         microsoft-ds
464/tcp     open         kpasswd5
464/udp     open         kpasswd5
1026/tcp    open         LSA-or-nterm
1028/udp    open         ms-lsa
1029/tcp    open         ms-lsa
1734/tcp    open         unknown

# Nmap run completed at Thu Nov  13 17:39:51 2003 -- 1 IP address (1 host
up) scanned in 343 seconds
root@testbox:
```

He didn't see anything out of the ordinary. It was, as far as he could tell, a perfectly normal ZFon gateway. There was neither a TCP nor UDP port showing that was abnormal.

"Wait, that doesn't make sense. How could…I mean, what's the point?" He thought for a second, staring at the screen. "Uh, there's nothing unusual here," he reported back to the group of suits.

"So, what does that mean? It's clean?"

"Well, it's not conclusive. It could be that they rewrote the Listener itself so that it'll respond to commands from the hackers too. I wish I had hashes of the binaries. Then I could check and see if…"

"Well, hold on a minute. We've been cooperating this far, but I think here's where we call it a day. You haven't been able to find one piece of evidence that indicates that this system is compromised. I'm satisfied that it's clean, and this has been a big wild goose chase for something that doesn't exist. What makes you so certain that it wasn't someone just checking to see who uses ZFon?"

"Well, actually, that's exactly what I think it was, but the question is why were they checking?"

"Well, who cares why? It doesn't look like any harm was done. Maybe they thought they could hack it, but it's not so simple. You didn't actually *hack* a ZFon server in the course of your testing, did you?"

Reuben felt himself starting to get angry. Extremely angry. He instinctively felt that he now knew who was behind the insecure deployment, and that he was now at his mercy in this room. "No, not during the testing. But Frank, the person who worked with me on the project…"

"The hacker from Seattle. Did you see him do it?"

"No, but I trust him. If he said he did, he did."

"So he says. Why do you believe it?"

"Because I know him. We're good friends, and he wouldn't care if it weren't true."

Jane winced, watching the whole scene unfold. Reuben was entirely screwed. Everyone demonstrated where they stood with body language, Jane siding sympathetically with Reuben while the suits formed a unified front. Unfortunately, Jane couldn't argue Reuben's case because she didn't have enough information, and the big cheese held all the power, and therefore would win by default.

"So says you. But how do we know we should believe your assessment, or think that you're qualified to make it?"

Reuben flushed red. "Why did you hire me in the first place, if you have such doubts of my ability?"

"Because we had to. That's why."

Reuben nodded, recognizing his own defeat. *At least I tried,* he thought, trying to console himself. *Dammit, I know this box is hacked. Where's the malware?* "I guess it's time for us to all go home, then," he conceded. There was no point in making this take longer than it had to.

The big cheese nodded in acknowledgement. "Jane can escort you out." Reuben nodded back.

Jane volunteered, "Don't worry about the laptop; I'll take care of it all later. No harm in leaving things here. Even if the laptop isn't hardened, the firewall is locked down pretty tight, nobody will be able to connect to it."

A light bulb went off in Reuben's head. *My God, I totally forgot about that! The firewall! The listening process HAS to be ZFon, because it's the only port anyone from the outside could connect to!* He looked for a brief desperate moment at everyone else, but they were already starting to leave the server room. And there wasn't much chance of getting them to listen at this point anyway. He walked out with Jane after they had all left.

Jane took him by the cube where Tom was still waiting. "Well? How'd it go?" He was anticipating interesting and exciting news.

Jane frowned at him with sad eyes. "Don't ask. Grab your stuff, we're all going out for a drink. Okay with you, Reuben?"

"Yeah, I guess. Hey, thanks for helping out. I know you were on my side back there…I hope I didn't get you into any trouble."

Jane looked back at him. "Don't worry about it. I know you're right, and I care about it. But for now, there's nothing we can do, so let's just go get drunk instead. Anywhere in particular you like to go?"

"Yeah, I go to a place in Adams Morgan pretty regularly. I live there...Adams Morgan, that is, not the bar…so it's a hangout for me. You'll like it, it's called 'The Reef.'"

"Cool. Let's grab a cab."

The trio trudged out of the Hoover building, Reuben surrendering his visitor ID at the security checkpoint on the way out. He hated this building, and what the FBI had been doing since 9/11, but he still felt a patriotic drive to protect it. Even at their worst, they still were guardians of

the nation, and deserved to be safe from attack themselves. It was a strange thing, defending an organization that was doing things you disagreed with, only to be smacked down.

They eventually caught a cab on Pennsylvania Avenue and sat in the back together while the cab worked its way to Adams Morgan. Debating the wisdom of speaking too openly in front of the cab driver, Reuben filled Tom in on the details in general terms, leaving it sufficiently unclear that no casual listener could make sense of it all.

"So, you're saying that what you think happened did, but you just need to look deeper for it. Yes?"

"Exactly. But it won't happen. I don't know what his deal was, but I think he's on the hook for the system. There's no easy fix for the problem, and he'll get in trouble for the downtime. So he wants to just bury it all and hope for the best. I think he might not get in worse trouble that way, even if he's wrong. And that way he does get a chance not to get in trouble at all."

"Yeah, that sounds about right," echoed Jane. "Wilkens is his name, by the way."

"Wilkens?"

Jane clarified, "Yeah, he's the man who was calling all the shots today. I don't think it was an accident he didn't let his name slip, so you didn't get it from me. But yeah, he's been responsible for the VPN project for a while. And I gather it was a situation where it was behind schedule for various reasons, so when you found problems with it, it was a major monkey wrench in the works. Whatever the story, we can all guess that he's the source of all the pushback."

"So now what?" Tom didn't want to consider that it would end without a resolution.

"Now nothing, I guess. Wait until it becomes obvious that I'm right, I suppose. I made a lot of noise before this, so people know who I am now. When the shit hits the fan, I only hope they'll be able to swallow some pride and get me involved again." Reuben didn't like the thought of it, but he was fresh out of options. He'd made all the calls he could, and happened to stumble across the man who had been blocking him all along, at the worst possible time. He had had enough for now, and just wanted to

get back to his current job and put this all behind him. Maybe he had been wrong, and perhaps it was just scanning and nothing more. Only time would tell.

The cab was getting close to their destination; it was Reuben's job to let him know where to stop. Neither Tom nor Jane had been there, and Reuben didn't know the exact address. "Ah, anywhere here is fine, man," Reuben instructed. As he pulled out his wallet to pay the driver, Jane beat him to it. Tom put his hand on Reuben's wallet.

"Don't worry about it, Reuben. Tonight's on us, you've had enough of a day already."

Reuben was touched by the show of support. Now that there was nothing left for him to do, he started to feel the weight he'd been carrying, and the pain of failure. Failing to prevent an insecure system from being widely deployed, failure to prevent the mass hack that was probably complete by now, and failure to get anyone to properly look into it after the fact. For all his efforts and hard work, he had not successfully accomplished a single objective of his profession in this matter. He felt less like someone who failed than someone who was in and of himself a failure.

Washington, DC: Thursday, November 13th, 10:56 PM, 2003

Reuben was feeling a little better now, if only from an elevated blood alcohol level. He was thinking less about the world outside and more about his time with two new friends, in his favorite haunt, with the soothing marine life in front of them. And Brian was working.

He stared at his beer before taking a drink of water. Brian was big on drinking water with one's alcohol, and Reuben was grateful for it. He'd always believed that keeping hydrated kept you from feeling like hell the next morning, but it was sometimes hard to remember to keep drinking water when you were drunk and extremely depressed.

"Jeez, bro. It looks like you had one rough day. I take it the right thing didn't go so well, huh."

Jane and Tom looked up at Brian, then at Reuben.

Reuben didn't even look up. "Relax, guys, I didn't tell him anything. Just that I had a hard choice."

Brian looked at the trio. "Whoa, what he said. No worries. And I guess that's a yes to my question."

Jane nodded to Brian. "He tried, he really did. But yeah, it didn't go so well. I don't think he could have done more, or accomplished more. He really tried."

Brian looked at Reuben. "I'm sure he did. He doesn't seem like the type to not try. Hang in there bro, I'm sure it's not over yet."

Reuben paled slightly at that thought. He would have welcomed being wrong at this point. While being right would contain the key to his redemption in this, it would only do so at a terrible price. He was willing to sacrifice himself to prevent that, were he given the choice. He couldn't decide if he was glad that it wasn't his choice to make.

"I wish it was. If it was, nothing bad would come of it that hasn't already. I could just be done with it and go back to doing what I was doing two weeks ago. I'm afraid it's not over though, and something awful is coming."

Tom listened quietly on Reuben's left side as Jane patted Reuben's back from his right. "Don't worry about that now. Right now, just do what you do normally. Hey, look at it like this. If something bad does happen, they'll call you. And they'll know more than they would if you hadn't gotten involved. Every day bad things happen because people let them. You fought as hard as you could, just like I'm sure you always do. So don't stop now, or you'll be letting all those future bad things happen. Chin up, and remember that doing good isn't one thing you do, but the way you live your life. Don't let this change you."

Brian smiled. "She sounds like she's pretty smart, bro. I'd listen to her if I were you. The next round for you guys is on me." And with that he went to tend to a customer on the other side of the bar.

Reuben smiled. Jane was absolutely right; he needed to look at the bigger picture, and keep in mind why it was he loved his work so much. It wasn't just the challenge, the money, or the enjoyment of being able to tell people what he did for a living. It was the chance to walk into a company, look things over, and walk out having left that part of the world just a little

bit safer. It was the notion of protecting people from being preyed upon by others. He liked the superman thing that happened when he had to go into a hacked network and save the client. There was no point in letting one failure sour his whole life.

He finished off his water, and then went back to the beer. "You're right. This isn't the end of the world. If I'm wrong, at least I was wrong doing the right thing. Gotta be wrong about something, so it might as well be a noble mistake. But here's a question. What if I am right? What I need to do is make sure that as soon as it gets noticed, I get back into the loop. Can you guys help me with that?"

Tom smiled. "Now you're thinking, buddy."

Jane nodded. "You bet. I don't think it would take much prodding to get them to bring you back in. We'll just have to make sure Wilkens isn't the guy who gets contacted first."

"No shit," agreed Reuben.

Jane clarified, "That's no problem; if something big does happen, people above his level will be coming down to visit, and that's when I can mention you. If what you fear is really happening, when the shit *does* hit the fan, I don't think it'll take five minutes for them to ask someone to pick you up to come help. And when the details come out, Wilkens will be done for. So he'll be the least of your worries then. His power will be greatly diminished before you even show up anyways, since the disaster will have happened on his watch. So don't you worry yourself about this. It's not over, if it needs not to be over. Get my point?"

Reuben nodded. "Yeah, I hear you. Good way to look at it. And thanks, you two."

Later that night, Reuben staggered through the front door of his apartment. *Good thing we went to a place in my neighborhood,* he thought. The apartment was dark; Brianna was in bed.

The first thing Reuben did was go over to his desk and call MadFast. It wasn't terribly late yet in Seattle, and MadFast was a night owl at any rate.

"Hey, hey. How are things over there?"

"Hey man. Well, it's been a hell of a day. Bear with me, I'm just a wee bit smashed."

"Right on. Celebrating, or crying into your beer?"

"Mostly the second, at least at first. Okay, here's the deal. I did everything I could, believe me. But we're stuck for now. I found out what the whole deal was, though, and there's a plan to bring me, or us, back in if or when the shit hits
the fan."

"Go on, I'm listening."

"Alright. The whole project was running way behind schedule before we even got involved. It was apparently at the point where the man with ultimate responsibility was going to get roasted for it. And of course, our findings would have pushed the whole mess over the edge, so he squashed it all."

"No shit. Wow, how'd you find that out?"

"I met the coolest sysadmins today. They're contractors, and one of them was helping me out…well, actually her job was to look over my shoulder to make sure I didn't do anything wrong today. But they're both cool, and on our side now. Unfortunately, today's meeting went absolutely nowhere. Oh! I need to tell you what I found, and what I think, and get your opinion."

"Right on, I'm listening." From the way Reuben sounded, MadFast was glad not to be on the front lines, but he felt a little bad that Reuben had to be.

"Okay. Their logs only went back five days, so I got nothing there, so I don't know if there was a restart. But I managed to stand up a Linux box and do an Nmap scan. There are no extra listening ports."

"Did they let you pull hashes of the binaries to compare?"

"No, things broke down at that point. But that's what I was thinking too."

"Yeah, I was giving that some thought. They'd need to modify ZFon itself, otherwise they won't be able to get through to any shell they set up. I'm willing to bet that they've got most or all of the gateways behind firewalls, so there are limited ports available. And the only port they could reliably count on is 1734."

"Cool, we're on the same page. I wish I'd thought of that beforehand though, but now that I know the politics behind it I don't think it would

have mattered. So I basically got handed my hat, and shown to the door. But here's the deal, okay? Jane and Tom…the sysadmins…will be watching. If the shit hits the fan, they'll be there. The guy who pushed through the deployment, Wilkens, is the real problem. But if the shit hits the fan, his bosses will show up, and Jane will mention us. So we can get back into the loop. And at that point, since the really high-ups will have gotten involved, Wilkens won't have the veto power he has now."

"Wow, you've had a hell of a day, man. Right on! Heh, its all DC stuff, getting thrown out because of politics, then recruiting a couple of spies on the inside!"

Reuben felt better, having heard MadFast put it like that. "Yeah, I guess that's what I did. It just kind of happened though."

"Maybe that's how it's supposed to be. Either way, you sound like you've got it under control. Keep me in touch, and get some sleep. What time is it there, anyways, like 3 A.M.?"

"Yeah, it's late. Going to be a rough morning."

"Well, sleep well and just relax. Even if nobody else is, you and I are ahead of the game now. Talk to you later."

"Good night."

Tuesday, November 18th, 2003

Reuben had stopped paying attention to the ISC's website. It was depressing. After a few days of looking in hopes that scanning would turn out to have resumed, only to discover otherwise, he tried to shut it out of his mind and focus on his current work.

Even had he kept watching, he probably would not have noted the scan that was underway for PetroilSoft SCADACommand systems. Like the ZFon scanning, it was of insufficient intensity to gain the attention of anyone who wasn't familiar with the port's use. And since the system was not one in wide use, nobody who happened to be responsible for it was among those who watch the ISC's reporting. The scan went entirely unnoticed by anyone, and the zombies continued without much interference, collecting their list of vulnerable systems. In fact, since this scan was pared down to avoid certain address ranges, it ran more quickly.

Tagig, The Philippines: Wednesday, November 19th, 11:27 PM, 2003

Lualhati came back from a quick check on the scan status, beaming with a grin from ear to ear as he stepped into the windowless room. Al-Hakim and Agpalo both looked at him, and suspected the cause of his mirth; Al-Hakim quickly dismissed everyone else from the room to give the trio privacy to speak.

"It is done. The second set of scans is done. We may strike at any time now."

Agpalo closed his eyes, smiling as he leaned his head back, bathing in the realization that they would succeed after all. All these years of work, of learning and practicing and planning, and he never dared to fully believe that they would truly arrive at this point. But now, he believed.

"Allah be praised. Begin when you feel ready, my pupils."

They both nodded. "Today, then. There is no value in waiting."

The pair quietly left, stepping out into the sunlight.

"We should take a few hours to calm ourselves, brother. It is not good to act when we are so excited," cautioned Lualhati.

Agpalo smiled back at Lualhati. "I will trust your judgment on this matter, brother, but I do not see the harm in acting swiftly. What can stop us now but time?"

"True, true. But it is often the unseen danger that strikes when one moves in haste. Be wary, friend. We should not have come this far just to err so close to the end of our journey. The caution we still must exercise is but a drop compared to the basins of care we have taken before now. It is no great burden, so let us not drop our guard so suddenly."

Agpalo wanted desperately to act, but he would stick by Lualhati. After all, without his help, none of this could have happened. And more than once, Lualhati had spotted or avoided risks that could have undone them both. "So, when? It would help me to prepare myself if I knew."

"This evening. Not long, brother. Be patient."

Baltimore, MD: Thursday, November 20th, 4:15 AM, 2003

The tanker was nearing the Port of Baltimore, after a relatively quiet trip. Arriving early, it was slotted to dock at the transfer facility in a few hours, where it would offload its cargo of gasoline. The Captain was up early, so as to be fully awake and prepared when the harbor pilot came aboard. He drank more of his black coffee, and thought how nice it would be to get some shore time. He was looking forward to having a nice meal, and perhaps even some female companionship, if he was lucky.

The water was quiet and calm, with few signs of life. It looked to be the uneventful end of an uneventful trip.

Tagig, The Philippines: Wednesday, November 20th, 5:15 PM, 2003

Agpalo was sitting in an Internet café, barely containing his excitement as he issued the final sets of commands to the zombie masters. He grinned as he imagined the actions cascading, the zombie masters repeating the commands to all of the zombies, who would in turn reach out to the now-compromised VPN gateways and soon-to-be-compromised SCADA systems. He loved the thought that his own skill had brought this into being, that his own ability was an essential part of the sequence that was now unfolding.

And just as he imagined, the actions did indeed take place, like dominos in sequence. The zombie masters, as before, repeated back to Agpalo the list of systems they had attacked. Agpalo went to save the file directly to floppy, but then realized he didn't have the floppy in the drive yet. He fumbled around for a second, looking for it before he realized the upload might time out if he didn't save it quickly. He decided to save it to C:\temp on the local drive until he could find the floppy disk.

Digging through his bag, he finally found the disk, between pages of a reference document, and put it into the drive. He right-clicked on the file and chose **Send To | Floppy drive (A)**, watching the light come on and the drive whir while it wrote to the disk. Popping out the floppy, he put it

back in his bag and logged out of the computer, not realizing that he'd not deleted the file off the computer's hard drive. He grinned one last time as he confidently strutted out of the café.

Baltimore, MD: Thursday, November 20th, 4:21 AM, 2003

The third shift was nearing an end in the control room of the storage facility. With morning coming, tanker trucks would soon be readying to take on gasoline, diesel, and other petroleum products for delivery elsewhere, further down the supply chain. The gasoline tanks were a little low, but that would change with a tanker coming to port to replenish them. There was more than enough fuel to last the day, and then some.

It was getting into the holiday shopping season, and already gasoline consumption seemed to be ticking upward. It would spike for Thanksgiving, and then stay high through to the end of the year. With the reconstruction of Iraq underway, gas prices promised to stabilize somewhat as the markets reacted to world events. The previous month had shown a strong drop in the price of crude, which was said to be acting as an economic stimulus. Which meant more demand, and more work at the facility.

Tony looked at the big board, the screen that showed the state of the whole plant. He'd worked in this facility for ages, and could remember back when the controls were nowhere near as pretty, or as centralized. Back then, it was a lot of walking and a lot of yelling back and forth. This was easier, and less dangerous. And here, the computer told you when things were wrong. You didn't need to know what the pressure ratings of valves and pipes were; when the display showed yellow or red, something was wrong. And fewer things seemed to go wrong, since you had such great control over everything. You could see little problems before they became big ones, and replacing failed components became almost more proactive than reactive.

The best part had to do with the environmental controls. The entire facility was peppered with drains to catch rainwater as well as anything else that fell on the ground, like diesel or oil. This runoff went to a central

holding pit, where the water was separated from the petroleum products that inevitably ended floating on top of it. The water was drained away, and the petroleum was dealt with in a non-polluting manner. There were specific regulations and safety standards as to when immediate action was needed, such as a situation where there was too much gas on top of the water. Having sensors report on this was fantastic, and made it easy to keep the tree huggers happy. *Well, as happy as tree huggers get*, he thought. The sensors also helped alert them to any major leakage that might occur. It had been a long time since a weld failed, spilling liquid out god-knows-where, but it did still happen from time to time.

Within one of the servers inside the control room, a burst of packets arrived from the outside world. Services stopped abruptly, running shellcode meant just for them, and then restarted to reload the altered files. Control panels became inoperative briefly, but with the shift near an end, neither Tony nor anyone else really noticed or cared.

Chapter 8

Exploit Impact

Baltimore, MD: Thursday, November 20th, 7:49 AM, 2003

The tanker approached the docking port at the facility. Slowly and carefully, the tug helped maneuver it into place, and enormous hoses were winched up to mate with connectors on deck. It was a lazy morning. The calm voyage had made the workers on deck somewhat sluggish for lack of any significant challenges over the previous weeks. Eventually everything was connected and tightened up, and the Captain informed the control room that he was ready to start pumping gasoline onshore.

What was to follow required a set of coordinated actions and proper sequencing. A pump onboard the tanker was started, and began pulling gasoline upward from within its tanks to the connectors above deck. Once the liquid cleared the deck, a siphon effect began to some degree, as vents to the tanks let in air and the pump was slowed. Valves would be opened to allow the fuel to pass through to the proper tank at the storage facility, with flow rate and pressure being monitored at both ends to avoid rupturing any of the fixtures. A final pump near the tank helped the process, pushing fuel into the tank against the pressure of what already remained within it.

This time, however, something different happened. As a technician issued a command to start the pump at tank number three, the additional code now running within the server took action. It generated a number between zero and three; this time, the number was three. As a result, the conditional statement within the code evaluated to "true" this time, and a subroutine was called.

SCADA systems operate using standard networking protocols, in this case TCP/IP. The RTUs, however, had never been designed to be robust networking systems, and were not built by specialists in networking. They were built by specialists in plant operations, and so the expertise went into their functionality. Unfortunately, this meant that the systems were prone to failure or unexpected behavior when subjected to input that deviated from what they were designed to accept. The additional code that Agpalo had designed took full advantage of this, and mangled the output that was being sent over the network to the RTU in charge of the pump at the tank.

The RTU accepted the command, and started up the pump. It also promptly locked up, its processor looping over and over again. Much like a desktop system that still showed what the user had been doing when it froze, but was no longer responding to keyboard or mouse input, it reported the same thing back to the SCADA master without change, over and over.

"Look at that. Nice steady flow at tank number three," reported the technician.

Gasoline flowed normally through the pipes, from the tanker through the dock fittings and onward, into the storage tank. The tanker gently rose out of the water as it shed most of its weight, the early morning water lapping against the weathered hull. The crew on deck moved around, keeping warm in the cold morning air.

On the bridge, the readouts for the tanks showed that they were nearly empty.

"All right, prepare to stop offloading," ordered the Captain.

His Executive Officer gave commands via radio for the crew on deck to get ready for uncoupling, and informed the control room onshore of their status. In the control room, the technician slowed the pump at tank three. Or, more accurately, he tried to, but nothing happened.

He blinked a moment, then tried again. No response.

"What the fuck?" He felt a chill as the flow rate maintained its arrow-straight line across the graph. The tanker was nearly empty, and so too would be the pipe leading up to the pump soon enough.

He turned in his seat, looking back to Tony. "Hey, Tony! Look at this."

Tony hurried over. "Jesus Christ! Stop it already! They're almost dry, you can't run that pump that hard now! What's the matter with you?"

The technician sputtered, "But that's what I'm trying to tell you! I can't! It don't respond!"

Tony motioned for the technician to slide out of his seat. "Move over." He calmed himself, and took a look at the display before trying to slow the pump down. Same effect. He had noticed the perfectly straight and featureless line that displayed flow rate over time, but didn't think anything of it at the time. That changed as he had a flash of insight. "Shit, I don't think we have positive control of pump A on tank three." The pump kept whirring, pushing more and more gasoline into the tank. The tanker's holds drained closer and closer to empty, and the time left before the pump got air ran down like a timer.

Tony kept thinking; he'd never seen this before. A pump that wouldn't turn off? "Do we have anyone near tank three?"

"Why?" asked the technician.

"Two reasons, dammit. One, to see if they can yank the power to that pump, but two to tell them to get their ass the hell away from there if they

can't! You ever see what happens to one of those pumps when they run dry?"

The technician blanched and grabbed a radio off the desktop. There might be a repair or maintenance crew nearby, if they were lucky. "All units near tank three, report in. All units near tank three, *report in now.*"

Tony pointed at one of the other men, who, at this point, was standing to the side, motionless. "YOU! Sound the alarm!"

The man jerked into action, turning to the side and hitting a large red button. Immediately, warning klaxons and red lights went on throughout the facility.

Aboard the deck of the ship, the crewmen heard and saw the commotion instantly. "What the hell…" Up in the bridge, the Executive Officer was calling to the control room for an explanation. With the pumps still running, the storage facility and the ship were bound together, unable to safely uncouple the connections between them.

Tony took the call in the control room. "Uh, yes, sir. Slight problem here, we're not able to shut down the pump at tank three, it's not responding. We're still trying to sort that out, sir. How much time do we have before you run dry?"

What the pleasant and sharp green line that cut across the moving graph in the control room did not show was that flow was actually decreasing, as the siphon effect in the tanker had changed. Once the level of gasoline inside the tanker dropped below that of the level in tank three, the pump had to work uphill to move the fuel. But that too was about to change.

The Captain had an idea. "Why don't we just close the valves on either side of the pump and try to at least contain the pump?"

"The problem with that, sir, is that if you just clamp the valves shut like that, you'll get a pressure wave back. It could blow out a weld, or worse. I don't think that's a good thing to try. Perhaps just shutting the valve at your end? You'll still get a bit of a wave, but it'll be closer to an open end, so it might not do as much harm. Hang on a second, sir." Tony looked at the technician. "Anyone near there who can help us out?"

The technician shook his head.

Tony nodded grimly and reported back to the phone. "Okay, sir. We don't have anyone near the pump who can cut power to it, so it's up to us. How about my suggestion?"

As the two discussed their diminishing options, time ran out. The holds in the tanker ran dry, and the last of the fuel was pulled vertically upwards to the couplings on deck. Once they cleared those, it was a downhill run for thousands of pounds of gasoline, with no suction resistance behind it. The pump whirred faster abruptly, as it went from being the source of flow to an obstacle to it, and the bearings shrieked from the change in forces applied to them. None of this was reported by any of the sensors attached to it, as the RTU to which they were reporting was still looping, reporting the same outdated information over and over.

Then, things went downhill. The last of the gasoline reached the pump, which was not intended to run dry. The speed of the impeller spiked far beyond its limits, blending air and fuel in a frothy mess as the blades tried to gain purchase on some liquid. The bearings started to deform as the motor heated up, until the impeller suddenly froze. The force of the pump's last act fractured two welds, which promptly sprayed fuel into the open air, the siphon effect of tank three pushing against them. The electric motor within the pump kept pushing against the frozen bearings, heating further, until the growing pool of gasoline around it ignited.

The crew on the deck saw it first, as a loud *whoosh* in the distance followed the sight of a small mushroom cloud caused by the igniting fumes over the failed valve. They stepped back a moment, seeing the raging pool of gasoline ablaze in the distance, and cringed as their eyes all followed the route of the pipes that led from the center of the blaze back to the couplings right next to them.

"Tony! Fire at pump A, tank three!" Fortunately, the fire detection systems ran on an entirely different set of machines, and were unaffected by Agpalo's handiwork.

"Oh shit! Fire suppression teams, send them out!" He turned back to the phone. "Sir, your problem just got solved for you. Close the valves at your end, the pump has failed at ours. And you'd better get out of here."

Fortunately for the ship and all aboard it, gasoline requires a good bit of air to burn, and nowhere near enough air was in the fumes that filled

the pipe between them and the refinery. On board, their valves closed, sealing them off from the burning conduit in the distance. The deckhands received word to uncouple the ship, which they did with remarkable speed and efficiency, enthusiastically casting them off the deck. Meanwhile in the bridge, the Captain ordered the engine room to prepare to make full speed, and the pilot was directing the tug to get in place to push them away from the facility. Nothing good could come of a gasoline-fume-filled tanker so close to a burning storage facility.

As the fate of the tanker was becoming more certain, things were becoming less so onshore. Gasoline continued to spill from the fractured pipe joints, adding to the intensity and size of the fire. The facility's fire suppression team arrived with their engine, but there was little that could be done to douse a fire that was still growing, fed directly from a full storage tank. And as the manual valve that could close off that supply of fuel was in the center of the blaze, not much could be done at all. The firefighters retreated, instead deciding to focus on keeping the blaze from involving any other tanks.

Tony sat in the chair in the control room, slumped down, unsure of what to do next. There was only one thing remaining to do. He picked up the phone and dialed a hotline number to contact corporate headquarters to report an incident.

Dallas, TX: Thursday, November 20th, 2:08 PM, 2003

"All right, tell me what we've got here. It sounds like the whole company's going to hell in a hand basket, so let's get to the bottom of it." Jim was a senior executive at the oil company, and had asked for this briefing.

Bill, a promising younger suit, faced Jim, his notes in hand. Looking past the senior executive, the scenic view of Dallas was visible through the floor-to-ceiling office windows. Bill had never been this high up in the building before, and had only heard about the view. This was an unexpected opportunity for him to advance within the ranks of one of the largest oil corporations in the world, and he wasn't going to waste it. As such, he had spent the last few hours mustering resources to get an overview of the strange events

of the day. "As of an hour ago, nearly every transfer and storage facility in North America has suffered some kind of incident. We have several fires, two explosions, a number of miscellaneous major-impact incidents and a large number of environmental impact incidents," he reported, referring to a spill that managed to escape the confines of a facility and pollute the area's soil or water table. "There appears to be no clear pattern at the moment, but they all seemed to begin happening this morning, oddly enough."

Jim sat back, alarmed by the report. "What's the impact on our supply chain?"

"At the moment, we are stopped. Fortunately, in most cases the plant managers are confident that they'll have things back under control by the end of the day. In cases where large fires or explosions have taken place, there will be diminished functionality for a time, and in other cases there'll be diminished capacity that can be handled by carefully increasing plant activity to compensate."

"Do the plant managers know this is happening to anyone besides them?"

"Apparently not, and it's my belief that we should keep it that way. They have their hands full at the moment with their own systems, there's no point in giving them more to think about. We're still waiting for the full reports with the exact details of what transpired, but should have them by the end of today."

"Okay. I want you to keep an eye on this. I don't think I have to say that it sounds pretty suspicious how all of these problems happened at once. I'm assuming we've ruled out sabotage?"

"Yes, sir. I just don't see how any group could have pulled it off. To get someone into every facility? Impossible. It just can't be done, no group could be that large or that effective. And the tree-huggers…well, it's just not their style. They'd want to break things, sure, but not like this. Nearly every incident has had some kind of environmental impact, whether it be from smoke, fumes, or spillage. No, I don't think this was sabotage."

"Now, what about the press? Have they picked up anything?"

"Not that we can tell. The majority of incidents have only involved minor spills and a handful of small fires, what we've officially declared as *minor equipment malfunctions* to any media outlet that has asked. The loca-

tions are geographically dispersed, and though we've had some coverage by a local news crew or two, no one on the National scene has picked up the multiple incidents or the fact that we can't unload the ships. Throw in the fact that the war in Iraq is still monopolizing the airwaves, and we're flying under the radar so far."

"Good. Let's make sure we keep it like that." Jim nodded signaling an end to the meeting. "Very well, come back to me with a status update in the next two hours, at the latest. Good briefing."

"Thank you, sir." Bill gathered up his notes and left.

Jim considered the next steps to follow in the matter. While he doubted the problem would last for long, the nature of it was strange enough that it probably required a certain degree of disclosure to the Department of Energy, which likely would have heard already. He really didn't relish the attention it might garner, but he also tended to believe that getting the bad news out early, in its entirety, was the best way to handle something like this. The EPA would be getting the reports of all the spills at any rate, and that was being handled through other channels, so he didn't concern himself with that aspect of it. He called his secretary. "Janice, get me the DoE. I need to report a potential issue with the distribution chain."

Washington, DC: Thursday, November 20th, 10:28 PM, 2003

Agpalo and Lualhati had fired off their final commands to the compromised VPN servers just before they attacked the petrochemical facilities. This attack, however, was a bit more subtle. The servers were randomly destroying sectors of data on their disk drives, slowly rendering themselves less and less stable. In the process, they were also affecting the manner in which the drives were formatted, thus making the disks unusable without a low-level reformat, something that few engineers knew how to do anymore. Such a task required knowledge of the specific commands to send to the disk controllers, even if someone did know precisely how to use them. And at that point, the servers would still be down, and in need of

reinstallation. And no matter how quickly they were set back up, Lualhati and Agpalo could take them back down again much more quickly.

The server that Reuben had examined only a week earlier was in the middle of this process, and while it had already defiled a quarter of its own disk space by this point, it was fortunate enough not to have affected anything terribly critical yet. And so it continued on, periodically destroying more and more of itself, for as long as it could continue to do so. Eventually, some critical bit of data would be affected, and the server would crash or lock up in some mysterious way. Attempts to restart the server would fail, and attempts to restore from backup would be stymied by the low level of damage caused to the magnetic patterns on the disks themselves.

Elsewhere in the nation, many other servers had already failed. Unlike this one, they were not intended to handle a large volume of connections, and thus were built with less beefy hardware and smaller drives. Smaller drives meant that less time would pass before a critical piece of data was eradicated; it was simply a matter of probability. And soon enough, the server in the Hoover Building would fail as well.

Washington, DC: Friday, November 21st, 8:10 AM, 2003

"Oh man, that sucks." Reuben needed to put more gas in his car before going to work, but the gas station was plastered with signs indicating they were out. "Guess they didn't pay their bills on time," he muttered as he drove back out of their driveway, trying to remember the next-nearest location where he could fill the tank of his sports car.

He drove through the city, looking for a place where he could fill up. He was running later than he wanted, but probably did not have enough fuel to make it all the way out to Sterling, and didn't care to gamble on it. As he worked his way out of the city, he focused his mind on what he had to accomplish that day, in hopes of getting out of the office somewhat on time.

Traffic out to work was normal enough, and Reuben smiled at the backed-up traffic that was entering the city, happy to have a reverse com-

mute every day. It was a strangely warm day for late November, and he had put the top down, relying on the car's heater and his lightweight jacket to keep him warm. He turned off the minidisc player, just enjoying the sensation of driving with the top down. He knew there would not be many more days like this before winter took hold, and he would have to drive with the top up every day for months.

He finally arrived at work, and took a parking spot in the back of the lot. He grabbed his bag, and strolled into the office building. Only a day before he had finally relaxed and let go of recent weeks' events, managing to focus on his job again, doing the work at hand. It was going to be a long day, but not too long.

Portland, OR: Friday, November 21st, 11:00 AM, 2003

Roger picked up the phone. "News desk, this is Roger."

"Hey, Roger, it's Anthony. How's everything?" Anthony was Roger's brother-in-law. While Roger hadn't cared for Anthony at first, he came to like the man, and they became friends, albeit friends who only spent time together occasionally. Anthony had bought a small chain of old gas stations, and was extremely busy with fixing them up, learning how to run the business better, and various other tasks that were imposed upon the entrepreneurially minded.

"Hey! Can't complain. How about you? Taking good care of my sister?"

"Doing the best I can! It's been hard, with work being so busy and everything, but I'm about to start redoing the last station. When that's done, then I'm going to take some time and carry her off to vacation somewhere exotic. Don't say anything though, it's a surprise. Oh, do you have any ideas of where she might like to go?"

"Funny you should ask. She's always been curious to go to Tahiti someday. But don't let that sway you too much. For all I know that was just talk."

"Good enough. Oh, but that's not what I was calling about. I've got a strange question for you. Have you heard anything about gas deliveries today?"

"Uh, no. Why?" Roger's curiosity was suddenly piqued.

"Well, I was expecting a delivery yesterday, and it didn't come. Not today either. I called up to ask what was going on, but they sounded like they didn't want to tell me. They just said they were running a bit behind, some drivers had called in sick. I don't buy it."

"Interesting." Roger had noticed two stations that were out of gasoline entirely, and the third, where he filled up, was out of hi-test. And neither of them belonged to the same company as Anthony's stations. "I haven't heard anything, but I'll look into it."

"Great! I thought it might interest you. Did you notice anyone else being out? I did, but I figured it could have been a coincidence."

"I don't think it is, Tony. I'll check into it though. Thanks for giving me a call."

"Sure thing. Talk to you later."

"Sure enough." Roger got off the phone, and got up to talk to the news director. *There might be a story here*, he thought.

Washington, DC: Friday, November 21st, 3:13 PM, 2003

Reuben leaned back in his chair, stretching. He'd been banging away at the deliverable for hours, and needed to take a break. He had decided that the next time he was good at something he hated to do, he would keep his skill a secret. He was sick of writing.

He got up and stepped out of his office partly to go grab a Coke, but more to just have somewhere to go. He'd thought of having coffee, but feared not being able to get decent sleep later that night. He hadn't been sleeping well lately, and it was forming a vicious circle where he was stressed about sleeping, which kept him up, which in turn added to his stress.

Walking down the hallway, flanked by offices of other geeks quietly working away, he realized how strange his life felt now. He'd been through so much in the past few weeks, he had lost his sense of direction as to what was normal for someone of his profession. And he sensed that it

wasn't over, that he was just waiting on the sidelines until called back into play. It was such a profound concept, the notion that he was involved in something as large as he suspected, and yet so powerless and anonymous. He'd learned to consider it pleasant in its own way. It meant that he got a chance to rest, to contemplate, and most of all, to be left alone.

He shot some change into the machine, and grabbed the soda. Popping it open, he leaned back against the wall and took a long drink. *Well, one thing is for certain,* he thought to himself as he smiled. *My conscience is totally clear. Brian was exactly right.* He took another swig, and just let himself relax. *And I sure did get into some interesting stuff.*

He walked around, looking to see if anyone else was taking a moment from being a worker bee, in hopes of some kind of conversation. No luck, nobody was available. It was a very boring work environment, with lots of bland engineers. Lots of thirty-something dads who didn't like having kids, but figured that it was what they were supposed to do, along with the requisite purchases of minivans and homes far out in the suburbs. *How did I start working here? I'm nothing like any of these people.*

He went back to his desk and put the Coke down next to the keyboard. He didn't have much more to do before he felt justified in calling it a day. He'd been productive today and wasn't going to stay late. He might even be done by the end of the day on Monday.

He went back to work, figuring out where he left things. *Ah yes, the database server.* He was writing up the deliverable for a vulnerability assessment that had been done a couple of weeks earlier. Some of the data was collected by a second group of engineers, and since he hadn't been there at the time, it took a lot more effort for Reuben to draw his conclusions. He never trusted anyone else to do data collection for him on these jobs; he always feared they would miss something. The real fear was that since it was his name on the deliverable, he would be the man who had to face the music for any mistakes.

He was just getting back into the flow of it when the phone rang.

"Hello?"

"Hello…Reuben?" The voice was familiar.

"Yes?"

"Hey, it's Jane."

Reuben's blood ran cold. He knew instantly what this was. "Hey! What can I do for you?" His mind silently begged God that he was wrong.

"Well, there's been some trouble with the VPNs. Most of them. Thought I'd give you a heads-up, so you won't be surprised."

Oh well. At least he probably didn't have to worry about getting fried for breaking the NDA after all. "Ah, thanks."

"Just sit tight, there's nothing you'll be able to do yet. But as soon as the opportunity presents itself, I'll be bringing your name up. Be ready to get a phone call, and drop everything. It'll happen pretty quickly, if you were right. And now I'm sure you were right."

"What's happening?" Reuben was suddenly dying of curiosity. He wondered what the symptoms were, what the attack's character was. How was it manifesting?

"I can't say anything without breaking the law, so don't worry about it. You'll find out yourself soon enough. Just stay put, and be ready, okay buddy?"

Reuben took a deep breath, and exhaled. "Alright. I'll be ready. You have my cell phone?"

"Sure do. I won't be the one calling you, just so you know. I'll talk to you later, have a good afternoon. And get some rest, you're going to need it."

"That bad, huh?"

"Yeah, pretty bad. Take care."

"You too…and thanks."

"No, Reuben, thank you. Really."

The phone went dead. Reuben just held the handset for a minute, thinking about what she had said. *Well, well, well. Sounds like everything turned to shit pretty fast.*

He figured he'd better finish the deliverable before he went home. Nobody would be too happy if he was the holdup on this project because he got pulled aside for some other thing outside of work.

Washington, DC: Saturday, November 22nd, 9:03 AM, 2003

The cell phone rang again. Reuben rolled sideways, groggily snatching it out of the charger on the nightstand. "Hello?" His voice sounded a bit creaky from sleep.

"Hello, I'm looking for Reuben Lev."

"Speaking." *Here we go,* he thought. He woke up a bit more, steeling himself for what was coming.

"This is Special Agent Jackson. Where are you located?"

Reuben cringed. Maybe this wasn't what he was expecting. "Uh…what is this about?"

The stiff and terse voice at the other end stuck to business. "There's no cause for concern, sir. You're not in any trouble. But I cannot discuss the matter over the phone. My instructions are to come pick you up and bring you in for a meeting."

Ah, so this is how it works. I wish to shit Jane had let me know that it would be like this! Fricking scared the hell out of me. "Okay, do you have a paper and pen ready?"

"Yes sir."

"Where are you coming from?"

The man at the other end answered, and Reuben thought a moment before rattling off directions on how to get to his apartment in the least amount of time. He had no doubt that the agent would not get lost on the way, and thus he only had a bare minimum of time to get ready.

"It should take you about ten to fifteen minutes. I'll try to be ready, but if not, just hang tight. Give me a call when you get here, and I'll come down."

"Got it. See you soon."

Reuben got off the phone, and out of bed immediately. Brianna rolled over, looking at him with worried eyes.

"Was that 'the call'?"

Reuben stopped moving, and looked back at her. "Yes. I'm sorry, but I have to hurry. I don't have much time, and they're sending a car to pick me up."

"Be careful?"

Reuben nodded, lying back down on the bed next to her. He gave her a warm hug. "I will, but I think that the risk to me is over now."

"I hope so. It's been hard, seeing you so stressed."

"I know. It's not over yet."

"I know. Okay, you need to go."

Reuben smiled. "I love you."

"I love you, too. Don't be late."

Reuben chuckled as he got up and started towards the bathroom. "Late, hell. They should have given me more notice! Don't they know I have important things to do today?"

"Like what?" called out Brianna, raising her voice to be heard as Reuben started the water in the shower.

"Uh, something! Grocery shopping, perhaps?"

Seven minutes later, Reuben was dry, standing in a towel trying to figure out what the hell to wear. *What do you wear to this? Emergency meeting with God-knows-who at the Department of Justice. Nope, never read up on the etiquette for that. They always say be better dressed than anyone else. Perhaps I should rent a tux?* He settled on khakis and a nice shirt, figuring it would be better not to look too desperately willing to accommodate the sudden imposition, but wanting to be professional about it at the same time.

He heard his cell phone ring as he was buttoning the shirt, and ran into the bedroom to get it. Brianna was at it first, and tossed it to him as he came through the door.

"Hello?"

"Agent Jackson again. I'm downstairs."

"Okay, I'll be down in a couple of minutes. Getting dressed now."

"Okay sir, I'll be waiting."

Reuben hung up, and put the phone down on the bed. He finished buttoning his shirt and tucked it in. He grabbed his keys and wallet, putting the phone on his belt, and grabbed some shoes. He decided to wear his hair down, letting it air-dry to save time.

He walked to Brianna's side of the bed and leaned down to kiss her on the forehead. "Wish me luck."

"Good luck, sweetie. Knock'em dead."

"Thanks. I'll give you a call when I have some idea what's going on, or how long I might be. Or if it's been a long time and I still have no idea of either."

"Should I wait for you, or just go on with the day?"

"Go on with the day. I don't think they'll be done with me too soon. Not if they sent a car like this. It's a feeb, too."

"Wow…Mr. Important!" She laughed.

Reuben blushed a bit. He did like the attention, and that he rated someone being sent to pick him up. "Yeah, yeah. Whatever. I'll talk to you soon. Have a good day."

"You too. I'm so proud of you. Good luck!"

Reuben smiled as he walked out of the bedroom, grabbing his jacket on his way out the door.

A minute later he was downstairs, where a laughably typical black unmarked car was waiting in front. He approached the man sitting in the driver's seat.

"Hey, I'm Reuben."

The man looked him over, and got out of the car. To Reuben's surprise, he opened the rear door for him, much as a limousine driver would. "Here you go, sir."

Reuben was taken aback at the courtesy. "Uh, thank you." He got in, unsure if he felt like a celebrity or a prisoner at the moment.

The back of the car was enormous, larger than the entire interior of his Miata, and more open as well. "Wow, I had no idea these cars were so nice inside. And clean, too."

Agent Jackson put the car into drive, and the car smoothly accelerated. Reuben suddenly noticed that the police lights on the car were flashing, which was a surreal thing to observe from inside the car. As they got to the intersection, Jackson pulsed the siren, slowing enough to safely blow through the stop sign at the end of the block.

"Whoa. Okay, I guess this is more than I had in mind. Can you tell me anything about the meeting I'm going to?"

"I'm afraid I don't know much, sir. I was told to come get you, and to do it as fast as possible while getting you there in one piece."

Reuben felt his blood chill a bit. "I see. Thanks. I'll just let you drive now, if you don't mind, then."

Agent Jackson blew through another intersection, the siren blaring. "That's probably best, sir."

Reuben sat back, losing the battle with his fear and apprehension, but putting up a good fight just the same. As an afterthought, he put on the seat belt. *Relax. They sent for you because you can do this. They didn't just pick you at random. You are Plan A, and there is no Plan B. So get your head together, get your shit in order and get your game on.* He inhaled and exhaled, fighting to relax as the car lurched back and forth, braking hard just before every intersection and at any group of cars that blocked the way.

Agent Jackson must not have used the lights and siren on the way to Reuben's apartment, because in half the time it had taken him to arrive in Adams Morgan, he had bypassed the Department of Justice and brought them straight to FBI Headquarters, Reuben was grateful that it was over so soon, getting his drivers license ready as they rolled up to the entrance to the underground garage. The guard stepped up to Agent Jackson's window, who flashed his credentials and was waved through.

Reuben saw Jackson's eyes look up in the rearview mirror. "You won't need that, sir," referring to his license. "They're expecting you, and I have your visitor's badge already."

Reuben shrugged, and put the license away. *I might as well just dump all my assumptions and preconceptions right now, because I am clearly* not *in Kansas anymore.*

Agent Jackson parked in a spot right near the entrance to the building, and escorted Reuben in. Looking around, Reuben thought back to early childhood and visits to Washington with his family. He'd been in this building as a child, and remembered the tours. But he'd never been in any part of the building that seemed significant, he realized. *What have I gotten myself into?* he wondered.

A few minutes later, he was walking into a conference room, and was shown to a seat. The room was filled with several important-looking people, including Wilkens. Wilkens did not look well, and looked even

worse when he saw Reuben enter. *Hello again, asshole,* thought Reuben as he stifled a smile. He guessed Wilkens didn't know he was coming. Sitting in chairs against the walls were a few secretaries and some other less-important looking people. Among them was Jane; who looked at Reuben, smiling slightly. She gave him a wink. Agent Jackson went back outside and the door closed.

"Welcome, Reuben," commenced the man sitting at the end of the table. "I called this meeting, and to cut things short I'll just introduce myself. I am Mark Johannsen, and I am the CIO for the Department of Justice. The people around this table and elsewhere in the room have other duties related to the current situation, specifically Jeff Montoya, the FBI CIO, and James Smith, a member of the FBI's Cyber Security Division, who, as you can well understand have a deep interest in this and will be carrying on their own investigation as we move forward with ours. I can only assume that you have some idea why you are here right now, but let's dispense with assumptions. I understand that you're the wizard who predicted our current issues."

Reuben stepped up to the plate. "These 'issues'…are with your VPN, I take it?"

The man nodded.

"Okay. What's going on right now?"

"I'll let Wilkens fill you in on that one. I take it you've met before?"

Reuben smirked. "Only once. About a week ago."

"Well, good enough. He'll fill you in."

Wilkens sat forward, resting his forearms on the table with folded hands. "Yesterday, VPN gateways in our field offices started to fail. This failure grew as time progressed, and now involves every single gateway."

Reuben whistled. "No exceptions? They're *all* down?"

"Yes, a complete loss," admitted Wilkens reluctantly.

Reuben wasn't going to let him off so easily. "What are the possible explanations for how that could happen?" He was going to press his advantage, now that he had it. And hopefully, if he made a good example of Wilkens, he could assert his dominance, and prevent any other bullshit from happening again in the near future.

He paused slightly giving Wilkens a chance to answer before continuing, "So I take it that's not a hardware problem is it? So, why not just restore from backup?"

"Well, we're not entirely sure yet. The drives seem to have become somewhat unreliable. Replacing them resolves the issue, but most sites do not have spare drives on hand."

Reuben was surprised by that last detail. "Now that is interesting. What's wrong with the drives?"

Wilkens nodded to someone sitting across from him at the table, who leaned forward. "I can answer that. From our forensic examination of the gateway here, it would seem that random parts of the drives have been overwritten. The problem is that the disks have been…it's as if small parts have had the formatting removed entirely, or had it changed enough to render it unusable."

"Low-level format?"

"We think that would work, but we haven't tried yet. First we want to get a sense of the problem we're up against."

Reuben couldn't maintain diplomacy for one second longer. "Well, jeez. I can tell you that. You've been owned, dumbass." Reuben saw a few smiles being repressed. "I've been saying that for a week now, and I tried to tell you that it would happen for longer than that. And before *that* I was telling you that you were vulnerable to it. So tell me, how many people in this room, besides you, of course, knew any of what I had been saying?" Reuben could feel all the anger and frustration from all of the events leading up to this bubble out of him. His face felt hot as he sarcastically vented at the source of all of it. "What, you didn't tell everyone that your rollout was inherently *unsafe?* Good job, skippy. "

Johannsen glared at Wilkens, who sat back in his seat. Johannsen redirected to Reuben, his visage softening. "Yes, all of this has come to my attention in the past 24 hours, and for all of that I apologize. I imagine it must have been very frustrating. But what we need to do now is put the past behind us and work on a solution. We were wondering if you had any suggestions."

Reuben sat back for a second, playing with his goatee as he looked up at the ceiling, thinking. After a few moments, he started speaking. "Okay. I

need more information to be able to come up with ideas, though. First of all, what are you using the VPN for, exactly? What is its role?"

Johannsen nodded. "We use it for communications between all of our agencies, and when applicable, their field offices. The primary customer, obviously, is the FBI, and they started using it quite heavily from the very beginning. Some connections, like the one between here and the CIA, for example, are on dedicated secure lines for obvious reasons, but otherwise the VPN is the foundation of digital communications from site to site."

Reuben nodded back. "That's a tough one, then. Even if you get it all back up and running, you'll just get taken back down." He looked around the room for any other familiar faces. "Uh…is anyone from ZFon here? What do they say?"

"No, the vendor isn't present here. I feel that perhaps they have been…overrepresented…within our organizational planning."

Ouch! Sucks to be them. I bet their stock won't be going up now, will it?

"Okay. I see a fork in the road. To the left, their latest and greatest version is still vulnerable. And to the right, it isn't. If the truth leads to the right, then that's your answer. I doubt it's so different that you couldn't use it in lieu of the version you were running before…2.2, wasn't it?"

"And if our path leads to the left?"

"Well, then you're really fucked, to put it lightly. You're going to need to drop some serious money to get something else. That's the bad news. The good news is that there are lots of great VPNs out there. I've used Cisco's and Checkpoint's products, and love them both. But you're going to need a lot of money to forklift your existing product out, and a small army of engineers to put it in place quickly. What are your options for running without one in the interim?"

Johannsen shook his head. "Not an option. We're not set up to be able to separate out sensitive from non-sensitive data. And we absolutely cannot put that data into the clear. I believe we'd actually be committing a felony if we did so, as ironic as that may be."

Reuben nodded. "Okay, I thought as much. Just had to ask." He exhaled, calming his thoughts again. "All right. Do you think you can get ZFon to give you a free upgrade?"

"Oh, I'm quite sure of that."

"Good. Let's see if their latest and greatest is safe, then, and see which way the path leads. How talented are your engineers at the field offices? Can they learn how to stand up a totally different VPN system over the weekend?"

Johannsen looked to another man at the table. "Jacobs?"

The man leaned forward. "It depends. At some field offices, yes. At others, definitely not. But what's good is that the better people are at the larger field offices. It's definitely an option."

"All right then, now we're talking. Start getting ready to train them, and figure out who gets your business in case the path leads that way. It's going to be expensive, but it can be done. I'm guessing that you must have some kind of way to pay for such an emergency."

"We can figure it out. Our strength in this is that we're a known quantity, and we can do acquisitions on P.O. The rest can be figured out in budgeting later. How do you plan to determine the suitability of ZFon's current software revision?"

"I have an idea, but I'll need support to do it. And some time. Uh, this is a strange question, but if I needed you to, could you fly someone over here? From the West Coast?"

"Reuben, we'll do whatever it takes to recover from this, as fast as possible. And yes, we do have access to jets that can serve that purpose."

"Wow. I was thinking you'd buy him a ticket on Delta or something. Okay, then." Reuben suddenly realized that he had brought nothing with him, especially his PDA. He didn't know how to contact MadFast from memory. "I need a few things from home, before I can look into the option I'm contemplating."

"Agent Jackson can get them for you, if you like."

"Great. Let's go with that for now. I need your permission to discuss this with a professional colleague of mine. He's the guy who helped me with the original assessment of ZFon's VPN."

"No problem, we'll send an agent to go bring him in."

"Wait, you don't understand. He's in Seattle."

"Ahh, the question about the jet. Okay. I have only one objection, which is that you not discuss any of this over open phone lines. And of

course, we're accepting your word that he can be trusted, so if he should happen to breach security, you will be held responsible with him."

"Uh, okay. And I have no problem tying my fate to his actions. I've done it before. But how do I talk to him, then?"

"We could send someone from the field office to his home, with a STU." He pronounced it "stew."

"A what? Stew?"

"S-T-U. Secure Telephone Unit."

"Oh, an encrypted phone?"

"Precisely."

Reuben grinned. That would be a hell of a wakeup call for MadFast. He could imagine it now. *Excuse me, I have an encrypted phone call for Mr. Frank Rizetti. Along with the encrypted phone.* That would be a riot.

"That's perfect. I won't know until I speak to him if I need him to come or not."

"Where's he coming from, again?"

"Seattle."

Johannsen motioned to someone sitting off to the side. "Jim, see to it there's a VC-10 ready in Seattle as soon as possible, would you?"

Reuben stepped in. "Uh, hang on. That might not be necessary."

Johannsen addressed Reuben as "Jim" left the room to complete the task. "Yes, but if it is, we can't afford to waste time waiting for a plane to arrive there and refuel. As I said, we will do what it takes."

Reuben gave up on being surprised, and just decided to consider himself a moron and out of his league here. "Ah. Okay. I need to call home, and have my girlfriend get together the stuff I need. Is there anything else we need to discuss here?"

"Gentlemen, do any of you have any questions?" Johannsen looked around the room. "No? Okay, Reuben, I think we're all set. We're going to discuss some other things, but you're free to go and get what you need to move forward on this. If you need anything at all, tell Agent Jackson and he'll get it for you."

"Great. Thank you, I really appreciate it. I will help you, and help get you through this. And I should let you know that for all the agony of not

being able to prevent this, it really does help to be able to fix it now that it has happened. I'm grateful for it, thank you. It means a lot to me."

Johannsen smiled. "You are very welcome, but I think it's us who should be thanking you. Any doubts I had about bringing you in," he said as he leaned forward to look at Jane in a very obvious manner, "have been entirely resolved. Welcome back aboard, Reuben. Make us proud."

Reuben stood up. "Yes, sir!" He went outside, noticing that Jane stood to follow him out.

Once outside the conference room, Reuben realized how tense he was, as he relaxed. Jane was right behind him, and Agent Jackson, who had been sitting patiently, stood.

Jane looked at Reuben, beaming. "Kick ass! You rocked that meeting, Reuben. Good job."

"Yeah, let's see how well I can handle it from here. Talk is easy."

"You don't have to do anything you haven't done before, I'm sure. It's on a larger scale, but so are your resources now. Don't be shy. Ask for anything you need. The point here isn't efficiency. Don't be afraid to waste resources on options, if it might mean getting things back in order sooner."

Reuben weighed that in his mind. "Makes sense. Okay, will do." He turned to Jackson. "I need a phone, and a few things from home."

Jackson nodded. "Follow me, sir."

Reuben turned to Jane. "Want to tag along? I could use a guide."

Jane grinned. "I wouldn't miss it for the world, are you kidding?"

"Come along, then."

The trio walked to an empty office that seemed to be in the IT department. "Here you go, sir," directed Agent Jackson.

"Uh, the 'sir' thing is making me nervous. As long as we'll be working together, call me Reuben?"

Jackson smiled. "Okay. I'm Paul." He held out his hand.

Reuben smiled back. "Ahh, much better, Paul." He took the hand and shook it. "Nice to meet you. I figure your job is to show me around, keep me out of trouble, that sort of thing, right? And remember, be informal. We're all going to be friends here, and we're all in the same boat."

"If you say so. In truth, I've never seen anything like this before."

Jane spoke up. "How long have you been with us, Paul? Oh, and I'm Jane, by the way." She extended her hand.

Paul took her hand, shaking it. "Good to meet you. Not too long. I graduated just last year."

"Ahh, so that's why you got this duty. Well, they must trust you, because Reuben here is our best shot at getting a handle on this, to give you the inside scoop. The guy heading up the VPN deployment screwed the pooch, and Johannsen doesn't trust the internal staff now because of it. You're looking after a very, if temporarily, important man."

Paul looked at Reuben. "I was told as much, and I tend to believe it."

Reuben winced. "Uh, okay. I need to make a phone call now. I'll be in the office if you want me…" And with that, he went in, and dialed home.

"Hello?" It was Brianna, sounding a bit concerned. The caller ID must have shown something fairly interesting.

"Hey, Bri, it's Reuben."

"Hey! How's it going?"

"Oh, I am WAY down the motherfucking rabbit hole, let's just put it that way. The surprise phone call and driver coming to pick me up has been the most normal part of the whole day so far, I think. I need a few things, and someone will be coming by to pick them up. Can you get them together for me?"

"Sure. Going to be a while, huh?"

"God yes. We might be flying in MadFast via private jet."

"Damn. Wow. I see. So should I plan on dinner by myself tonight?"

"Uh, yeah. And breakfast, lunch and dinner after that, I think. I need to do a lot of work before I will even know how much work I'll have left to do. It's big. But the good news is that I'm the flavor of the day now. Bitchboy is in the doghouse, and I've even gotten to yell at him in front of his boss." Reuben was struck by how odd it was to be speaking that way about someone who had so much power over him a week earlier. *Oh well, reversal of fortunes, eh? Welcome to Washington.*

He could hear Brianna's smile as she spoke into the phone. "I bet that felt good."

"You have *no* idea. Okay, I need to get on things, so let's get back to it. Get a paper and pen. Ready? Okay, here's what I need…" He listed off the items, including some clothing and his travel kit.

"Wow, long list. I'll get it together. Overnight bag?"

"Yeah, perfect. Special Agent Jackson…call him Paul, and introduce yourself, he's a nice guy…will be coming by to pick it up."

"Special Agent…He's a fed?"

"Yeah, but don't hold that against him. Nobody's perfect. Thanks for getting everything together for me."

Brianna laughed. "You're welcome. Anything for my superman. I love you."

"I love you too. Talk to you later."

Reuben hung up, and stepped out of the office. "Uh, is this my office or something now?"

Jackson nodded. "Yes, this is you. Is everything ready for me to go pick it up?"

"Yep…well, it will be by the time you get there. Unless you drive up like you drove here, in which case you might be waiting a minute or two."

Jackson smiled. "Be back soon, then. Jane, you want to take care of him while I'm gone?"

"Sure. I'll make sure he doesn't burn the place down. But don't take too long, I can't guarantee anything."

Jackson grinned back and walked down the hall.

Reuben put his thoughts in order, trying to figure out what he could do while he was waiting. "I might need a lab."

"Follow me, I'll get you set up. Get you a room, and any hardware you need. I think we can borrow some things from the forensics lab."

"Great! I also need some index cards and pens, and some post-its."

"Office supplies, this way!"

As Jane led the way to the supply closet, and Reuben grabbed what he needed, he became aware of just how intensely hungry he was. "Uh, what do you do for lunch around here?"

"Hungry?"

"Hell yes. It just hit me."

"Why don't we wait until Paul gets back, and we'll see about eating after that. You need to call Frank, right?"

"Oh yeah. Which means I need his address, which means…yeah, once Paul gets back I can sort that all out. I guess I'll be giving his address to someone, and then they'll have someone show up at his home with the STU?"

"Probably. Will he be there?"

"Well considering the time of day, it'll still be morning. And it won't be early enough that he'll still be up, but he'll definitely be sleeping. Hell of a wake up call for the guy. This is going to be a hoot!"

Meanwhile, just on the other side of the Mall, where Saturday morning tourists were enjoying the beautiful autumn day, another meeting was taking place in the Department of Energy. The problems that plagued petrochemical storage facilities were pandemic, and the impact was already being felt as gas stations began to run dry. What one plant manager took for a single bizarre issue was viewed by the parent company as a freak outbreak of issues within their distribution network. In fact, the problem cut across nearly everyone, including the storage sites for the Strategic Petroleum Reserve, the enormous emergency supply of crude oil that the government maintained in case of emergencies. Soon, airports would also be affected, their supplies of avgas and aviation kerosene running out as well. With diesel also running low at gas stations, trucking would soon be at risk as well. And nobody had any answers yet.

Washington, DC: Saturday, November 22nd, 12:21 PM, 2003

Reuben looked at the STU. It was like a standard desk phone, except larger and with some added buttons. "Uh, you'd better dial for me. I have absolutely no idea how the hell to use one of these things."

Jackson grinned and started dialing the phone. At the other end, a still-sleepy MadFast was sitting in front of a different STU that was set up in his apartment. His reaction to the fed's arrival had not been entirely warm, until he learned that the Special Agent was merely the courier bringing

the phone. After that, his fascination with the situation took over and he waited anxiously to find out what was going on.

The phone in Seattle rang, and Reuben waited for it to be answered. Considering that the phone call had been arranged, it seemed to be taking a long time for MadFast to pick up.

"Um. Hello?"

"Hey man! Guess who?" Reuben grinned into the phone, savoring the drama of it all.

"Uh…Reuben?!? What the fuck…okay, why are you calling me like this? Is there something you haven't told me all this time?"

"Absolutely not. But things have gotten very interesting, and I've been pulled in to help fix it all. Obviously, the attack has hit, and they're totally screwed now. I might need you here to help me with some things, and you'll get paid well for it. Don't worry about getting in trouble from missing work, these guys are prepared to make anything okay to make it all work for you."

"How willing are they?"

"Well, right now a private jet is being readied. If you're willing to come on board, the gentleman who brought you this phone can help you pack and drive you to the airport, right now."

"No shit?"

"No shit. Like I said, they need us now, and they know it."

"Why the change? I mean, they needed us before too but you'd hardly have known it."

"It's just politics, don't sweat it. That problem is dead. I can tell you about it later. Right now it's more important to stick to fixing a huge network."

"What do you need to do?"

"Okay, the problem is this. Their entire VPN infrastructure is hopelessly borked now. The servers are eating their own drives, basically. And they could just reinstall…"

"But then they'd get hacked again all over."

"Right. So they can upgrade, but only if the latest version is safe."

"Which it may not be."

"Yes, I know, and I told them. That's where we come in. The first thing we need to do is figure that out. We've got a lab being set up now. By the time you get here we'll be entirely ready. If they can use the newest version of ZFon's VPN, they can recover faster. If they can't, they have to choose, architect, buy, and deploy an entirely new infrastructure, right now. It's a nightmare."

"Ah, got it. So the time spent for a quickie assessment of the new version is worth the trouble. Right on."

"Yeah, you got it. So, are you on or not? I need you man."

"Hell yeah. This will be über-cool. Private jet?"

Reuben grinned from ear to ear. "Yep. Just you, and people whose job it is to look after you. Straight shot flight to here, driver and car waiting when you arrive. We're getting the red carpet, red tape-cutting treatment. So be prepared to work like hell when you get here."

"Right on! See you later."

"Sure thing. And thanks."

"No, thank you. I'm into this now."

They hung up. Reuben looked to Jackson and Jane. "Well, that went well. I think the private jet hooked him, frankly. At any rate, he's packing as we speak. Is there anything else we need to take care of right now?

Jane looked at him, then glanced back at Agent Jackson. "Nothing I can think of. Unless you can start work without the software."

"No, I don't think there's anything left to do. The machines are being set up, right?"

"Yes, to DoJ standards."

"Well, then I think that's it until Frank and the software arrive. Let's get some lunch."

Portland, OR: Saturday, November 22nd, 10:34 AM, 2003

Roger looked across the Willamette River in surprise. He saw two tankers, just sitting in the river. At the offloading point, no ship sat, oddly enough. And the tankers were low in the water, still fully loaded from the look of it.

He had followed up on his brother-in-law's inquiry, and indeed had determined that gasoline wasn't being delivered to anyone. He started learning about the chain of supply, and followed it upstream…literally…to the point on the river where gasoline and other such things were delivered by tanker. Only it seemed that they weren't exactly getting deliveries either.

He wondered what the story was with the dormant tankers, and decided to find out. He got back in his car and drove toward the storage depot. This would be a good time to drive around and see if he could guess what the local hangout for the workers would be.

Baltimore, MD: Saturday, November 22nd, 3:02 PM, 2003

"So it looks like for whatever reason, we've got a bunch of failed RTUs. Right?" The meeting was a mixture of high-level workers and suits who were gathered to sort out the difficulties at the plant.

The men around the table nodded in agreement. "Only possible explanation I can think of. I'm guessing maybe a power surge or something messed some of them up."

In the past 24 hours, the fire at tank three had been extinguished, once it burned down enough to be extinguishable. The column of smoke and fire had made the local news. But what didn't make it to the news was the fact that they had another incident shortly after that, where another RTU locked up. Fortunately, this one didn't bring about the same degree of disaster, but it was followed hours later by another failed unit that came close. This meeting was held in hopes of getting a firm grasp of the problem, and until that happened, the facility was completely shut down for safety reasons.

"So, first order of business is to replace the RTUs that we know are bad. But how do we check the other ones?"

"We can have the techs worry about that. We'll bring them in and have them take care of all of it. Just as long as we know that it's the RTUs, so we call in the right people. How long will we be down while they check them all?"

"A day, maybe two. Hard to say for sure, though."

"Well, we'd better see about getting them here today, if possible. We can't stay down for too much longer."

"Hey, I wanted to ask about that. I'd expect to be catching more heat from upstairs. Has anyone heard from corporate?"

"Funny you should mention it, but no. Not a peep. Odd. Ah, you know how suits are. It's the weekend, they're probably all out driving their sports cars or playing golf or something."

"Yeah, you're right. All the more reason to get us back up by Monday."

Dallas, TX: Saturday, November 22nd, 2:12 PM, 2003

"So, what you're saying, essentially, is that we're suffering a company-wide rash of failed RTUs at storage and transfer sites? That doesn't make any sense." Jim was getting another update from Bill, and what he was hearing wasn't too promising.

"I have to agree with you, sir, but at the same time, that is what the evidence indicates. What adds credibility to it is the fact that each facility has independently reported the same thing. For the most part, none of them are aware of each other's problems, and so that cannot be tainting their assumptions."

"But even if the RTUs suffered from some form of defect, how could they all fail at the same time?"

"That, I cannot say. But I do have a different theory. The problem may lie with the SCADA master at each site. I've been speaking to a few engineers, and one of them came up with the notion."

"Okay, but that still doesn't change the fundamental problem. Why would all of the SCADA masters fail at the same time? And what could possibly be wrong with them to make RTUs…only some of them, mind you…fail?"

"Yes, that's the problem with the theory, I admit. We're looking into it now. Most of the sites are giving their RTUs a thorough once-over now, and we should have more information soon. Until then, all we can do is develop possible explanations that we can test with the data that comes in."

"Okay, good. I want you to bird-dog this as hard as you can. The boys in Energy are watching now, and while they've been calm this far, I can tell they're getting antsy. We need this resolved, and fast. Keep me posted."

"Yes, sir."

Washington, DC: Saturday, November 22nd, 9:34 PM, 2003

MadFast stepped off the elevator with Special Agent Johnson, who looked around for a moment before leading him down the hallway to Reuben's temporary office.

He stuck his head in the doorway to see Jane, Jackson, and Reuben sitting inside, talking casually. Jackson had removed his tie and jacket, exposing the holster on his right hip. Reuben had stopped noticing the armament hours ago.

"Hey hey hey!"

"MadFast! Welcome back to DC, man." Reuben got up and walked around the desk to greet him. "Who's this?" he asked, offering his hand to Agent Johnson.

The man took it, shaking hands with Reuben formally. "Special Agent Johnson, sir. I've been detailed to look after Mr. Rizetti."

Reuben smiled back at Agent Jackson. "Do you guys all get your names changed or something? We've got Agent Jackson and Agent Johnson here!"

Everyone laughed, including Johnson, although he seemed uncomfortable with the informality.

"Relax, Agent Johnson. I know it's not the culture you're used to, but Frank and I keep things pretty informal. It's a geek thing, really. Formality just gets in the way of open communication, and we live or die by the information we can share, so we ditch formality. I'm Reuben, so please call me that. And this is Frank…or MadFast, whichever you prefer." He turned to indicate the others in the room. "This is Paul, and Jane." People traded handshakes as everyone got to know each other.

"Okay, with that out of the way, we need to start getting ready. The lab is about as set up as it can be at this point. We're trying to come up with a copy of ZFon's latest software version. The problem seems to be with the

fact that it's a weekend. None of the resellers are able to deliver today, and we're having trouble contacting the account manager for ZFon. Apparently he's on vacation or something. So what's left to do is for you, Frank, to make sure you're good to go when we get that last bit in place. We're going to go through the same things as the first time, only we'll be finishing the job this time."

"Right on. I started working on it during the flight. Have the testing app ready and everything now. I think I'm about as ready as I can be without ZFon's new code."

"Okay, then I guess we need to go get some dinner. How will we know if the software shows up tonight?"

Jane spoke up. "I can have them give me a call on my cell."

"Good. Let's all trade phone info, so that we can call each other. I have a feeling we're going to be going to bed without having that software, so we should be ready to wake up if it comes before tomorrow morning. MadFast…uh, Frank…oh hell, I'm just going to call you MadFast. Simpler that way. Do you want to put your gear down? We've got an office for you if you want your own, or we could be in this one together. And I don't think you have to worry about anyone stealing anything. After all, we're in FBI headquarters."

"Right on. Yeah, I'll set up in here, if that works for you."

"Sure thing."

Chapter 9

Damage Control

Washington, DC: Sunday, November 23rd, 5:28 PM, 2003

It had been a long, trying, and unproductive day. There had been no progress in acquiring a copy of ZFon's VPN for testing. Without the software they needed, MadFast and Reuben spent the day double-checking everything to make sure they were ready, discussing concepts and definitions of computer security with Jane, Paul and Mark to pass the time.

Jane had a solid IT background, but learned a lot about the specifics of security and how systems get attacked, while Paul and Mark came to develop an interest in computer crime. These were the only achievements of the day, however, and they all started feeling stir-crazy from sitting around and waiting.

The legion of suits that had held the conference had disappeared, leaving only the occasional call from one of them to check on their readiness and ask about alternate actions that could be taken while someone else tried to procure the software they needed. Apparently another group was working on selection of a new VPN system, which helped Reuben relax. The last thing he wanted to do right now was design an entirely new infrastructure under the gun. He was just happy that the various vendors up for consideration were all well known and considered secure this time.

Mark spent some time explaining the impact of the VPN network being down from an end-user perspective, and this was the main thing that helped Reuben and MadFast keep their sanity while being cooped up. Without the ability to communicate over secured links, the recently deployed, but instantly popular e-mail system had stopped being useful to most of the DoJ, as only their largest facilities were connected securely to each other using dedicated links. People in field offices needed to speak over telephone lines when communicating, returning to the way things had been not too long ago.

It looked like nothing was going to happen today. Reuben wanted to get back home and spend some time with Brianna. She'd been a good sport about all of this, but he could tell she wasn't happy. And neither was he at this point. The upswing in his mood from being vindicated and acknowledged had given way to the boredom of sitting in the quiet building, stuck between the pressure to fix things and the inability to do anything to fix them.

The night before, Reuben and MadFast had gone back to Reuben's apartment late, utterly exhausted. MadFast crashed on the couch while Reuben went to bed, finding Brianna already deep in slumber. It was just as well; there wasn't much Reuben could talk about.

Now, another day was coming to a close, with no progress. "Well, at least tomorrow everyone goes back to work, and we can get the frigging

software," Reuben observed. Everyone else nodded in strong agreement. Apparently they were all tired of sitting around.

"Well, we should call it a day, I guess," observed Jane.

"Yeah, good idea," agreed Paul. He turned to Mark. "I'll drive tonight."

"Okay."

Everyone began collecting their coats and readying themselves to leave.

Reuben was already planning how the next day would progress when he suddenly remembered his regular day job. "Uh oh. I forgot something."

Everyone looked at him. "What's wrong?" asked Jane.

"Work, tomorrow. We took care of MadFast, but I totally forgot about me. They don't know I won't be in."

Paul smiled. "I wondered when you'd say something about that. Just give me the information and we'll take care of it."

"They won't be too happy about it."

"Not necessarily. They might come out of it happy that they have you on payroll. You're a very important man right now. I'll see to it that they're made aware of your value."

Reuben smiled, the momentary panic subsiding. "Thanks."

"Don't mention it."

Portland, OR: Sunday, November 23rd, 7:14 PM, 2003

Roger sat at the bar, flanked by workers from the storage depot. There seemed to be more of them than he'd expected, given that it was a Sunday night. And they seemed to have a lot on their minds.

The one next to him seemed to be building up a fairly good buzz, from the number of beers Roger had seem him drink, and he decided to work him for some information.

"You look like you had a rough day, man."

The worker looked back, sizing him up, and smiled slightly. "Yeah, not the best day I've ever had. But I've had worse. Who are you?"

Roger lifted his glass. "Roger."

The worker lifted his beer and clinked it against Roger's. "Ramon."

"Nice to meet you. You had to work today?"

"Yeah. Some problems we're having, they brought in techs from the outside. Needed us to show them around. Funny, we pay all that money and they supposedly know so much, but then they need us to keep them from getting lost or hurt."

"Yeah, I know what you mean. My brother's an oil worker, and he tells me about the geologists. For all that time in college, they can't be trusted not to get themselves killed around a rig."

"Ah, didn't take you for that kind of guy."

"What kind of guy?" Roger knew exactly what kind of guy he meant, of course.

"You know, someone in the oil business."

"Oh, well, I'm not like that. I don't know, I'm the odd one out. My brother-in-law runs some filling stations, and my brother works on the rig. Me? I'm still trying to figure out what I want to do. Why, you in the business?"

"Yeah, I work at the depot just half a mile away.'

"Oh, where all those tanks are?"

"Yep." Ramon looked into his beer again and took another swig. "Not like they're doing anything right now, though."

"Huh? What d'you mean?"

Ramon sighed. "Something's messed up. It's got something to do with the control systems for everything. That's why the techs have been in. They've been poking at all the remote terminals."

"Remote what? Remember, it's my relatives that know this stuff, not me."

"Oh, yeah. Remote terminals. They control all the things around the depot, and report back to the control room. Some of them aren't working right. We had a bad spill, couple of days ago because of it. So they shut everything down…goddamned tree-huggers…and called in the techs." He looked into his beer again. "Well, at least I'm getting overtime for today."

Roger smiled inwardly. There *was* a story here. "What does it mean? I mean, to everyone else?"

"Well, we can't deliver gas, for starters. And we can't get any either. At least not until those pencil-necks fix what's wrong. But if you ask me, they

don't know what the fuck they're doing. They didn't have any idea what's wrong, they even said the terminal that caused the spill wasn't broken."

"Hey, you're about to run dry, let me buy you another." He motioned to the bartender. "Let me get this guy another beer and settle up." Putting his cash down on the bar, he slid off the stool, patting Ramon on the back. "Good luck, Ramon. Good talking to you. I hope it works out soon." *He had to learn more about those systems Ramon mentioned, this could be big.*

"Yeah, thanks. Be safe."

"You bet."

Roger walked out of the bar, hoping he didn't get pulled over on the way home. He definitely had something to follow up on now, and he was sure there was a solid story behind all this. He felt it in his bones.

Washington, DC: Monday, November 24th, 10:02 AM, 2003

Reuben and MadFast were in much better spirits this morning. Getting up early, they were picked up by Mark who whisked them through rush-hour traffic downtown, lights and sirens going full-tilt.

"These guys drive even crazier than you do," MadFast observed to Reuben, who smiled back.

"Yeah, but you don't know how I'd drive if I had a siren too!"

Mark called back from in front, "Most guys have trouble with it. It scares the hell out of them. You two don't mind?"

"Nah, not at all. We trust you," responded MadFast. "You'll get us there in one piece. And it's cool to be able to beat the traffic!"

Getting into the office, they were greeted with the good news: a copy of ZFon's newest version was on its way, along with a programmer to help with support. Reuben had been adamant that nobody from marketing, including any pre-sales engineers, would be allowed to have anything to do with this effort. He needed people who could absolutely be held responsible for any concealment, misinformation, or simple inability to answer questions.

He wasn't terribly surprised when John showed up.

"Well, well, well. Look who it is, MadFast!" Reuben had his energy back, and was going to savor this.

John was surprised to see the two of them, here of all places. He shrunk, obviously thinking this had to be bad news.

Hmm. That's an interesting reaction. I'm guessing this software might not be so secure, even now, thought Reuben.

"What, surprised to see me, John? Still hoping that nothing would have happened after all that scanning?"

"Yeah, I guess that's what we hoped for."

"Didn't any of you *care* about what might happen? Dammit, you people make security software, and you left all these people twisting in the wind, knowing full well that it was insecure!"

MadFast watched quietly to the side Reuben. He thought Reuben was going a little over the edge, but didn't think that this would be a good time to interrupt.

John seemed to take it fairly well. He shrugged and said, "If we raised a ruckus, we'd lose the deal. We were told that the deployment had to go as planned, and that they'd patch later. Later on, they didn't patch, apparently. At that point we didn't have any control anyways. It's not like it's our network."

Reuben stopped his rant instantly. He hadn't thought of that. "Oh shit, that didn't even occur to me. Wilkens. He would have pressured you guys too, huh? I'm sorry, I didn't even think of how this might have played out from your end. Okay, I get it now. Well, now we're all in the same boat, so let's see if we can plug the holes." He extended his hand. "Sorry I ripped into you, man. Let's get this done together."

MadFast relaxed, glad that had blown over without getting any uglier.

John took the hand, shaking it. He seemed relieved. For the nightmare that this had been for Reuben up to this point, John must have been facing a worse one. He was, after all, from the vendor responsible for the now-exploited vulnerabilities.

"Okay, here's where we stand. They're totally down. And we think if they just reinstall, they'll get taken down again. Adding to that, they can't redeploy the same version anyways, since it's clear they can't trust it to keep from being compromised. Aside from downtime issues, they can't risk

compromise of their communications. But they need to get back up, and fast. And the shortest way to get there is to use the latest version."

"Okay, with you so far. So what's stopping them?"

"Well, their past experience, to be blunt. They want us to make sure the new version is safe, or at least safe enough, first. We won't be looking at the client, just at the gateway side. But we need to go over it carefully and make sure that the old bugs are all gone and that there are no new ones we don't know about. I suspect they'll do a more thorough check later; what they most care about right now is being safe enough that they can deploy with minimal delay. If they think they need to use some other product after that, they can do it in a more sensible manner. Sorry, but I think they'll probably end up forklifting this out eventually, even if it's perfect. You should have seen the meeting on Saturday. I don't think they're going to forget this."

John nodded. "I expected that anyways. Okay, what do you need me to do?"

"Well, we'll need some answers, and some support here and there. Basically I wanted a good source of answers on tap, to save time."

"Okay, you got it. Uh, I've been asked to see if there's anything I can do to help our, I mean ZFon's, situation here. Sorry, I have to ask."

"Just be helpful and honest, and that's about as much as I can think of."

"Okay. Well, here's the software." John patted the briefcase he had brought in. "Mind if I watch you guys work?"

"God no, you're entirely welcome to. That is, if it's okay with you, MadFast?"

"Right on! I think it's always good for a programmer to see how people break applications. Helps them write stronger code."

"Okay, that's settled then. Let's go to the lab."

As they entered the lab, John excused himself to make a phone call before they started. Once he left the room, MadFast took the opportunity to pull Reuben aside, pulling him into their office and closed the door.

"Hey, I just wanted to talk to you for a sec, just you and me."

Reuben was unconcerned, but curious as to what was up. "Sure…what's on your mind?"

"I just wanted to say, don't be too hard on John. I think I know what happened. They don't teach coders how to write securely, and this is what happens."

"Yes, but it's not like he writes text editors or first-person shooters. He writes code that's meant to withstand attack."

"I know, and you're right about that. But you gotta see it through his eyes, dude. He didn't know that the code he wrote was insecure. He did it as he was taught, and nobody ever told him, 'By the way, this is the wrong way to write functions if you want to be secure.' And he didn't know how to attack it to test it either. He simply didn't have all the information. Trust me dude, it's not a rare problem. It's like that everywhere. I mean, to you and I, we've been looking at security for years, so we forget that not everyone else does. But really, not everyone does understand it. It's a problem that has to be addressed in the colleges, the books and the tech schools. Should he have been more careful? Sure. And his company *definitely* should have. But he didn't fuck up as bad as he just plain didn't know."

Reuben paused as he absorbed this. "I see your point. He does seem to care, it's not like he's a bad guy or anything."

"Yeah, and did you notice? He's blaming himself for this. He's taking it hard enough, I guess that's my point. It won't help anyone for us to be hard on him on top of that."

"Okay, point taken. And I see it, you're right. Should I say anything?"

"No, at least not unless the right time pops up. Don't sweat it, this will all work out fine. Let's get to work."

They returned to the lab, and began working a few moments before John came back, none the wiser. "So where were we?"

"Well, we're comparing the data fields with the old design. Seems to be the same, yes?"

"Uh, yeah, we didn't change that. That part of it seemed entirely fine."

"I agree. Don't tell us what you fixed, though, let us find it. No offense, but you may have missed something, and we might find something where you thought it was already solid."

"No offense taken. That's been the whole story of this damned thing." Reuben saw what MadFast was talking about. John was watching a disaster

unfold because of flaws in software for which he was primarily responsible. It had to hurt.

"Hey. Let me guess…they never taught you a lot on secure coding practices, right?" Reuben saw the opportunity he was hoping for.

"No, they did, but we never seemed to cover too much material."

"So you didn't know, right? I mean, you got a good education, and learned how to write tight code. This software isn't bad, it's stable and fast and lean. And the basic protocol design is fantastic. So it's not like you're a sloppy or lazy coder. You just never knew about the nuances of coding to make it secure."

MadFast jumped in. "I think what he's trying to say is, don't be down on yourself. It's not like you did something stupid. They told you how code should be written, and they got it wrong. And security bugs don't make themselves known automatically, so you couldn't have figured it out. So don't be so hard on yourself, dude. You'll know how to do it more securely after this."

John listened to them quietly. "Have you two been talking about this already?"

Before they could answer, Paul and Mark both popped into the lab having stepping away for a bit. Paul announced, "Reuben, MadFast. We need you for a moment." He looked serious. "Right away."

They looked at each other, shrugged and stood to leave. "We'll, uh, be right back, I think, I hope," Reuben said to a puzzled-looking John. "Just make yourself comfortable, I'll have Jane come by and keep you company if you want."

"Okay." John seemed to be accepting things as they came. There wasn't much of an alternate option.

The two Special Agents led Reuben and MadFast to the elevators, but instead of going up as they expected, Reuben and MadFast found themselves going down. Instead of going deeper into the FBI building, they exited it, walking instead across Pennsylvania Avenue to the older-looking building that housed the Department of Justice proper.

Entering the building, Reuben discovered that their visitor passes were honored here as well, as they walked into the lobby and to the elevators. Going up to the top floor and navagating through hallways, they finally

entered a large office. The polished nametag to the right of the door read *CIO, Department of Justice* complete with the standard trimmings of a highly placed position in the federal sector. Behind the wooden desk sat Johannsen. "Good to see you again, Reuben. I hear you've been busy."

"Uh, yes sir. Waited a bit for the software, but now we have it and we're starting to work. Oh, this is Frank Rizetti, but goes by the name MadFast."

"Ah, the wizard from Seattle. How was your flight over?"

MadFast seemed uncomfortable within the large room and hesitated before answering. "Great, thank you. I've never been on a private jet before."

"I'm glad you enjoyed it. Our pleasure. I understand you're quite critical to the success of our recovery effort. I won't waste any time, I'm sure you're wondering why I called you here, yes?"

The pair nodded.

"Well, I'm not exactly sure what I'm trying to ask, in truth. Here's the situation. It's come to my attention that there may be a second attack in progress. I wanted to see if you have any insight into that possibility."

Reuben decided to handle this, since he'd already spoken to this man before. "Can you tell us more about what you know? It's hard to work with just that bit of information."

"Well, I'm not sure exactly what I should share with you two, as it's only conjecture at this point, and highly sensitive conjecture at that. By the same token, however, I suppose our fate is already in your hands, so if you're not trustworthy it's a bit late to start worrying. Have either of you needed to buy gas over the weekend?"

They looked at each other, not having been near a vehicle that they had direct control over since Friday. "No, sir. You detailed drivers and cars for us."

"Oh yes, that's right. Well, let's simply say that you'd probably notice that a significant number of gas stations were running dry. Particularly in areas of high population density, like here in the city."

"Oh, I did see that on Friday morning. But what does that have to do with an attack? What kind of attack are you talking about?"

"It is believed that the petrochemical supply chain has been disrupted, possibly by a network-based attack."

"Petrochem…you're saying that the reason that gas stations are running out of gasoline is because of a hack?" Reuben wasn't expecting an entirely new attack to be the subject of this meeting.

"In essence, yes. I called you two up here to see if you had any insight on it. I see a number of possible combinations. One, it isn't an attack, just an extremely bizarre set of circumstances. I don't know all the fine details yet, but from what I do know, I consider that highly unlikely. Two, it is an attack, but one that is not connected to the attack we suffered. Again, I consider that unlikely. I do believe in coincidences, but I don't trust them. And finally, the possibility that it is an attack, carried out by the same people who attacked us. Since you're the only ones who saw our attack coming, I believe you can help with this second attack, assuming there is a second attack."

MadFast spoke up, with his own question. "I, er…I don't know how to ask this, but it seems odd. I mean, you're the CIO here. Why are you asking for our help with this?"

"That's actually an excellent question. As you can imagine, I've been aware of your work for us with regard to the VPN. And as I have already stated, I suspect that this is a second attack, largely because of the nature of it, but also because of the improbable coincidence that it would have to be otherwise. But my view is not universally shared at the moment. And while I feel strongly about it, the Attorney General wished for me to speak with you and get your thoughts. And more to the point, to be prepared to step in should it turn out to be an attack."

He continued, "First, let me draw you a general outline of how things are right now. There has been some political infighting, perhaps more than usual, because of the convergence into the Department of Homeland Security. Some feel that their parochial interests are being taken away, and of course are resistant to accept this."

MadFast and Reuben nodded. "With you so far."

"That said, it is entirely possible that…well, let me just say that it is not out of the question that some people would profess it not to be an attack, even as they investigate it as an attack."

"Why would someone do that?" Reuben didn't understand.

"Well, by maintaining the notion that some other cause is to blame, they manage to buy some time for themselves, for one. And then when it becomes obvious that an attack is the true source of the problem, they are better prepared to look good. Everyone is jockeying for influence right now, to put it bluntly. I won't name names, but it's going on nonetheless."

Reuben got it now. "Ah, I see. And because we helped with the first attack, we've got an inside line?"

"Perhaps. At the very least you seem sensitive to what to watch for. But in any case, you've been tremendously useful up to now, and I'm sure we can use your help again. Obviously, we can't have you taking part in the investigation as such, as you're not qualified. You might accidentally render evidence inadmissible, for example. But the investigation isn't even half the story. Whatever the cause, this needs fixing."

Reuben felt the room spin. He was not prepared in the least bit for this escalation of things. His mind reeled back to things he had learned in business school…how supply chains worked, the importance of petroleum to most of them. Without gasoline, diesel or aviation fuel, shipping would stop. Travel would stop. Food could no longer be delivered to grocery stores, people could no longer travel, and the impact would ripple outwards from there. And he was supposed to help with this?

MadFast was as surprised as Reuben, but seemed to be taking it better. "Uh, dude…you don't look so good."

"God, I don't…I need to sit down." Reuben sat in one of the extremely comfortable chairs in front of the desk. MadFast took the one beside it.

Reuben collected himself, and cleared his head. "Okay. I need more data. First of all, what are the details of what people are seeing? Why do they think it might be a hack?"

Johannsen smiled softly. "Well, some believe it is, and some believe otherwise. I need to make that clear. Those who do believe it to be an attack are pointing to the widespread and simultaneous nature of it. Let me explain what I've learned about the supply chain in the past two hours.

"Petrochemical supplies come from central points, simply because there isn't oil everywhere. The oil goes to refineries, which then send finished

products like gasoline to other parts of the country. Near all population centers are large depots that store various petroleum products for use. You've seen them, I'm sure. They are basically large sets of storage tanks. From these sites, the products go out, usually by tanker truck, to gas stations, airports, and whoever else consumes them."

Reuben nodded. "Okay, I follow you so far. That makes sense."

Johannsen continued. "Well, in essence, the majority of these storage facilities became unsafe to use about three days ago. The affected sites all showed relatively similar symptoms within hours of each other, regardless of their location in the country. It took some time for the pattern to emerge, as companies didn't know that other companies had the same problem, and didn't want to let on that there was one. It took almost a whole day for any of the companies to really catch on that this was not just some unusual quirk, curiously enough. I would imagine they simply never considered it possible, and thus the notion of this kind of attack never even entered their minds. But there is one thing that all of the failed sites share. They are all connected to the Internet, and have very similar computer systems as well, I am told."

MadFast leaned his head back. "Ohhh…and what else could do that, besides a hack…I got it. That makes sense. What are they running?"

"Running? I don't follow you."

"What applications are they running? For them to all be hacked like that, you're right, they must be running the same apps. But it matters what is alike and what is different."

"I don't know, but I'll ask about it. And that might help settle the matter. What else should we be looking for?"

Reuben jumped in. "Well, once you find out what they all are running in common, find out what listening ports the software uses. Then we can go back and see if there's been scanning for those ports. We spotted the impending attack on the VPN because I happened to remember what port it listened for. I saw scanning commence for that port, and put two and two together. But every day scans for all sorts of things happen. Who knows, at some point I might have seen some data for the scan leading up to the attack…if it is an attack…on the storage facilities. But because I

didn't know the significance of that particular port, I didn't know to pay attention."

"I see. I'll get that information too. I think that's a good start, and maybe we can give some more attention to the theory that this is an attack. Thank you, gentlemen. I'll let you know what I find out, and in the meanwhile, I need you to help us get our VPN back up. If this is an attack, we're going to have a hard time dealing with it without secured communications."

Reuben and MadFast nodded, and got up. "Great, will do. We'll get you back up. It's just a question of how fast. We'll do everything we can."

Johannsen stood up with the pair. "And while you're working on that, see if you can come up with any ideas as to how to recover our petrochemical infrastructure, if it is indeed under attack. While we aren't the normal agency to deal with that area, I would love to be able to offer an alternative option when the time comes."

"Um, we'll try." Reuben didn't like the idea of being caught up in these power plays that he was just now learning about, but decided he could stomach it in the name of making a difference.

The pair left, wondering just what had happened to get them both so deep into this mess. As they walked back, they looked around at all the people working, wondering what it was like to work here, to permanently be responsible for the protection of a nation from both foreign and domestic threats as they manifest within the United States. Mostly, Reuben wondered if one ever got used to the job, if the responsibility became less suffocating after a while. He certainly felt like he could use some air at the moment.

"I think we'd better go to our office and talk a bit before we get back to the lab. We sure as hell shouldn't be talking about this in front of John."

MadFast was all too happy to agree. "Right on. I like John, but I don't think he's supposed to know about any of this, and I want to get a grip before we have to deal with other people. This is just far out of anything I ever thought I'd ever face."

"Yeah, no shit."

Neither of them said another word as they walked back with Mark and Paul leading the way. Once inside the office, they closed the door and started talking it through.

MadFast wanted to check his bearings first and make sure this wasn't just a dream…or a nightmare. "Okay, let me see if I have it right. The DoJ just asked us to help them figure out if the whole country is under attack. And to help fix it if it is?"

"Uh, yeah. I think that's what just happened."

"Aw, shit."

"Well put, my sentiments exactly. So, what the hell do we do?"

"I think we've done what we can. We need to know more to do anything else. He didn't really tell us all that much."

"Good point. I don't think they know that much either. So maybe what they really need are questions. We should be thinking of things to ask, so that we can dig a bit deeper."

"Right on. I follow you there. Well, that's easy, but what after that?"

"I guess we'll cross that bridge when we get to it. Maybe they won't need anything from us at that point."

"Hmm. I wonder if I want them to, or not. I mean, one part of me wants to help save the world. The other part is scared as shit that I won't be able to." MadFast laughed. "Jeez, dude…what the fuck did you get me into?"

Reuben laughed back. "I've been asking myself that too. Sorry."

"Ah, don't mention it. I honestly don't mind. It's just…I mean, wow."

"Yeah. We should get back to the lab. If there is a second attack, we really need to clean up after the first, I mean, even more urgently. There's going to be a lot of data that needs to move around to diagnose this."

"Okay."

They left their office and walked across the hall to the lab, finding Jane had joined John.

"Hey, we're back."

"So, what was all that about?" asked John. He was both worried and curious.

"Uh, can't really talk about it. It was just a bullshit meeting, but you know how these guys are." At least Reuben was being half-honest. "No big deal though."

Jane looked at them, knowing he was lying. John had told her of their summons, and she had been around long enough to know what it meant when you suddenly got pulled like that. "So, mind if I watch you guys work?" she asked, diverting the subject.

"Sure, pull up a chair. We're just getting warmed up," replied MadFast. "Okay, I need to recompile. I still have my source code from before, but I don't have the compiled executable."

"No problem, man. While you work on that, we'll set up the VPN."

John spoke up. "Ah, while you guys were away, I took the liberty of doing that. I figured that since Jane was here, I could go over it with her, and that way it would fill the requirement for that."

Reuben smiled. "Oh, cool. Good thinking, you saved us some time. Okay, so now what we do is set up a sniffer. You have two gateways up and talking to each other, right?"

"Yep, and they work just fine."

Reuben got up and looked at the switch that everything was plugged into. "Ah, okay. Do we have a hub here? It might make things easier, from a sniffing perspective. Otherwise I have to configure a span port on this switch."

Jane hit her head. "Oh, duh! I should have thought of that. Yeah, no hubs around, but I can get you into the switch. I've never done what you're talking about though, so you'll have to show me."

"No problem, it's easy if you know how. I'll show you."

Jane logged on to one of the servers in the room, and opened up Putty, a commonly used SSH client. She connected to the switch and logged in, then set it into *enable* mode, which gave her the ability to make changes to the switch's configuration. She then turned the keyboard over to Reuben.

"Okay, I'm only going to span the port that one of the servers is using. That way we don't have to worry about performance issues from trying to jam too much traffic onto one port." He looked at the switch, and saw that port #4 was not being used. "Okay, I'll use #4. Hand me that network

cable?" Jane grabbed a cable for him, and he plugged one end of it into that port. "Which port is the target server on?"

"Eleven."

"Okay." He typed the initial commands to get the switch into configuration mode.

```
Labswitch#
Labswitch# config t
Enter configuration commands, one per line. End with CNTL/Z.
Labswitch(config)# interface fa0/4
Labswitch(config-if)# port monitor fastethernet 0/11
```

Reuben hit **Ctrl** + **Z**, and the configuration settings were put into effect. He checked to make sure that he had set it up properly.

```
Labswitch# show port monitor
Monitor Port Port Being Monitored
--------------------- ---------------------
FastEthernet0/4 FastEthernet0/11
```

The table demonstrated that port 4 on the switch would be sent a copy of all traffic that traveled through port 11.

"Okay, now you see, the first thing I did was put the interface that the sniffer will sit on into configure mode. You configure the port that will be getting the traffic to listen in, rather than configure the ports that will be monitored. With me so far?"

Jane nodded. "Yes. Go on."

"Okay, the commands differ a bit between the various versions of IOS and the different switches, so it's always good to look it up on the Internet if you're not absolutely sure, but the concept is always the same. In this case, it's the *port monitor* command, which specifies a port or VLAN to monitor. The command does nothing more than say, 'watch this port' or 'watch this VLAN.' Make sense?"

"Sure. I see what you meant, about it being simple."

"Now, there are a few caveats. One, you can't monitor a port that is on a different VLAN. If you had been running different VLANs, and ports 4 and 11 were on different ones, I would have gotten an error. And it is possible in some cases to set mirroring up in such a way that you cause traffic problems, so be careful. But it's all stuff you can look up on the net. Cisco has done a great job of documenting the commands on the web."

Jane nodded. "Okay."

"So, let's sniff." Reuben powered up his laptop, and plugged in the cable that led to port 4 on the switch. He waited for it to finish booting up, and launched Ethereal. He didn't bother configuring the laptop's IP address to match the network he was on, since he'd only be sniffing right now. "Okay, John…are the two gateways associated with each other right now?"

"Yes. Why?"

"Because I want you to disassociate them. I want to capture the sequence that happens when they first link to each other."

"Okay, give me a minute." He clicked on a few things on the screen of one of the gateways, then on the other. "Done."

"Alright, when I give the word, associate them again." He started configuring the settings for Ethereal to only sniff the traffic he wanted to capture. He didn't want to capture any broadcast traffic like ARP requests, DHCP requests, or any Microsoft networking stuff. Like loud voices in a crowded room, these would just distract him when he looked at the output. He started sniffing. "Okay, associate them."

John clicked on a single button, and one of the servers started talking to the other. Reuben saw the captured packet count increment as Ethereal captured the traffic.

"Okay, they're done associating."

Reuben stopped capturing traffic. "Great, thanks. Let me have a look at what we've got here." He looked at the sequence of data that went back and forth. "Wow, this takes me back." It looked like it had years earlier, the same data fields in each packet, and the same delimiters between them. "Well, this looks like it'll make our work easier. It's the same exchange back and forth…time request, time response, and login. No changes?"

"Right, no changes. Nothing seemed to be wrong with the nature of the sequence, so why alter it?"

"No reason, but I figured I'd make sure just to be safe. Okay, cool. We can test with the old payloads, for a start. How's the compile coming, MadFast?"

"Uh, I've got a bug somewhere. I guess I have the older version of the source code here or something. I can't remember what I did wrong the first time though. Still debugging."

Reuben found this amusing; he could remember the bug. "Think Chinese food. Chow…what?"

MadFast looked at Reuben like he was out of his mind. "What?" He thought for a minute, and it dawned on him. "Oh, dammit!" He laughed and fixed the typo. "How did I forget that?"

"I don't know, man. I sure didn't!"

John and Jane exchanged puzzled looks.

"Inside joke, sorry," explained Reuben. "You know you've been working hard with someone else when you remember the bugs in their old code, eh?"

"Okay, that was it. It compiles now. Jeez, I feel like a dumbass for that! I've got the old payloads too, so we can try those first."

"Good. Go ahead, start cycling through the payload sequence. I'm hoping we won't get anything on any of them. Here's to hoping." Reuben pondered what to recommend if none of the old attacks worked. It probably made sense to implement the new version at that stage, as the attack had probably focused on flaws that were fixed in that case. He would recommend further testing in that event, but at the very least they could get the VPN network back up and running quickly, and buy some time. DoJ was probably going to replace ZFon with something else, but if they could be running normally in the meanwhile, so much the better.

MadFast loaded and fired payload after payload at the ZFon server while Reuben and John watched for any effect it might have. A couple of the payloads caused momentary tiny bumps in processor utilization, but nothing problematic. "So far, so good, man."

"Right on. So if we don't find anything in a cursory check, we recommend they upgrade in place?"

"Exactly what I'm thinking. It'll get them up and running fast, and even if there are problems with the new version, it'll take days at the very least, for the enemy to pick up on them and exploit them. And I think it'd probably take weeks. So it buys them some time to be sure it's really safe, and to get something else if it isn't." *But only if what the enemy found is the same thing we found,* Reuben thought. *Ah, no sense worrying about it. Hell, the fruit was hanging so low it was on the ground. Of course they probably found the same vulnerabilities we did.*

"Right on." MadFast kept clicking away, and eventually exhausted the entire set of payloads. "Good news, dude. That's the whole set. That server still working right?"

Reuben double-checked again. "Looks right to me. John, you're the expert, what do you think?"

"Let's disassociate and re-associate the servers and see what happens."

"Good idea. Go ahead."

John repeated the sequence of commands to break the VPN connection between the two test systems, and then re-established it once more. Just as before, no problems were evident. "Looks perfectly healthy."

"Okay, last thing, let's check the Event Logs. I want to be sure nothing bad happened. We only get this one shot before we have to make a decision and run with it. Can anyone in this room think of anything else to account for? Anything to check or try that won't take a couple of days?" Reuben looked at the others for anything additional, but they were silent. "Okay, good." The Event Logs were pristine, showing no errors.

"Okay then! Paul? We need a meeting."

Paul had been standing by, silently watching the geek session. "That's it?"

"Yeah, the good news is that MadFast and I seem to work really well together. We've got our own individual things, and we do them independently. Even more importantly, our larger goal has a clear first step to it, which was easy to finish, considering MadFast saved his work from years ago. You guys need to be back up and in business again as fast as possible, and we intend to deliver. John, I just want to make sure. This version, there's an upgrade path from 2.2? They can just restore from old backups, and upgrade with this? It'll keep the configuration information?"

"Yes, exactly."

"Right on!" MadFast was relieved too. This meant that the VPN network could be restored within a matter of days. The slowest part of it all would be the distribution of the new software.

"Okay, I'll set up the meeting. Be right back." Paul disappeared out the door as everyone sat back and relaxed.

Reuben looked at MadFast. "Well, that wasn't so bad, was it?"

"Yeah, I only hope it stays this simple. I'm kind of doubting that though, dude."

"Well, then let's enjoy it while it lasts. At least now we've been able to deliver on what was asked of us."

Paul came back in. "Okay, just got off the phone with the CIO from the DoJ. They'll be ready for you in twenty minutes."

John whistled. "Damn! You've been dealing with Johannsen?"

"Uh, yeah. Or more like he's been dealing with us, actually. It's a bit weird. He's given us all sorts of support. They even sent a private jet to pick up MadFast."

"No shit?"

MadFast grinned. "That's right. Nice flight too."

"Well, it looks like they did the right thing. You two are about to save their butts, from the look of it. So they got their money's worth."

Reuben and MadFast looked at each other. "Oh yeah. We should be tracking our hours, huh? We get paid for this too," Reuben observed.

"You forgot about that too, huh?" asked MadFast.

Washington, DC: Monday, November 24th, 1:27 PM, 2003

"Okay, gentlemen. I understand you have some good news for us?" Johannsen smiled from his end of the conference table. All the attendees of the previous conference were present except Wilkens. Reuben wondered about that, but doubted it could be a problem for anyone but Wilkens.

"Yes, sir. We have a recommended recovery plan for you, and I think you're going to like it."

"Good, let's hear it."

"Alright, there are multiple phases to this recovery. Stage one is an upgrade in place of ZFon. Recover from oldest-possible backups, and upgrade prior to putting the servers back on the network. The newest version of ZFon is free of any of the older vulnerabilities, and in the event there are newer problems, it will take time for anyone to discover or exploit them. This part can be done almost as quickly as you can hand the software out, and will get you back up in the shortest span of time. The software is functionally similar, and will require little or no retraining for people in the field. You'll need to restore from an old backup, a complete one, prior to updating, then upgrade in place."

"Excellent, that's what I like to hear. What's next after that?"

"That's up to you. You can either conduct a more thorough certification and accreditation of the new ZFon software, or take advantage of the time you have bought to examine and select an alternative vendor altogether."

"Do you have a recommendation as to which of those two options we pursue?"

Reuben wasn't ready for that question. He thought of John, who asked him to help. He thought of the company whose future might depend on what came out of his mouth in the next ten seconds. And he thought of the problems that their software had caused.

"That's a difficult decision for me to make, sir. I've become somewhat entangled in this. I know one of the programmers personally now, and am aware that ZFon is in a precarious state."

"Yes, but that's not your concern. I realize it's a tough call, but I need input from all sides of the situation, including yours. Think only of security. You have to embrace the bigger picture, so we don't go through this again."

Reuben sighed, agreeing with Johannsen. "Very well, sir. I would go with another vendor. As to which, I cannot say precisely, that's an entire project of its own."

"Not a problem, we have that project in progress already, in the early stages. I wanted your thoughts on it, however. We have certain guidelines we must follow to avoid causing problems. Government procurement is a

strange thing, but you don't have to worry about it. We will ask your guidance a bit later on, if you're comfortable with that."

Reuben relaxed, the worst of the meeting having passed. "Most definitely, sir."

"Now, onto the next item. I have some information for you about the petroleum situation."

Reuben tensed. The worst of the meeting was not over. "Okay, I'm listening."

"MadFast, is it? You were on the right track. We checked into the systems at several of the sites. So far, every one we've heard back from is running the same SCADA architecture."

MadFast looked to Reuben for some clarification of the term. Reuben shrugged back, looking just as puzzled. "Uh, scade-ah? What is that?"

"Oh, sorry…I take it you don't work with industrial systems."

"Afraid not," apologized MadFast.

"SCADA is an acronym that refers to the category of systems used to network an industrial plant. That might not be an exact definition, so don't quote me, but it covers things well enough here. To sum it up quickly, nodes throughout a facility report back to a central system, and take commands from that system. And in this case, all the sites are running the same software."

Reuben and MadFast both reacted to this, pondering the obvious implications. "I see," said Reuben as he jumped in. "How many sites in general run this? Could it be a coincidence?"

"That's an excellent question that someone else has already posed. Apparently, this system is by far the most widely used. So it's not conclusive. What we're trying to do is find somewhere that isn't affected, and see what they're using. The trick is doing so without making too much noise. We want to delay the release of this information as long as possible, so that we have something to say when we're asked about how we intend to react to it. I may be passing you off to the Department of Homeland Security, or the Department of Energy. The problem is quickly escalating, and now that you've gotten me a solution for the VPN issue, I think we can share you. Of course, there are multiple agencies working towards a solution at the moment, as there should be. In the meanwhile, keep working at it.

Whoever solves the puzzle first wins, and I want to use every shot we've got to resolve this as quickly as possible before the situation gets worse."

Jesus! There are multiple agencies that want us now? thought Reuben. *This is insane. Who the hell is behind this attack?* "We are at your disposal, sir. Just keep giving us what we need, and we'll do anything we can to help."

MadFast piped up. "Yeah, I want to thank you for letting us help out. It's good to be able to make a difference."

"No, I should be thanking you. And I'm sorry that your concerns weren't heeded earlier on."

Reuben grinned. "Not as sorry as Wilkens, I'm betting."

Johannsen smiled back. "Well, it would not do to speak of such things, but I think you know the answer to that. Feel free to gloat privately, off the record. You have indeed been vindicated."

MadFast spoke up again. "That reminds me. Reuben broke his NDA when he started trying to get your attention. Is he off the hook? He volunteered to take the risk on his own rather than involve me too."

"Is that so? Well, yes, naturally there'll be no adverse impact from that. After all, you were doing the right thing. I only wish more people displayed the courage to act. No, of course you're in the clear, Reuben."

"In truth, I had entirely forgotten about that. Thank you."

"Okay, I think we've covered everything for now. I'm going to make some calls and see where you two can help next. Thank you for your time, and good work."

"Oh, there's one more thing."

"Yes?"

"I'm not exactly sure what it is I'm asking, but…well, it's like this. John, the programmer I mentioned earlier, from ZFon. He seems like a good guy, and he's been very cooperative today."

"As well he should be, his work has cost us dearly."

"Wait, hang on, sir. That's what I'm getting to. We spoke with him, and the truth of the matter is, I don't think the guy deserves to get roasted for this. He's a good man, and he genuinely didn't know that he was writing code that was all that awful. And the latest code seems to be pretty good, at least so far. And he's beating himself up worse than anyone else could at

this point. He's punishing himself enough, and it'd be a shame to toss him away now that he has learned his lesson."

"Let me get this straight. This is the guy who works for the company that caused you all this stress and anguish? You were willing to risk being sued over the disaster you saw coming, because of this man, among others…and now you're asking me to look after him?"

"I guess that is what I'm asking, yes, sir."

"You've given good advice the whole way through this, I shouldn't start to doubt you now. I'll tell you what. Let me see what I can do, and I promise I'll give it serious consideration. I can't promise anything obviously, but I'm not terribly concerned, if he really is worth your recommendation."

Reuben smiled. "Thank you, sir. I really appreciate it."

"Don't mention it. I'll let you know what we…or anyone else…needs from you next. Go have lunch."

"Yes sir."

They left the conference room and went back toward the lab. MadFast patted Reuben on the shoulder. "That was very cool of you, dude. Right on."

Reuben smiled. "I couldn't just let him swing in the breeze. But I couldn't just recommend ZFon either. It was the best solution I could come up with."

"It was a good one. Hey, ZFon's management was probably the worst of it anyways. So let them fry while John gets a safe out. Very cool."

"Yeah, I do like the thought of that. I didn't really have it all figured out when I was in there, I just went with the urge to say something."

"Well then, über-leet instincts, dude. You should tell John."

"Okay, I think I will."

Portland, OR: Monday, November 24th, 6:03 PM, 2003

"And on breaking news today, an explanation for the rising gasoline prices and empty pumps in our region." The news anchor finished up the list of stories for the evening news, and went right into the first story, which

Roger had spent some considerable bit of time putting together. The coverage detailed the lack of deliveries to gas stations, and expanded to describe the tankers sitting in the river, the lack of any word from "authorities" and no clear explanation, other than unnamed sources' descriptions of the problems at the storage depot. On a finishing note, they concluded with the report from affiliates in other parts of the nation, all of whom were reporting a similar shortage of gasoline.

The anchor sternly looked into the camera, hair neatly in place. "As we learn more about the emerging crisis, we'll keep you posted," he said before turning with a smile, "And to you, Tina."

Washington, DC: Tuesday, November 25th, 9:52 AM, 2003

MadFast and Reuben stood in Johannsen's office again, having been summoned there minutes earlier.

"Gentlemen, I want to bring you up to date on what is happening, and what you'll be doing. There is now officially a national crisis."

The pair tensed, now sure that they had been right in thinking that there was a second mass compromise in place.

Johannsen continued, "I've forwarded on your insights and requests for information, and they mirrored what some others have put forward. Indeed, this is now being viewed as a likely cyber-attack aimed at critical national infrastructure, the first such event in our history. For one, the affected plants all run precisely the same SCADA systems. Evidently, these plants are relatively generic, and one company has an overwhelming market share in this particular niche market. The impact is growing as time passes. Gasoline prices are rocketing upwards as stations run out. There are already reports of cars being abandoned on the road as they run out of gas while their owners seek a station that still has gas to sell.

"But that is far from the worst of it. Shipping is already feeling the impact, and airports are beginning to run low on fuel. This is not for you to repeat outside of this office, but the President is about to declare a national state of emergency. As such, certain people will be granted expanded powers to act to end this crisis as swiftly as possible."

"A question, if I may, sir?" asked Reuben. "How long do we have before shipping stops?"

"That's not entirely known, but it could be as little as a day, from what I've heard. Last night the press finally caught on, and the networks are now carrying the story. Be prepared to be very busy, gentlemen, your country needs you right now. I'll be going with you shortly to a meeting with the Attorney General and the President. Since you two predicted, spotted, and played a major role containing the first wave of this attack, you are our point men on dealing with the second."

Reuben and MadFast looked at each other, or more accurately, they looked at what each other were wearing. Reuben was irreverently wearing a black t-shirt that displayed a modified version of the OSI model. Where the OSI model typically had seven layers, this one had two extra ones added to the top, "politics" and "money," along with humorous descriptions of how they both interfered with the proper development and construction of efficient or secure networked systems. MadFast was wearing a black DefCon t-shirt from the previous year's conference. They both wore jeans.

"Yes, I know. You're not exactly dressed for the occasion. I don't think anyone will mind, don't worry. And there isn't time for a change, in any case. We're due over there in about half an hour. We could do this by video, but I'm guessing you might want the opportunity to shake hands with the President."

"Wow, uh, thank you. Okay. Should we grab our laptops or anything?"

"No, but if you need to use the men's room, I advise you to do so now. It may be a long meeting, and it's poor form to get up to leave in the middle of one."

MadFast and Reuben didn't even look at each other to debate. "Be right back," advised Reuben as they turned to leave. Once outside, they asked Paul for directions, and were led to the nearest restroom.

While washing their hands, they spoke briefly with each other. "Just what kind of a meeting do you think this is going to be?" inquired MadFast.

"I haven't got the slightest idea, man. Just try to relax. We're being brought in as experts now, remember that. Just try to relax, and remember

that you do know your stuff. Don't let the titles and positions intimidate you. Of course, I'm trying very hard to tell myself the same advice right now."

"I bet it'll be easier when we're actually in there, and not just freaking out over it like we are now."

"Good point. Okay, let's get our game on, and go back to Johannsen's office."

"Right on."

They walked back to the office, and steeled themselves for what was next, whatever it would be. Reuben noticed how after enough sequential days of shock after shock, one became used to being in a perpetual state of it. At least he was sleeping well at the end of every day. Between being utterly exhausted from the mental exertion needed just to keep up with everything and the long-needed relief of being able to finally take action and make a difference, he passed out as soon as he hit the bed at night.

Washington, DC: Tuesday, November 25th, 10:30 AM, 2003

The waiting area was quite comfortable, with large plush chairs and a sofa. Reuben and MadFast followed Johannsen's example in sitting down, looking around to take in the surroundings. Reuben had once been on a White House tour, but he was so young at the time, he didn't have any recollection of it now. And he doubted that the tour had visited this part of the building. For want of anything else to do at the moment besides breathe or panic, he chose to breathe, taking deep slow breaths to try and relax.

MadFast was sitting next to him, feeling equally out of his element. Only moments before, they had been introduced to the Attorney General for the first time, and he was slowly getting a grip on that.

The drive over had been a matter of briefing the pair on protocol. Some of this was familiar to Reuben, being a fan of television shows that centered on the White House, and some of it was entirely alien. There was so much protocol with regard to who got to speak first, and about what. Reuben felt that it would have been better if the speaking order were

determined by the meeting, but he was mindful that he had no idea how to run a country, either.

"Are we really going to be in the Oval Office?" asked MadFast quietly.

"Yes, we are. Scared?" asked Johannsen. He smiled, but appeared somewhat nervous himself. The room was almost foreboding with the power it held.

"Uh, yes. A bit."

Reuben nodded jerkily in sympathy. "Yeah, me too." He went back to breathing.

The door opened, and out stepped several people, including some high-ranking military officers who were utterly covered with insignia. Reuben tried not to ponder what the meeting could have been about.

The President's aide exited and addressed the group waiting outside. "The President will see you now."

Reuben took and exhaled another large breath as he stood up. *Here we go,* he thought, as they walked into the Oval Office.

Behind the huge wooden desk was the President, who was appeared to be sorting through a small pile of papers, looking at a small note on one sheet. Upon finishing, he looked up in acknowledgement of their presence. He stepped around from behind the desk and approached everyone, shaking hands with the Attorney General and Johannsen before turning to MadFast to do the same.

"Mr. President, this is Reuben Lev and…Frank Rizzeti, but prefers to be referred to as MadFast," said the Attorney General as he introduced each one in turn.

"MadFast? Interesting alias. What does it mean?" the President asked as they shook hands.

MadFast felt his knees weaken slightly at the question. He was prepared for business, but something personal like this caught him entirely off guard.

"It's an inside joke, Mr. President. Some years ago, a researcher, um, he has a good sense of humor, and I'm not sure how to explain it, but he put a commercial break in the middle of one of his advisories. It purported to be a commercial for something called 'XOR', which is a really awful algorithm that some companies use for encryption. It's completely useless for encryp-

tion, but the commercial focused on some of its good points, and one of them said, 'It's mad fast!' It's one of my favorite jokes, Mr. President."

The President smiled. "Interesting. I hope you'll forgive me if the humor is a bit lost on me."

"It's really geeky, Mr. President. I'm kind of glad that the humor is lost on you, in a way, if that makes sense." MadFast was feeling extremely awkward, and tried to remember the coaching from the car ride over.

The President turned to Reuben. "And you must be Reuben then."

"Yes, Mr. President. Good to meet you." Shaking hands firmly with the leader of the free world was a profound experience.

The President looked down at Reuben's shirt. "Ah, more hacker humor?"

Reuben blushed. "A bit less specific, Mr. President. More like just geek humor."

The President read the t-shirt for a moment. "That's funny. Have a seat, everyone."

"Thank you, Mr. President." Reuben sat down along with everyone else, glad that the meeting would get underway. He felt more comfortable talking business, strangely enough.

"Now, gentlemen," the President began. "Before my press secretary gives the word that I'm declaring a national state of emergency, I need some information from you, and a plan. My understanding is that you two gentlemen have the inside line on the attack, so I wanted to hear what you have to say."

The Attorney General spoke up. "Mr. President, at present we are near to confirmation that this situation is indeed the result of a coordinated attack against both our petrochemical infrastructure and the communications infrastructure of Department of Justice by an unknown attacker. This conclusion is supported by a number of factors, including the simultaneity of the effects and the common characteristics of the impacted facilities."

"Who do we think is behind this? I've already asked this question of other advisers, as you know, but I want your take on it."

"Mr. President, at present we have not received any claims of responsibility for the attack. We know of several countries with an information

warfare capability, ranging from nascent to well-developed, but at this time no other data suggests that any of them is to blame."

"Who's at the top of the list? Who is most able to do this? Speak freely. I know you're not the National Security Adviser, the DCI or the Secretary of Defense. We've got a big problem, and I want everyone's opinion."

The Attorney General nodded. "That would be North Korea, Mr. President. Possibly China, but we feel North Korea has the strongest information warfare program. Intelligence indicates that their capability may even rival our own program at Langley. Of course, I don't know that for a fact, you'd have to ask the DCI for confirmation of that."

"So why don't we think they had any part in it?"

"Well, Mr. President, as I see it, the main reason is one of motive. We can see no reason why they would risk provocation at this time, with the current situation in South Korea being what it is. As you are aware, the South Koreans have been increasingly unhappy with the presence of American troops on their soil. An attack of this form would likely turn sentiment back in favor of maintaining a strong military force on the peninsula, and would also likely provoke us into retaliation. At this time, they have nothing to gain from the attack.

"Despite their actions at times, the North Koreans are not stupid. In a sense, the sophistication of their capability works for us. They know that it's not a guaranteed thing that we might not trace back the attack to them, either using technical means or through HUMINT. And even if they could maintain anonymity in the attack, the impact on our economy would not alter our position or readiness in that part of the world, so they would have nothing to gain."

"So you concur with everyone else who thinks this is an attack, that it's a terrorist incident?"

"Mr. President, at present that remains a mystery to us. We were hoping someone would claim responsibility before it becomes public knowledge, but that is not considered likely at this point. This is the reason for our earlier request that the details of the attack be kept from the public, so that we can validate any claims that may come at a later time."

"Okay, so we don't know who the hell is doing this. So give me some good news. Tell me about the first part of the attack. First of all, how did you see this coming?"

After a moment of silence, the Attorney General prodded Reuben. The President had been asking him.

"Oh, I'm sorry, Mr. President. I'm not accustomed to this, so I tend to clam up."

"Understandable, but it's time to speak up. Your country needs your contribution to this."

Reuben nodded. "The answer to your question is not short, Mr. President." Reuben was eternally grateful for having watched so many television shows about the White House, just for the fact that he reflexively remembered to address the leader correctly now.

"Some years ago, my colleague and I performed a vulnerability assessment on a VPN product for the Department of Justice. We identified a number of issues with the software…"

"Hold on a second. What's a VPN?"

"Ah, sorry Mr. President. VPN stands for Virtual Private Network, and refers to a system that uses encryption to protect communications that pass over public networks, like the Internet. In this case, the VPN is used to enable secure communication between multiple facilities at the DoJ."

"Go on."

"We found a number of serious vulnerabilities with the software, Mr. President." Reuben suddenly realized the predicament he was in. The next words out of his mouth might embarrass his sponsors at this meeting, but at the same time he needed to answer honestly and with all the relevant information. He glanced at Johannsen for a moment, who nodded his head affirmatively. Reuben hoped that meant that the DoJ was ready for what he was about to say.

"Unfortunately, our findings were not exactly taken to heart, Mr. President. A version of the product was implemented that did not include fixes to all of the problems, and we were bound by our NDA to keep quiet. Further calls to attempt to bring the issue to light were unanswered."

"This was still years ago?"

"Yes, Mr. President. Several weeks ago, I happened to notice that scanning had started on the Internet, searching for the VPN application in question."

"You saw the scanning?"

"Yes, Mr. President. There is an organization that, in concert with volunteers, gathers information from multiple organizations and companies and provides summary data. It's called, appropriately enough, the Internet Storm Center, and many professionals look at their website on a daily basis."

"And this site showed the scanning activity you were talking about?"

"Yes, Mr. President. I saw scanning start suddenly, looking for an application that listened on a specific port. And I recognized that port as belonging to the VPN system we had examined earlier."

"What is the purpose of scanning such as you describe?"

"Mr. President, there is only one purpose I can imagine. And that is to discover the location of such systems on the Internet, to attack them later."

"You saw the scan, knew what it was looking for, and knew that an attack was coming. Interesting. Why didn't anyone else do the same?"

"I cannot speak to that, Mr. President, as I don't work for the Department of Justice. I was brought in only a few days ago, after the attack began."

"I don't understand. Why did they bring you in, then?"

Reuben blushed. "Because I wouldn't leave them alone. Once I saw the scanning, I started raising hell, to use the technical term, Mr. President. I tried to warn them."

The President looked toward Johannsen.

Johannsen took the opportunity to step in. "Mr. President, the difficulties described here are largely attributable to a single person, our CISO, who was in charge of the VPN project. Once the attack commenced, one of our contractors was able to bring the matter to the attention of someone not directly under him, and awareness of the issue allowed us to deal with it."

"Ah, I see. I trust this individual has been dealt with?"

"He has been taken out of the loop and will be dealt with accordingly later, yes, Mr. President."

"Good." He turned his attention back to Reuben. "So, do you have any insight into who may be behind the attack?"

Reuben pondered a moment. He had no idea who, but he had an idea of how they worked. He noticed the patterns, and there was some distinction there.

"I'm sorry Mr. President, but I cannot guess what organization is behind it. But I will tell you what I believe. For one, they are very organized. This was not someone playing around. They started scanning all at once, with an organized botnet. In a single day the amount of scanning went from practically nothing to a solid effort. And when they were done scanning, they attacked shortly thereafter. The payload delivered to the machines was quite sophisticated. Rather than just use some kind of rootkit, they instead modified the binaries of the VPN software itself, so that it acted as the listener they needed. Beyond that, I don't know the details, as we've been concerned with getting things back up and running rather than forensic analysis. Someone who can reverse-engineer the binaries could determine more, I'm sure, but I'm not that man."

"First off, I don't understand half of what you just said, but I could just mentally summarize it as an attack by a hacker, yes?"

"Yes, Mr. President."

"Alright then. Now, you said something about reverse-engineering. That's where someone takes the attack apart to see how it worked, correct?"

"Yes, Mr. President, in this case that is exactly correct." *Dammit, you got too geeky. He's the President, not one of your co-workers,* Reuben thought.

"Has anyone been working on that?"

"Not that I'm aware of, but my colleague is capable of performing that task." Next to Reuben, MadFast grinned in acknowledgement.

"Okay, we're getting a bit off track. Do you have any other observations about the attackers?"

"Yes, Mr. President. As I stated, they are savvy. They are also patient. This attack was planned out well in advance. They knew where to hit us, and how, but they were careful not to make a lot of noise on the Internet until they hit us. So either it's a large group of professionals, in which case

I would think they'd be hacking corporations instead, or it's a small group of, well…not professionals."

"If they were in it for the money, they'd do something profitable. They can't make money shutting down our oil supply."

Reuben nodded. "Yes, exactly. There are hackers for profit out there these days. They find business with serious vulnerabilities, and threaten to hack them unless they pay a certain sum. In essence, it's like a protection racket. They seem to like hitting online bookies these days, threatening them with denial of service attacks. The companies get warned that unless they pay up, they'll be knocked offline for long periods of time leading up to large sports events like the Super Bowl, when lots of people place bets. If they're offline during such periods, they lose a lot of business."

"Interesting. Very informative. So, you think it's a few talented hackers with no profit motive and a lot of determination. It sounds more like terrorism to me."

The Attorney General interjected, "Having heard his analysis of it, I have to concur, Mr. President. I'll have a profiler talk with them, but I think he'll arrive at the same conclusion."

Reuben smiled. "I happen to know a few bad guys, Mr. President. I've seen the various types out there, and there are definite types of hackers."

"I take it that if we had to worry about you being one of them you wouldn't be here right now, would you?"

Reuben smiled back. "I suspect not, Mr. President. I will say one more thing. Hackers do things for money, glory, or revenge. None of those reasons are served by secrecy. You will hear from them, one way or another. They aren't doing it for money, so they'll either start bragging to their peers with increasing volume, or they'll take credit outright and contact the government."

"Assuming they aren't in the employ of a nation-state," added one of the quiet intelligence community types.

Reuben nodded. "That's true, Mr. President. That's a twist I hadn't considered. But at the same time, hackers do not always follow authority easily. It's possible that even so, someone will talk. Glory and secrecy are entirely at odds with each other."

"Okay, I've heard enough." The President addressed the Attorney General. "Get these two fully involved, immediately. Bring them into the fold, give them what they need, and make sure we keep them comfortable. We need their help."

"Yes, Mr. President," replied the Attorney General.

Reuben and MadFast simultaneously echoed, "Thank you, Mr. President," as they stood up, the Attorney General joining them. In the back, a smiling Johannsen stood as well, and the quartet left to depart together.

Once outside the meeting room, there were smiles all around. "Well done, gentlemen," said the Attorney General. "I see Johannsen was right about you two."

"I cannot believe that just happened," grinned MadFast. "We were in a meeting with the President! Right on!"

Reuben was suddenly drained, the pressure of the meeting no longer present to keep his energy and focus up. "Wow."

"Okay, I think the next step is to get you two hooked into the effort to recover these facilities. What do you need first?"

"Information," answered MadFast without hesitation. "We don't know much of what's going on. We need to sit down and get some questions answered."

Reuben nodded. "And after that we'll either have more questions, or some ideas. But we don't know enough to do anything but ask questions yet."

"Johannsen, you know better than I do who might have the kinds of answers they're looking for. I'll leave you to look after these two. See to it they can get their work done, and let me know if you get any push-back from anyone." He looked at Reuben's t-shirt, his lips moving as he silently read the words. "Oh, that's *funny!* Great t-shirt, Reuben."

"Thank you, sir."

Later on, back in the Hoover Building, the pair bid goodbye to John, who had been waiting patiently to hear if he was still needed. They reassured him that one way or the other he would be safe. Once he had left they started discussing where to start off with their new task.

"First, we need a solid data set. We're getting information here and there, through sources, but we don't know how reliable it is."

"How's that?"

"Well, they say that all of the facilities are running the same systems software. But what if there are just a few that aren't? Then we have to reconsider everything we're assuming right now. Or if half of them aren't even hooked up to the Internet? Then the attack came in another way. It changes everything."

"Right on, good point."

"So we get some real data collection going on. We need a list of the affected sites, and certain things about them. What systems they run, if they're connected to the Internet, what kind of connection, their IP address range, if they have a firewall, and what the settings on the firewalls are if applicable. Anything I'm missing?"

"Versions. Software versions. How many servers, operating systems. Oh, and recovery things, dude. How often do they backup their stuff, and what's their schedule?"

"Good point. Okay, let's draw up a list. What do we do when we feel sure that it is a hack?"

"Hmm. We need to see what's running. I guess we need to take a field trip to one of these places and see what it actually looks like. Way better than sitting in a room trying to guess."

"Okay, we'll do that while they gather the data for us. Good."

"Oh, duh, I just thought of one more thing."

"What's that?"

"What ports do these systems listen on? Bet you the attackers used the same trick to turn any existing listener into one with extra features for them."

"That makes sense. Gets around firewalls that way too."

"Yep."

"Okay, give me a little while to write this up. Hey, can you ask Johannsen to set up the site visit for us? And then we need to see about lunch. I'm fucking starving. How do you feel about steak for lunch?"

"Right on."

Washington, DC: Tuesday, November 25th, 11:58 AM, 2003

The pair sat down to eat at a French brasserie across the street from the FBI headquarters. Reuben was utterly famished, and had the most bizarre craving for beef.

"So, when do we go?" asked Reuben as he put his menu down.

"This afternoon sometime. He'll let us know when it's all set."

"Great. So I guess we've got a bit of downtime while we get some answers. Are you as scared as I am?"

"Hell yes. I don't feel like I know what I'm doing."

"Me neither. But I've felt that way since Saturday, and it seems that we're still able to do the job. I just keep wondering when we'll hit the point where we can't do it anymore. It's like being off the map; just because you didn't run into a rock yet doesn't mean there aren't rocks out there to hit."

"Yeah, exactly. So what're you thinking?"

"Well, we never promised we could fix it all. I guess we'll just do what we can and hope it helps."

"Right on. Yeah, it doesn't sound like they have another plan. There wasn't another geek at that table today, did you notice?"

"Yeah, I did."

The waitress came, and took their order. It was just before the lunch rush, and the restaurant was ready for the crowd. She sped off to put their order in.

"MadFast, how can you possibly bear to eat your steak so well done?"

"Dude, how can you eat it while it's still mooing?"

They laughed at each other. "You're going to love the steak, this place is great. Although in your case, I don't think I'll recommend their *boudin noir*," he joked, referring to the traditional French blood sausage. "Although it really is quite good here."

"Yeah, I saw that on the menu. No thanks, dude."

"Well, you know me. I'll eat anything."

"Hey dude, you know what you should have done? Had Brianna come join us!"

"Oh, yeah. That's a good idea. Ah well, I should have thought of that myself, and earlier."

"How are things between you two since this ZFon thing came back to haunt us?"

"They were pretty good up until a few days ago. I don't think she's too happy with me being away like this so much, not calling or anything. I'm so stressed, though. I feel like it's all I can take just to be doing this stuff. I panic at the thought of anything else on top of it. This is really important, and I feel like just talking about it will push me over the edge. So right now, we're just in a holding pattern until things calm down. "

"Dude, you gotta relax. You're worrying too much. You've been awesome, I'm glad you're stepping up to speak. I don't think I could deal with it."

"Sure you could, you're a bright guy."

"Yeah, but I'm not from around here. I don't know how this world works."

"Uh, MadFast? We were just both in a meeting with the President of the United States, and we were the only ones wearing t-shirts. I don't have a clue now either, I don't think. But it doesn't matter. They want people who can bring a solution to life, and that's *all* they care about at the moment. Rather unlike the government, isn't it?"

MadFast laughed. "Yeah well, maybe the government really does try."

"Man, where is our food? I'm so hungry. Now, you see? This is what happens when you order your meat well-done. It takes longer than medium-rare." Reuben grinned, teasing MadFast.

MadFast looked around, seeing a sign on the table. "They do cigar dinners here?"

"Yeah, I've been a few times. It's great. It's a prix fixe meal, with cigars that are picked to go with each course. It's a night of heavy smoking, but it's fantastic. Total decadence. And in truth, considering the food and cigars together, it's not really all that expensive for what you get. First Monday of every month."

"Right on. Maybe if I'm still here next week we can come."

"Hey, that's an idea! That is, if things are still running next week."

"Well, if they aren't I think we'll be too busy to smoke cigars and eat French food."

"Good point."

Their food arrived, and Reuben immediately started tearing into his steak. "Mmm, that's good. Yeah."

MadFast must have been just as hungry. "No kidding. What are vegetarians thinking? They're seriously missing out."

They didn't talk much as they polished off their food. Their desire to relax and take some time balanced against the knowledge that they might be needed back at any moment. Their hunger tipped the balance against a leisurely lunch, and they were done eating in short order.

Reuben picked up the check, leaving his customary excessive tip. He noticed for the first time how incredibly strange it felt to walk among all the people around him, knowing that he was aware of things that affected their lives, things they had not the slightest idea were happening. He was responsible, in a way, for all of them on some level. And it was all a secret. He found the secrecy of it oddly comforting. If these people knew his role in their fate, the pressure would be overwhelming. At least in the anonymity came a certain shelter from expectation or accountability.

They crossed the street, pulling their visitor badges out of their pockets, hanging the lanyards around their necks again before re-entering the building. They were starting to find their way around the large building, and had no trouble getting back to their office. There, Paul and Mark were waiting for them with some gear.

"Hey guys, how was lunch?"

"Great. Was good to get out for a bit."

"Excellent. We've got some things for you. Since you'll be in the field you might need these."

Paul handed each of them a cell phone and a document to sign, accepting responsibility for the phones.

"Uh, we have cell phones."

"Not like these you don't. They're encrypted. Fortezza-plus cards in them, they're rated for communications up to top secret. If you need to talk to each other, or to anyone else with regard to your work, use these. I'll show you how they work."

Reuben and MadFast shrugged, and signed the forms. As he pulled out his own phone and started walking through the instructions for establishing a secure connection, Reuben wondered why they were being given this stuff. Neither of them had a clearance, so what was the point of giving them phones that were safe for classified communications?

MadFast asked the question first. "Uh, Paul? What's with the James Bond toys?"

"I don't think I understand the question."

Reuben joined in. "I think he's asking…we don't have a clearance, you guys know that, right?"

"Yes, we know."

"So why do we need phones like this?"

"Well, you *didn't* have a clearance before. But now, you're both being granted TS level."

"What?" MadFast didn't understand.

"You're both being given an interim Top Secret clearance. Orders of the President. You two must have done quite well there. Congratulations."

"Uh, say what? Just like that? Isn't there some kind of, I don't know, like don't you have to ask us things?" MadFast wasn't a Washingtonian, but he clearly had some sense of how such things worked.

"Yes, that's normally how it progresses, but time is short, and your clearance doesn't extend beyond what this project involves. And besides, you've already been party to classified information for some days now, here and there. Why did you think we were standing around you all the time? Part of our job has been to keep an eye on you to see if we thought you'd be trustworthy. Kind of an informal clearance process if you will."

"Wow. Okay. I think I get it now. We've been doing the deed, so there's no harm in taking the leap. You can do that?"

"Yes, in special circumstances, an exemption can be granted to certain aspects of the standard clearance process, and we can get it done as fast as we need. This definitely qualifies, don't you think?"

"Right on," replied MadFast. "Sorry to interrupt, let's get back to learning how to use these hella-cool cell phones."

Everyone laughed as the tension of the moment evaporated.

After Paul was done going over the procedure, which seemed fairly straightforward, he had Reuben and MadFast call each other to make sure they had it down. "Now remember, the phones may be secure, but your immediate environment may not be. Don't make the mistake of discussing sensitive material while in the presence of people who are not cleared for it. You're going to have to use your own judgment as to how to handle that. There's normally a whole day set aside when you get a clearance, where you learn how to handle certain things, and keep out of trouble. You'll get that eventually, and I'm sorry you won't have a chance to have that right now. Just be careful. This afternoon, the President will be releasing a statement declaring the state of emergency and then everyone is going to want to know more. When you show up somewhere, they may ask you. When in doubt, keep quiet. Saying nothing is better than lying, but if you need to lie a little, remember that the best lies are as close to the truth as possible. And once information gets out, it can't get put back in. That about covers it."

"We got it, I think," answered Reuben. "So, where are we going, and when?"

"Good thing about being in the city, we don't have to go far."

Chapter 10

Recovery

Washington, DC: Tuesday November 25th, 3:02 PM, 2003

The pair stood in the control room, looking around. The various workers looked at them strangely, wondering why these two guys in t-shirts rated an FBI escort and a tour of the plant. The two seemed pretty bright, though, and definitely picked up on the computer-oriented aspects of the tour faster than everything else. They mostly seemed interested in the servers of the SCADA master, and how it was interconnected with the rest of the plant. They were awfully serious for people their age, and sure didn't say much aside from some whispers to each other from time to time.

This visit had something to do with the accidents that were happening at all the plants, but that was all anyone was told. Nobody was stupid; they all knew something *big* was happening, and as regularly scheduled programming on the television in the quiet control room was interrupted for a press conference in the White House, the pair suddenly became even more interesting.

"At precisely three P.M. today, Eastern Standard Time, the President has declared a national state of emergency, due to the current situation involving petroleum distribution." The press secretary continued on, finishing the brief statement without providing too much more information. As he droned on, everyone in the room was silent, watching and listening intently. There was a promise of a later address from the President himself, and then the statement concluded. A flurry of hands went up as the press corps started clamoring for answers to questions, at which point people stopped looking at the television, turning instead to look at Reuben and MadFast, with their federal escorts.

Reuben felt the anonymity he was thinking about earlier evaporate around him like a fine mist in the breeze. Not knowing what to do, he simply pretended like he had nothing to do with the press conference, and went back about his business.

Shortly after, the quartet walked out of the facility and got into their car.

"That was really, *really* freaky," commented MadFast as the engine started and Paul drove them out of the plant.

"Yeah, it sure was."

Mark and Paul smiled at each other. Mark smiled and said, "You're doing just fine."

Reuben had no idea what Mark was alluding to. "Huh? Excuse me?"

"The recognition, when people know you're part of something important and secret. Well, some people, when that happens, it gets to them, you know?"

"I certainly felt like it fucking got to me," interjected MadFast.

"Yes, but not like that. I mean, they welcome it. They want more. This is not a good thing for a person who needs to use an encrypted cell phone. It's bad for secrecy, it's bad for security, and most of all, it's bad for judgment. You two clearly don't want the glory, you really do want to help."

Reuben nodded, "Ohhh, I see. Yeah, I really didn't like the attention at all. It's just added pressure, but it doesn't change anything. It isn't like the problem got better after they all started looking at me, or changed. It was just pressure."

"See? That's my point. You two will be just fine as long as you can keep that clear in your heads. You've done well enough."

"I'm glad you have faith, dude," said MadFast, "because I have no fucking idea how we're going to do any of this. That VPN was easy; we were the first people on the planet to know how it was broken, and we had years to think about it. This? I don't even know what half of this stuff is or how it works. I mean, I'm not entirely sure that it's even to blame. It sounds like things work some of the time, and that just doesn't add up."

"Let's see what the data looks like when we get back, MadFast. Remember, it's about the overall picture. Besides, wouldn't that really screw with someone's mind, a problem that only happens part of the time? All you need is a random number evaluator, and there you have it. Think about what they said about how they did the troubleshooting. If the problem comes and goes, it's hard to replicate."

"Yeah, true enough. Okay, that makes more sense to me. Hey, I just had an idea."

"What's that?"

"What you were saying before, about the ISC. Do you think they keep their records for long?"

"Yeah, a while at least. Why?"

"Because their database has both targets and sources, right?"

"Yeah, so?"

"Dude. Their database has sources. They have a list of all the bots. There have to be clues to follow from there."

"Oh, yes! But what if the bots are in other countries?"

Paul answered that question. "You need to keep in mind that we are essentially in a state of war right now. Don't worry about what country the bots are in. We'll send people to go examine them anyways."

"Right on."

Tagig, The Philippines: Wednesday, November 26th, 8:05 AM, 2003

Al-Hakim had summoned the young men as soon as he heard the news. He sipped at the full cup of coffee in his hand as they walked in.

"Good morning, Al-Hakim. You wished to speak with us?" asked Lualhati.

Al-Hakim put the coffee down. "The infidels have finally learned what has been done to them. Their president has called a state of emergency. You have succeeded."

"Allah be praised," replied Agpalo.

"Now it is time for us to take responsibility for the act. We wished to wait, lest we alert them, but now there is no point in the secrecy. It is time for them to learn that they may no longer sit safe in their homes while they oppress our Muslim brothers and send their troops to invade our lands."

The pair became anxious. They loved the notion of getting credit, but feared what may come of them for the notoriety. Ibn Kelbeh had not fared well in recent years, as the Philippine government was cracking down on them.

"Ah, I sense your concern. Fear not, you will be sent to a safer place than here. You have proven your commitment, both to us and to Allah. For a while, we will send you to Pakistan, to be safe among Muslim brothers. It will be a long journey, as you will first go to Indonesia, but I think you will learn much in your travels. Perhaps you may even be able to make a Haj, if you are lucky."

Lualhati and Agpalo didn't know what to make of this. "Our families?"

"Unfortunately, you will need to leave them behind, for now. In time, they may understand. But we cannot risk them accompanying you."

"Yes, Al-Hakim," answered Lualhati. He was torn. On one hand, he had always wanted to belong, to be accepted, and to leave this awful place. But on the other hand, he never imagined that he'd be doing it without his mother, that he would be leaving her behind. And he yearned to be where being Muslim was not something that got you beaten up and ridiculed.

Washington, DC: Wednesday, November 26th, 6:22 AM, 2003

Reuben rolled over, reaching blindly to the floor for the phone that was still attached to his pants. Flipping it open, he laid back in bed. "Reuben."

It was Paul. "Get up, we need you. There's a development."

"Hey Paul. What's up?" He fought to wake up more quickly, and his body started to respond.

"There's been a claim of responsibility, a credible one."

That helped immensely, adrenaline pushing into Reuben's veins. *Jeez, I wish coffee were as strong as bad news,* he thought. *It'd make it damned easy to get to work earlier every morning.*

"Who did it?"

"Ibn Kelbeh. They described both phases of the attack. They apparently don't know we're almost done fixing the damage from the first one."

"Fancy that. Okay, I'm up. I'll get MadFast up, give us ah, 45 minutes?"

"Try to make it 30. There's a meeting."

"Oh shit. Okay."

He put down the phone and put on his watch. He dragged out of bed and stumbled into the living room, where MadFast had crashed on his futon. "Hey man, get up. We've got a meeting to go to."

MadFast stirred and groaned. "Aw, fuck. What time is it?"

Reuben looked at his watch. "Not even six-thirty yet."

"That sucks, dude."

"Yeah, I know. Someone's taken responsibility for the attack."

"Who?"

"Ibn Kelbeh."

"Never heard of them. Who?"

"Ibn Kelbeh. Militant Muslim group in the Philippines. Nasty fuckers, they were behind the kidnapping of some tourists, last year I think. Killed a bunch of them, and then the Philippine army screwed up the rescue and killed off most of the rest of them trying to save them."

"Oh, yeah, I remember hearing about that. Shit, dude, what got us into this? We're fighting terrorists now."

"Don't look at me. I just work here."

MadFast dropped his legs off the futon, and sat up. "I'll make the coffee, you start the shower."

"Works for me." Reuben went into the bathroom and started running the water. He heard the grinder in the kitchen as he walked into the bedroom to pick clothes for the day. He felt it wise to dress a little better in light of the people he would likely be seeing.

Brianna stirred in bed. "Ohhh…what time is it?"

Reuben leaned over the bed and kissed her cheek. "It's early. I'm sorry, Bri, but I gotta go. There's a development." He then kissed her forehead.

She smiled. "Mmmm, head kisses."

"Sorry for waking you up, we'll be out of here soon. There's a meeting we have to get to."

"Good luck, sweetie."

"Hey, Bri? I wanted to say something. I know it's been hard, not knowing from one day to the next when I'll be around, and all that, but thanks for sticking with it and not giving me grief. I can't tell you what I've been doing exactly, but it really is important."

Brianna sat up, propping herself up on one elbow. "I know it is. I see how you've been feeling, and I know that it must be something important. I know how you are, you aren't this driven unless it really does matter."

Reuben smiled and kissed her forehead again. "I met the President yesterday. I'll tell you that much."

Her eyes widened. "Really?"

He smiled wider. "Yes, really."

"Wow. Oh, I'm so proud of you! She hugged him, pulling him back to the bed.

MadFast stuck his head into the bedroom. Reuben struggled to free himself from his girlfriend's bear-hug, feeling embarrassed. "Am I interrupting anything?" MadFast asked.

Brianna let go, and Reuben sat up. "Ah, nope."

"Aw, shucks. Hey, coffee's ready. I made a whole pot in case anyone else wants a cup." He grinned.

"Cool, thanks man. You want the first shower?"

"Sure."

"Water's probably hot now, then. It heats up quick in the morning."

"Right on." He turned and left.

Reuben turned his attention back to Brianna. "I don't know what I can tell you now, but a lot of it will be clearer later on. I'm sure I can say more after this has blown over."

"I watch the news, I can figure some of it out. The FBI sends a driver to pick you up, later that day a private jet flies out to bring MadFast here, you work like crazy down at the FBI and come home exhausted every night, and then the President declares a state of emergency. I think I can guess that they're all connected."

"Well, I can neither confirm nor deny…"

Brianna laughed and hit him with a pillow. "You dork!"

Less than half an hour later, Reuben and MadFast stepped outside to find Paul and Mark waiting for them. They quickly slipped into the car. "Jeez, do you guys ever get to sleep? We're exhausted, you two must be far worse off."

Mark turned to face the pair. "Good morning. And yeah, it's long hours. But during they days it's been pretty easy. You two are doing all the work, all we have to do is stand by in case we're needed. It's not the hardest job in the world."

"Well, that's good. No sense in you two having to suffer because of us."

"Hell, guys, we're loving it. You two are a trip. Who else gets to tag along as two hackers run amok? This is a story to tell our grandkids!"

Reuben and MadFast looked at each other. Neither considered themselves to be of any historical importance.

"Are you goofing on us?" asked MadFast.

Paul spoke up as the car sped down the road. "Are you kidding? You really don't understand yet, even now, do you? This is *history* being made. Do you know what's happening all over the country right now?"

Reuben suddenly noticed how much smoother the trip was, with less lurching of the car. He suddenly realized why. There was practically no traffic.

Mark caught him looking outside. "Yeah, now you get it. Nobody's driving, because there's no gasoline. Shipping is failing. Grocery stores are about to run low. Air travel has been stopped, with the exception of people returning home. And, let's not forget, it's Thanksgiving tomorrow. Or, I

should say, it would be except that everything is breaking down. It's the digital 'Pearl Harbor' that some had been predicting. This is history. And we're two guys who get to hang with the two guys who are helping fight it."

MadFast sat there with his jaw open. Reuben managed to speak. "I gotta ask a favor of you guys. I think I speak for MadFast here too. Please, please, whatever you do, don't talk about us like that again, okay? I can't handle it, and it looks like you put MadFast into shock too. We're just two guys doing what we love to do, and trying to help out. We're not legends, we're not supermen, we're just two guys who happened to be here when it all went down."

"Okay, but if it helps, you should remember that that's true of everyone in history. Nobody was anything like what the books make them out to be. So don't stress it. I'm sure they all felt the same way too. Just keep doing what you've been doing and we will all be fine soon enough."

"Okay, deal." The pair sat back, and remained silent as the car sped along. Instead of turning to go toward the Hoover Building, it went directly to the White House.

"Guess who we're going to see again?" joked MadFast.

"Hey, glad to see you dressed nicer, too," responded Reuben as he realized that MadFast had come to the same conclusion as him when picking clothes.

"This time, it's a big meeting, guys. Not the President, but the Secretary of Homeland Security. The President is getting his morning intel briefing, after which he wants to hear what DHS has to offer."

Reuben and MadFast felt disappointed. They had wanted the President to see what they looked like when they were more presentable, after all.

The car pulled up to the checkpoint, and a Secret Service uniformed officer checked everyone's identification while another officer walked around the car, examining the underside with a mirror. Satisfied as to the occupants, the car got a quick wave through and rolled toward a parking spot outside.

"Different entrance?"

"Yes, last time we didn't have your clearances entirely done, so we had to follow a different protocol. Only people cleared for presidential access

can come in this way. And now that includes all of us. Thanks for the clearance upgrade, guys. We weren't cleared for that before."

"Uh, don't mention it. We've been keeping our eyes on you. I figured you could be trusted." MadFast grinned sardonically.

For whatever reason, all four of them found this to be utterly hysterical, and heads turned in surprise as the four men laughed reservedly, on their way into the White House. The tension had been eating at all of them, so the first thing to make them laugh had an enhanced effect, the way water rips open a dam once it has a small crack to work through.

Ten minutes and a metal detector/X-ray combination checkpoint later, MadFast and Reuben were stepping into the Roosevelt Room. A few people from the Department of Homeland Security were there, and the Secretary was expected shortly. Some of the people sitting around the table were more talkative than others; a few were utterly silent.

Most of the seats at the table were taken, and they were directed to the two that were set aside for them.

A door opened, and the Secretary of Homeland Security entered. "Good morning, everyone. Have a seat."

Everyone settled down, and the meeting began.

"So, we have a credible claim as to who did it, I understand?"

The Attorney General spoke up. "Yes, Mr. Secretary. Ibn Kelbeh, a radical Islamic group in the Philippines, has taken responsibility. We believe they are the true originators of the attack."

"Why, may I ask, do you believe that?"

"Well for one, of all the various claims we have gotten, this is the only one that appears to be genuinely from a terrorist organization. And more importantly, they described both phases of the attack accurately. The first phase is not public knowledge. So we are following that lead, and have contacted the Philippine government. Unfortunately, Ibn Kelbeh operates in a large area and is cellular in structure, so it is difficult to determine which specific group may be behind the attack. But we are following that lead now. Incidentally, Mr. Secretary, I should point out that by the close of business today, the DoJ VPN network will be entirely restored to working

order, thanks to these two gentlemen. The VPN played a part in our communications to chase this lead down."

"Indeed? Well, that's the best news I'm going to hear all day. Fine work, you two."

"Um, yes, Mr. Secretary. Thank you." MadFast replied.

"No, thank you. Both on my behalf and on behalf of your country. But I think I liked you better in the more casual attire. I happened to pass you on my way out the other day, as you were waiting to go into the Oval Office.

Reuben blushed red. "Uh, yes, Mr. Secretary. It's a hacker thing to some degree, I believe. You'll have to forgive us, we're still a bit tired. We're not usually awake this early, much less at work."

"Understood. We keep an early schedule here. But we need to keep moving. I understand you have some ideas as to how to fight this, and some leads to follow in tracking down the attackers?"

"Yes, Mr. Secretary. If you recall, I mentioned an organization called the Internet Storm Center yesterday. It dawned on us that their database probably contains the IP addresses of every machine that performed scanning. And since these machines would have been involved in the attack, it's a start."

"But there's a catch, right?"

"Yes. The machines are not likely to all be within the United States. Most good hackers know to use systems that are in multiple countries, to avoid a trail that exists in only one jurisdiction. So they are in one country, we are in another, and the compromised machines used in the attack are probably in a third. But that's all premature; I have requested the list from the ISC, and I understand they may have provided it to the FBI by now for examination."

The Attorney General interjected. "He is correct, Mr. Secretary. I don't have all the results yet, but as of the last update, it appears all of the systems that can be positively identified are located in Asia. A lot of them happen to be in South Korea."

"Great. I trust you'll be moving on that."

"Yes, Mr. Secretary. We have some people flying out to get to work on that as we speak."

"Good. Keep me posted."

"Yes, sir."

"And you two have an action plan for recovering our petrochemical facilities?"

Reuben prodded MadFast. He really needed to speak to this one.

"You start, I'll pick up when it's my part." MadFast wanted to let Reuben handle as much of this as possible. Not all the faces in the room looked kindly upon their presence, and he definitely felt like an unwelcome interloper. It was clear enough that protocol was being shelved for the moment to give the young intruders a voice.

Reuben nodded, and began speaking. "Mr. Secretary, from what I understand, recovery is complicated by a number of factors. Problem one is that we don't know exactly what the attackers did to the systems at the facilities. I understand that forensics work has determined that they have not used any tools or rootkits that have previously been seen elsewhere. Problem two is that there is no certainty as to when the systems were hacked, so backups may not be trustworthy. And problem three is that since each SCADA implementation is customized to fit the plant, reinstallation is a significant problem."

He continued, "These three factors pose an enormous hurdle to mass recovery of our infrastructure within a short period of time. Our resources are too centralized and limited to deal with this using traditional methods."

"You're learning fast, Reuben. You're speaking like one of us. Go on, I assume you have something that will leap over this hurdle?"

"Yes, sir. We need people who can ferret out the changes in software, and reverse-engineer them. As I said, traditional resources of this type are too few and far between to utilize. But there are non-traditional resources that would be all too happy to serve their country."

"You mean, hackers?"

"Exactly, Mr. Secretary. Not all of them, or just any of them. We are in the unusual position of knowing quite a few. MadFast holds more of that distinction than I do, by far. We suggest you tap their skills. Send them to nearby facilities, and let them work. Give them binaries from a test installation of the SCADA master software, and they will find the parts that do

not belong. They can then develop a patch so that we can repair the installations instead of having to rebuild them."

"Why should we just invite hackers into our petroleum facilities and trust them?"

"An excellent question, Mr. Secretary. I would point out that early on, such people were the only source of information on security. When everyone else was simply building systems any way possible, hackers were the ones testing them, and warning the public about the problems they found. They were the vanguard, the only people trying to get everyone's attention. And those hackers are now heads of companies in an entire industry whose job is to do this kind of work."

"Yes, but what about the hackers who do things like damage websites or commit other crimes?"

"With all due respect sir, there are corrupt police as well. Would you dismiss the entire law enforcement community over their actions? Remember that the crimes you are talking about are relatively new phenomena. The older hackers, the old-school ones, never did such things. It's the script kiddies who do the harm. And script kiddies do not have the skills we need."

One of the quiet types spoke up. "Mr. Secretary, we must advise strongly against this. Granting access to this pair is one thing. But giving criminals access to our key infrastructure, especially at a time like this, is madness." The man spoke as though Reuben and MadFast weren't even in the room.

"Do you have an alternative plan?"

"I, er. Not at this time."

"So what are my other options? Anyone?"

The people all looked at each other. MadFast and Reuben held their breath.

MadFast finally spoke up. "Mr. Secretary, sir. I know these people. They are my friends, some of us go back for years. I trust them. Years ago, Reuben spoke for me, and he told his boss that he would gladly tie his fate to mine, professing that I could be trusted. His boss took him on his word, and because of it we were ultimately able and prepared to help when this attack came. Had his boss refused to trust me, none of that would have

happened. Now, it is my turn. This is important. Whatever harm may arise from anyone I recommend, punish me along with them for it. I know they will do no harm. Tie my fate to theirs."

Reuben lifted his eyebrows and sat back. There wasn't a word he could add to that. Nor was there from anyone else, it seemed. He patted MadFast on the shoulder.

"Well said, MadFast. My kids are going to hear about this. I can't help but share the story of how a hacker named 'MadFast' changed my mind. That's it, then. Make the list and I'll take it to the President. How soon will you have it?"

"That depends, Mr. Secretary. If I need to talk to them first, then that could take a day or two."

"That's not necessary. Time counts."

"Then, for those whose locations I can easily determine, we should give them an invite like the one I got. That will sway them, for sure, without scaring them off. For the others, I can reach them my own way."

"Good. Get going, before things get so bad that our economy starts to fail. Your country is depending on you." He stood up. "Thank you, everyone."

The room stood as well, repeating "Thank you, Mr. Secretary."

The Secretary motioned to Reuben and MadFast, "You two, hang on a moment."

Reuben and MadFast froze in mid-action, sitting back down. This was scary. "Yes, Mr. Secretary," responded Reuben.

"Relax, I just wanted a word with you alone. No cause for concern."

"Yes, sir."

Once the room had emptied of everyone else, and the door was closed again, the Secretary spoke. "I wanted to tell you a couple of things. One, coming into this meeting I was extremely skeptical of you two. But I must say, you have impressed me. I'm going to meet with the President next, and I'm going to push for what you suggested. You have me entirely on board. Well done, both of you."

Reuben and MadFast broke into relieved smiles. "Thank you, Mr. Secretary."

Seoul, South Korea: Wednesday, November 26th, 9:52 PM, 2003

The knock on the door came as the family was preparing for bed.

When the door finally opened, the unhappy-looking gentleman inside was greeted by a member of the police, and a Caucasian in a suit with a large bag.

The officer spoke. "Sir, I apologize for the intrusion at this late hour. It is a matter of great importance. May we come in?" He displayed his badge and credentials.

"Oh, yes, yes, certainly. Come in, please." The man opened his door widely enough to grant access, waving them into his home. "What do you need of me?"

"This is hard to explain, but there has been an attack, and your computer is believed to be involved."

The man flushed red. "How dare you! I have done no such thing. Please leave immediately."

The two visitors cringed at this reaction, while the Korean official slowly waving his hands in hopes of placating the man. "Please, sir, I must explain. We do not think you or anyone in your home had anything to do with the attack. Hackers use other peoples' machines to do their bidding. We believe your machine was used in this way."

The man paused, and began calming down. "Really?"

"Yes, I am afraid so."

"Oh. What do you intend to do?"

"We only need to examine it for a short while. We have brought with us equipment that will make a copy of its hard drive, which is all we require. I must recommend that you reinstall the operating system when we are done, for your own protection."

The man looked positively relieved from this news. "Yes, yes, of course! Here, I will show you where it is. This way, follow me please."

An hour later, the pair departed, with a copy of the drive in their possession. Only two more stops to go.

That night, technicians from the FBI's forensics unit worked tirelessly on the drives. Within hours, they were able to identify the addresses of

some of the bot masters. Fortunately enough, one of them was also in Seoul; a man was sent out to retrieve a drive image of that system as well.

Later examination of the bot master's drive would reveal the address of the machine that controlled it last, located in an Internet café in Tagig. And sitting on its hard drive, in the C:\Temp directory, would be the list of afflicted SCADA systems, right where Agpalo had accidentally left it.

Washington, DC: Thursday, November 27th, 8:09 AM, 2003

"Good news, Reuben." The phone had rung again, but this time Reuben was ready for it. He was getting used to earlier mornings with surprising ease.

"Yes, Paul?" Brianna stirred in the bed next to him, rolling over irritatedly as he got out of bed.

"They know where the attack originated. Tagig. They found the list of attacked SCADA systems on the hard drive of a machine in a cybercafé there."

"Where the hell is that? The Philippines?"

"Bingo. But it's not where they expected. It's not in Mindanao, where Ibn Kelbeh is strongest. It's right near Manila."

"So they're sure this is the machine?"

"Not the only one. The list wasn't complete. Good idea you had, getting the IP address of every afflicted host. We checked this list against that one, and it's only half of them. So there was another machine in the attack."

"You say that like it means something. Does it?"

"Yes, it means there were two people directing the attack. You were right about the size of the group, good call. I thought you'd like to know, I just got word."

"Do we need to come in?"

"It's probably a good idea, yeah. There'll be some activity soon, I think. Some of your boys have been burning the midnight oil. You hacker types are nuts, you know that? I heard that most of them couldn't be held back. They

wanted to get to work instantly, and just went full out from the second they got there. Blue hair, piercings, and all. Hell of a sight, I'm told."

Reuben laughed. "I told them that the recruits would be dedicated. Getting any results back?" Reuben knew that among them were the best reverse-engineers in the world. Success was not a possibility, it was a certainty.

"Not yet, but probably soon. Which is why you guys need to get up. We're coming to get you in a bit, see you in 45."

"Okay, talk to you then." He quickly went to wake up MadFast.

On the drive into the office, they noticed that there were almost no cars to speak of. Parking spots were abundant, and while there were people walking on the sidewalks, there were less than there should have been. It was Thanksgiving morning, and everything was closed, but there was the creepy sense that there was more than a holiday keeping people in their homes. The sooner they got this fixed and started things running again, the better. The previous night, Reuben had put on the news, curious to see how it looked from the perspective of an ordinary citizen. He couldn't bear it for sixty seconds. The impact was so uniformly devastating across the nation that it had made him dizzy, and he went to go play a video game on his computer to try and get his mind off of it. People had canceled plans to be with family and loved ones, everyone was afraid of what might happen next, and to top it off, economic forecasters were predicting dire consequences from such an event happening at the start of the Christmas shopping season.

As for Reuben, he was already doing everything he could think of, and at this point the work was all in the hands of other people. If he exposed himself to any additional pressure, it was a certain fact that he would simply fail to deal with it any longer.

The good news was that the recommendations and plans that MadFast and Reuben had put forth were working amazingly well. Paul's report about the rabid devotion that the hacker recruits demonstrated was no surprise. Such people had no illusions about the tremendous opportunities for upward mobility in their country, and had taken advantage of it. On some level, and hackers were almost universally tremendous fans of democracy.

And to be called to serve as elite soldiers in this online war was, to top it off, an honor that would tap deeply into anyone's ego.

As for the management of such a task, this was the contribution of the government. Apparently, all sorts of plans existed to deal with various disasters, and one of them was an excellent fit for this. Once given both a plan and a purpose, feds and hackers alike truly cooperated, working together so closely that both knew they could trust the other. The feds let the hackers work without interruption and helped wherever they could, and as a result, the hackers relaxed and openly shared their knowledge as they worked. In the end, the entire process ran through a chain of command that had been linked together in short order.

In their office, Reuben and MadFast looked over e-mailed reports of the progress that was being made. Working with known good binaries, the hackers had started finding that which had been changed. There were many files where the changes were a matter of version or configuration differences, but these were sorted out over time. By now, multiple groups in different locations had produced matching lists of the few binaries that were altered and were reverse-engineering the changes. Separately, others were working on patches that would restore them to their original state, while a third group sitting in a lab was winnowing out the vulnerabilities that made the attack possible in the first place.

"This is unfuckingbelievable!" exclaimed MadFast. "It's like an army! Can you believe what they're doing?"

"Yeah, it's pretty rocking! I can't believe that it's going so well. Do you realize that a company that worked like this would just *own*? Can you imagine the work we could accomplish?"

"Yeah, that's what I'm thinking. We're doing what's never been done before, and it's only been one day so far. One day, and we're almost to being fixed. But let's not build business models yet. We've still got a country to fix."

"Well, we did invent the personal computer, *and* the Internet. We've got three-year olds who are computer literate all over the country. We've got a hell of a mindshare to tap into. With all these geeks working on it, of course we can recover quickly. It's beautiful to watch."

"Right on. Well, after this, going back to work normally will be just boring as hell. Thank you, thank you, thank you, for bringing me on board."

"Are you shitting me? Do you really think I could have left you out? Man, you were there from day one. And at every step, I've needed you. Don't get me wrong, I wanted you on for the ride. But I wasn't ever doing you a favor by including you. You totally paid your own way, and then some."

"Right on! Thanks man."

The realization that the end finally was in sight, and that things actually *would* be okay soon, had sunk in. The pair was becoming giddy with the adrenaline, as Paul and Mark watched with amusement. Jane stopped by later that morning.

"Hey fellas, how's it going? I hear it's been a busy week for you. You wouldn't have anything to do with the national crisis, would you?"

"Do you mean causing it, or fixing it?" MadFast grinned.

"Duh. After all, the VPN is back up, and you two are still around. And looking mighty tired, I might add."

"Uh, Jane, what's your clearance level?" Paul was keeping an eye on the details here.

"What?" She looked at MadFast and Reuben. "I thought you two weren't cleared?"

They grinned back at her. "We…weren't. Before." answered MadFast.

"Yeah, we got TS. It's been a busy week."

Jane's jaw dropped. "No shit. Okay, no more questions from me. I'll wait for the motion picture. So, how are you doing? Holding up okay?"

"It's been rough, but we're alright. I think it's almost over, thank God. I doubt I could handle much more." It felt good for Reuben to talk about the strain, to just get it off his chest for a while, talking about himself instead of the country.

"Good, good. We all need to go get blind, stinking drunk after you're done. You too, guys," she added, speaking to Paul and Mark. "The past two weeks have been so totally off the hook, it's a requirement. We must go on a wild drinking bender."

"Hear, hear," chimed in Reuben.

"Right on! Count me in," added MadFast. "And that goes for you two too."

"Which reminds me, guys," spoke Reuben. "You three *must* go to DefCon next year. I insist. And you have to let us spot you."

"Spot us?" asked Jane.

"Why, of course," said MadFast. "You haven't heard of Spot the Fed?"

Tagig, The Philippines: Friday, November 28th, 12:23 AM, 2003

The group was comprised of people from the State Department, the FBI, and the Filipino National Intelligence Coordination Agency, which was tasked with investigating domestic terrorism. They had been going over the combined harvest of technical and human intelligence, and were in agreement. They had found the cell responsible for the attack.

The big break was the bot master in Seoul, which led to the Internet café in Tagig. This, combined with the claim of responsibility by Ibn Kelbeh, brought them to focus the investigation here. In this part of the country, there were relatively few Muslims, and thus even fewer radical Muslims. The cell operating here had never really done much, and thus never really warranted much attention before now. But given the current degree of importance, the NICA gave full cooperation to the United States, and worked a source they had in the area. Apparently, two kids who were quite the computer geeks had started showing up around the cell's local haunt, often spending time in solitude with some older man known only as "Al-Hakim." Some further investigation showed Al-Hakim to be Pakistani, and he seemed to have quite a file with their security force.

The decision was made to strike that night, while they still had a chance of grabbing Al-Hakim and hopefully the kids, as well. Unfortunately, they didn't know that Lualhati and Agpalo were already gone.

Washington, DC: Thursday, November 27th, 6:10 PM, 2003

"Is that it?" Reuben was delirious with disbelief.

"I think so, dude. They found all the bad code, we've got a patch, and the vendor is working on the fix. We recovered the systems, got some fuel flowing, and in a couple of days we patch the fix. I think that's it."

Reuben slumped into his chair. It was over. Years of wondering what might happen, followed by the worst-case scenario, then something far worse heaped on top of that. Surprise visits from the FBI, encrypted phones, private jets, meetings with the President. *My God, how did I get here?* thought Reuben, mimicking an old song in his mind.

MadFast had fared better, amusing himself by changing settings on his laptop. "Dude, check this out," he begged, as he booted up. His computer came up, announcing itself with the classic sound of an old science fiction robot saying, "By your command," with its metallic synthesized voice.

Reuben was finally feeling the entirety of his fatigue. He wanted to sleep for days. And then he wanted to eat, drink, and do utterly nothing of any real value. He wanted to drive his car, ride his new motorcycle, and learn to play the guitar his brother had gotten him the year before. He was tired of working, and knowing he was responsible for a few million people.

"So, do we have to handle patch distribution?" he asked. He wasn't entirely ready to accept that he was done, until he knew for a fact that everything was done.

"No, they have someone taking care of that. I'm telling you, dude, we are *done.* It's *over.*"

"Wow. I can't believe it. It's been…it's been…I don't know what it's been, but it seems so odd to have ended so quietly. A phone call, a couple of e-mails, and that's it?"

"Yeah, I guess so. Sorry dude. I, for one, am ec-fucking-static. I'm going to sleep and then we're all going to go out. You'll feel better after you get some sleep."

"Yeah, you're right. I just need some rest, I guess."

They packed up their gear, looking around the office one last time. They left their spook cell phones behind, and took only what they brought with them at the very beginning when they had first arrived. It felt so strange to leave like this. It was kind of sad, leaving. In this nondescript room that they didn't even really move into, they fought two simultaneous attacks, and won. They changed the course of the first large-scale cyber-terrorism incident in history, and nobody knew just how much of an impact they had caused yet.

They dragged themselves down the hallway one last time, with Mark and Paul behind them. They got into the car and moved out of the underground parking beneath the Hoover Building. The car had enough gas to make it to Adams Morgan and back, which was a good thing since the gas tanks for refueling the FBI's cars had just run dry earlier that day. For the last time, Reuben and MadFast sat in the back as the sirens and lights announced the car's path through the city en route to Reuben's apartment.

But this time, Reuben was barely awake. One thing remained in his mind. "Hey, man."

"Yeah?"

"What do you think happened to the two guys in the Philippines?"

"Huh. I don't know dude. Good question."

Tagig, The Philippines: Friday, November 28th, 2:10 AM, 2003

The team stacked up in a low crouch along the wall, just outside the door. The man in first position inched up, a short-barreled shotgun in his hands as the man in second position pulled the pin on a flashbang grenade, nodding his readiness. Behind him, four other men formed a line, with each man's hand on the shoulder of the man in front of him.

The first man put the muzzle of his shotgun up to the lock on the door, and pulled the trigger. A powdered lead charge fired, blowing a clean hole through the locking mechanism and unlocking the door in a permanent, but effective manner.

As the door swung open, the second man yelled, "*Flashbang, flashbang, flashbang!"* and tossed the grenade through the open door. One and a half

seconds later, a deafening blast and blinding flash of white light erupted inside the small home, and the team moved into the room, splitting left and right to spread across the walls.

Al-Hakim had always known that a time like this might come. He did not expect it now, but that was of no importance. Awakened by the shotgun blast, he rose up straight in bed in time to be deafened by the stun grenade, and somewhat blinded by the flash in the next room. Grabbing the knife by his bed, he got to his feet and charged into the next room somewhat unsteadily.

The FBI assault team did not expect this older man to be so ready. Faced with the choice between losing a team member or killing their objective, they chose the latter. The nearest man to Al-Hakim squeezed the trigger on his submachine gun, which spit a three-round burst into the chest of his target. Al-Hakim swayed for a moment, the bright red of his blood spreading down the white of his clothing, and dropped, slumping to his side.

The team moved into the next room, acting in concert to cover all angles as they slid around the corner. Seeing no other people within the residence, they each announced, "*Clear!*" in turn.

The team leader turned and went to examine Al-Hakim's body. He pulled down the lower part of his balaclava, and pulled out a field radio. "Team leader here. Objective down. Site clear, please advise."

Later that morning, after intelligence agents from both countries worked to exploit the value of the documents found in the apartment, it would be determined that Lualhati and Agpalo had managed to slip away. Their names would be added to watch lists, but it was unlikely the pair would be caught anytime soon. The dissolution of the Ibn Kelbeh cell in Tagig would only serve to increase the caution with which they moved from place to place. The American agent pondered how many had been caught after fleeing in such a fashion, and felt certain that the pair would be caught someday. For now, however, they were safely away, hidden in the world.

The United States, Friday, November 28th, 9:30 AM, 2003

The impact to the economy was significant, but not permanent. As the facilities became trustworthy, they began releasing the stores they contained for distribution, and in turn accepted the contents of various container vehicles that were lined up to replenish them. Gasoline and diesel first went to tanker trucks, then to support shipping, and finally to consumers.

The markets rebounded vibrantly to the recovery from crisis, regaining the losses they had racked up on pessimism following the state of emergency. Later, specialists would estimate the cost over the few days of the event to be in the realm of billions of dollars, but reported that the cost would have increased by orders of magnitude within a week, had it not ended so quickly. For all the damage, Americans rejoiced at their resiliency and power for fending off the attack, and fear gave way to jubilance. The traditional orgy of gift shopping that did not occur the day after Thanksgiving was replaced by frenzied buying throughout the latter half of the season, as optimism and patriotism surged.

Statements from the White House attributed the quick recovery to an unnamed pair of outside experts brought in to address the problem. No names were given, as Reuben and MadFast had requested. They remembered the importance of keeping the pressure away and just focusing on the tech, and worried that the sudden exposure would affect their professional lives to the point where they could no longer manage it. The event went down in the annals of history as the first of a new kind of battle, with the inevitable and correct assumption that there would be more.

Appendix

The Laws of Security

By Ryan Russell

This book contains a fictional account of a zero day exploit, demonstrating criminal hacking techniques that are used every day to exploit vulnerabilities. While this story is fictional, the dangers are obviously real. As such, we've included this appendix, which discusses how to mitigate attacks, such as the one described in this book. While not a complete reference, these security laws can provide you with a foundation of knowledge to prevent criminal hackers from hacking your network and exploiting your vulnerabilities…

Introduction

One of the shortcuts that security researchers use in discovering vulnerabilities is a mental list of observable behaviors that tells them something about the security of the system they are examining. If they can observe a particular behavior, it is a good indication that the system has a trait that they would consider to be insecure, even before they have a chance to perform detailed tests.

We call our list the *Laws of Security*. These laws are guidelines that you can use to keep an eye out for security problems while reviewing or designing a system. The system in this case might be a single software program, or it could be an entire network of computers, including firewalls, filtering gateways, and virus scanners. Whether defending or attacking such a system, it is important to understand where the weak points are.

The Laws of Security will identify the weak points and allow you to focus your research on the most easily attackable areas. This Appendix concerns itself with familiarizing you with these laws.

Knowing the Laws of Security

The laws of security in our list include:

- Client-side security doesn't work.
- You cannot securely exchange encryption keys without a shared piece of information.
- Malicious code cannot be 100 percent protected against.
- Any malicious code can be completely morphed to bypass signature detection.
- Firewalls cannot protect you 100 percent from attack.
- Any intrusion detection system (IDS) can be evaded.
- Secret cryptographic algorithms are not secure.
- If a key isn't required, you do not have encryption—you have encoding.

- Passwords cannot be securely stored on the client unless there is another password to protect them.
- In order for a system to begin to be considered secure, it must undergo an independent security audit.
- Security through obscurity does not work.

There are a number of different ways to look at security laws. In this Appendix, we've decided to focus on *theory*, or laws that are a bit closer to a mathematical rule. (At least, as close as we can get to that type of rule. Subjects as complex as these don't lend themselves to formal proofs.) There's another way to build a list of laws: we could make a list of not what is *possible*, but what is *practical*. Naturally, there would be some overlap—if it's not possible, it's also not practical. Scott Culp, Microsoft's Security Response Center Manager, produced a top-ten list of laws from the point of view of his job and his customers. He calls these "The Ten Immutable Laws of Security." They are:

- Law #1: If a bad guy can persuade you to run his program on your computer, it's not your computer anymore.
- Law #2: If a bad guy can alter the operating system on your computer, it's not your computer anymore.
- Law #3: If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.
- Law #4: If you allow a bad guy to upload programs to your Web site, it's not your Web site any more.
- Law #5: Weak passwords trump strong security.
- Law #6: A machine is only as secure as the administrator is trustworthy.
- Law #7: Encrypted data is only as secure as the decryption key.
- Law #8: An out-of-date virus scanner is only marginally better than no virus scanner at all.
- Law #9: Absolute anonymity isn't practical, in real life or on the Web.

- Law #10: Technology is not a panacea.

The full list (with explanations for what each rule means) can be found at www.microsoft.com/technet/columns/security/10imlaws.asp. This list is presented to illustrate another way of looking at the topic, from a defender's point of view. For the most part, you will find that these laws are the other side of the coin for the ones we will explore.

Before we can work with the laws to discover potential problems, we need to have a working definition of what the laws are. In the following sections, we'll look at the laws and what they mean to us in our efforts to secure our networks and systems.

Client-Side Security Doesn't Work

In the first of our laws, we need to define a couple of concepts in regard to security. What, exactly, are we talking about when we begin to discuss "client-side?" If we were in a network (client-server) environment, we would define the client as the machine initiating a request for service and connection, and the server as the machine waiting for the request for service or connection or the machine able to provide the service. The term "client-side" in the network is used to refer to the computer that represents the client end, that over which the user (or the attacker) has control. The difference in usage in our law is that we call it client-side even if no network or server is involved. Thus, we refer to "client-side" security even when we're talking about just one computer with a piece of software on a floppy disk. The main distinction in this definition is the idea that users (or attackers) have control over their own computers and can do what they like with them.

Now that we have defined what "client-side" is, what is "client-side security?" Client-side security is some sort of security mechanism that is being enforced *solely on the client*. This may be the case even when a server is involved, as in a traditional client-server arrangement. Alternately, it may be a piece of software running on your computer that tries to prevent you from doing something in particular.

The basic problem with client-side security is that the person sitting physically in front of the client has absolute control over it. Scott Culp's Law #3 illustrates

this in a more simplistic fashion: *If a bad guy has unrestricted physical access to your computer, it's not your computer anymore.* The subtleties of this may take some contemplation to fully grasp. You cannot design a client-side security mechanism that users cannot eventually defeat, should they choose to do so. At best, you can make it challenging or difficult to defeat the mechanism. The problem is that because most software and hardware is mass-produced, one dedicated person who figures it out can generally tell everyone else in the world, and often will do so. Consider a software package that tries to limit its use in some way. What tools does an attacker have at his or her disposal? He or she can make use of debuggers, disassemblers, hex editors, operating system modification, and monitoring systems, not to mention unlimited copies of the software.

What if the software detects that it has been modified? Remove the portion that detects modification. What if the software hides information somewhere on the computer? The monitoring mechanisms will ferret that out immediately. Is there such a thing as tamper-proof hardware? No. If an attacker can spend unlimited time and resources attacking your hardware package, any tamper proofing will eventually give way. This is especially true of mass-produced items. We can, therefore, generally say that client-side security doesn't work.

You Cannot Securely Exchange Encryption Keys without a Shared Piece of Information

Although this law may seem obvious if you have worked with encryption, it presents a unique challenge in the protection of our identities, data, and information exchange procedures. There is a basic problem with trying to set up encrypted communications: exchanging session keys securely. These keys are exchanged between the client and server machines prior to the exchange of data, and are essential to the process

To illustrate this, let's look at setting up an encrypted connection across the Internet. Your computer is running the nifty new CryptoX product, and so is the computer you're supposed to connect to. You have the IP

address of the other computer. You type it in and hit **Connect**. The software informs you that it has connected, exchanged keys, and now you're communicating securely using 1024-bit encryption. Should you trust it? Unless there has been some significant crypto infrastructure set up behind it (and we'll explain what that means later in this Appendix), you shouldn't. It's not impossible, and not necessarily even difficult, to hijack IP connections.

The problem here is how do you *know* what computer you exchanged keys with? It might have been the computer you wanted. It might have been an attacker who was waiting for you to make the attempt, and who pretended to be the IP address you were trying to reach. The only way you could tell for certain would be if both computers had a piece of information that could be used to verify the identity of the other end. How do we accomplish this? A couple of methods come to mind. First, we could use the public keys available through certification authorities that are made available by Web browser providers. Second, we could use Secure Sockets Layer (SSL) authentication, or a shared secret key. All of these, of course, are shared pieces of information required to verify the sender of the information.

This boils down to a question of key management, and we'll examine some questions about the process. How do the keys get to where they are needed? Does the key distribution path provide a path for an attacker waiting to launch a man-in-the-middle (MITM) attack? How much would that cost in terms of resources in relation to what the information is worth? Is a trusted person helping with the key exchange? Can the trusted person be attacked? What methods are used to exchange the keys, and are they vulnerable?

Let's look at a couple of ways that keys are distributed and exchanged. When encryption keys are exchanged, some bit of information is required to make sure they are being exchanged with the right party and not falling victim to a MITM attack. Providing proof of this is difficult, since it's tantamount to proving the null hypothesis, meaning in this case that we'd probably have to show every possible key exchange protocol that could ever be invented, and then prove that they are all individually vulnerable to MITM attacks.

As with many attacks, it may be most effective to rely on the fact that people don't typically follow good security advice, or the fact that the encryption end points are usually weaker than the encryption itself.

Let's look at a bit of documentation on how to exchange public keys to give us a view of one way that the key exchanges are handled: www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/113ed_cr/secur_c/scprt4/scencryp.htm#xtocid211509.

This is a document from Cisco Systems, Inc. that describes, among other things, how to exchange Digital Signature Standard (DSS) keys. DSS is a public/private key standard that Cisco uses for peer router authentication. Public/private key crypto is usually considered too slow for real-time encryption, so it's used to exchange symmetric session keys (such as DES or 3DES keys). DES is the Data Encryption Standard, the U.S. government standard encryption algorithm, adopted in the 1970s. 3DES is a stronger version of it that links together three separate DES operations, for double or triple strength, depending on how it's done. In order for all of this to work, each router has to have the right public key for the other router. If a MITM attack is taking place and the attacker is able to fool each router into accepting one of his public keys instead, then he knows all the session keys and can monitor any of the traffic.

Cisco recognizes this need, and goes so far as to say that you "must verbally verify" the public keys. Their document outlines a scenario in which there are two router administrators, each with a secure link to the router (perhaps a terminal physically attached to the console), who are on the phone with each other. During the process of key exchange, they are to read the key they've received to the other admin. The security in this scenario comes from the assumptions that the two administrators recognize each other's voices, and that it's very difficult to fake someone else's voice.

If the administrators know each other well, and each can ask questions the other can answer, and they're both logged on to the consoles of the router, and no one has compromised the routers, then this is secure, unless there is a flaw in the crypto.

We're not going to attempt to teach you how to mimic someone else's voice, nor are we going to cover taking over phone company switches to reroute calls for administrators who don't know each other. Rather, we'll

attack the assumption that there are two administrators and that a secure configuration mechanism is used.

One would suspect that, contrary to Cisco's documentation, most Cisco router key exchanges are done by one administrator using two Telnet windows. If this is the case and the attacker is able to play man-in-the-middle and hijack the Telnet windows and key exchange, then he can subvert the encrypted
communications.

Finally, let's cover the endpoints. Security is no stronger than the weakest links. If the routers in our example can be broken into and the private keys recovered, then none of the MITM attacking is necessary. At present, it appears that Cisco does a decent job of protecting the private keys; they cannot be viewed normally by even legitimate administrators. They are, however, stored in memory. Someone who wanted to physically disassemble the router and use a circuit probe of some sort could easily recover the private key. Also, while there hasn't been any public research into buffer overflows and the like in Cisco's IOS, I'm sure there will be someday. A couple of past attacks have certainly indicated that such buffer overflows exist.

Another way to handle the exchange is through the use of SSL and your browser. In the normal exchange of information, if you weren't asked for any information, then the crypto must be broken. How, then, does SSL work? When you go to a "secure" Web page, you don't have to provide anything. Does that mean SSL is a scam? No—a piece of information has indeed been shared: the root certificate authority's public key. Whenever you download browser software, it comes with several certificates already embedded in the installer. These certificates constitute the bit of information required to makes things "secure." Yes, there was an opportunity for a MITM attack when you downloaded the file. If someone were to muck with the file while it was on the server you downloaded it from or while it was in transit to your computer, all your SSL traffic could theoretically be compromised.

SSL is particularly interesting, as it's one of the best implementations of mass-market crypto as far as handling keys and such. Of course, it is not

without its problems. If you're interested in the technical details of how SSL works, check here: www.rsasecurity.com/standards/ssl/index.html.

Malicious Code Cannot Be 100 Percent Protected against

During the last couple of years, we have seen more and more attacks using weaknesses in operating systems and application code to gain entrance to our systems. Recently, we've seen a number of programs that were quickly modified and redeployed on the Internet and have resulted in widespread disruption of service and loss of data. Why is this? It is because we can't protect 100 percent against malicious code when it changes as rapidly as it does now. We'll take a look at some examples of this in the following section and discuss the anti-virus protection process as an example.

If, like most people, you run a Windows-based operating system (and perhaps even if you have something else), you run anti-virus software. Perhaps you're even diligent about keeping your virus definitions up to date. Are you completely protected against viruses? Of course not.

Let's examine what viruses and Trojans are, and how they find their way onto your computer. Viruses and Trojans are simply programs, each of which has a particular characteristic. Viruses replicate and require other programs to attach themselves to. Trojans pretend to have a different function than the one they actually have. Basically, they are programs that the programmer designed to do something you generally would not want to have happen if you were aware of their function. These programs usually get onto your computer through some sort of trickery. They pretend to be something else, they're attached to a program you wanted, or they arrive on media you inserted without knowing it was infected. They can also be placed by a remote attacker who has already compromised your security.

How does anti-virus software work? Before program execution can take place, the anti-virus software will scan the program or media for "bad things," which usually consist of viruses, Trojans, and even a few potential hacker tools. Keep in mind, though, that your anti-virus software vendor is the sole determiner of what to check for, unless you take the time to develop your own signature files. Signature files are the meat of most anti-

virus programs. They usually consist of pieces of code or binary data that are (you hope) unique to a particular virus or Trojan. Therefore, if you get a virus that does not appear in the database, your anti-virus software cannot help you.

So why is the process so slow? In order to produce a signature file, an anti-virus vendor has to get a copy of the virus or Trojan, analyze it, produce a signature, update the signature file (and sometimes the anti-virus program too) and publish the update. Finally, the end user has to retrieve and apply the update. As you might imagine, there can be some significant delays in getting new virus information to end users, and until they get it they are vulnerable.

You cannot blindly run any program or download any attachment simply because you run anti-virus software. Not so long ago, anti-virus software could usually be relied upon, because viruses propagated so slowly, relying on people to move them about via diskettes or shared programs. Now, since so many computers connect to the Internet, that connectivity has become a very attractive carrier for viruses. They spread via Web pages, e-mail and downloads. Chances are much greater now that you will see a new virus before your anti-virus software vendor does. And don't forget that a custom virus or Trojan may be written specifically to target you at any time. Under those circumstances, your anti-virus software will never save you.

I'd like to tell my favorite "virus variant" story. In April 2000, we saw the introduction of the "I Love You" virus via the Internet. This was another of the virus worms running in conjunction with Microsoft's Outlook e-mail program, and had far greater impact because it sent itself to all of the e-mail recipients in the address book rather than just the first fifty, as did the earlier "Melissa" virus. However, despite the efforts of anti-virus vendors and others to contain the virus, it spread rapidly and spawned a number of copycat viruses in the short time after it was introduced. Why couldn't it be contained more quickly? In the case of a number of my clients, it was because there were far too many employees who couldn't resist finding out *who* loved them so much! Containment is not always the province of your security or implementations of protective software.

Trojans and viruses actually *could* be protected against completely by users modifying their behavior. They probably wouldn't get much done with a computer, though. They'd have to install only software obtained directly from a trusted vendor (however one would go about determining that. There have been several instances of commercial products shipping with viruses on the media). They'd probably have to forgo the use of a network and never exchange information with anyone else. And, of course, the computer would have to be physically secure.

Any Malicious Code Can Be Completely Morphed to Bypass Signature Detection

This law is fairly new to our discussions of security, and it has become much more prevalent over the past year. It is a new truth, since the attackers now have the ability to change the existing virus/Trojan/remote control application nearly as soon as it is released in the wild. This leads to the discussion of the new problem—variants. If we continue the discussion with the anti-virus example, we'll find that if there is even a slight change in the virus code, there's a chance that the anti-virus software won't be able to spot it any longer. These problems used to be much less troublesome. Sure, someone had to get infected first, and their systems were down, but chances were good it wouldn't be you. By the time it made its way around to you, your anti-virus vendor had a copy to play with, and you'd updated your files.

This is no longer the case. The most recent set of viruses propagates much, much more quickly. Many of them use e-mail to ship themselves between users. Some even pretend to be you, and use a crude form of social engineering to trick your friends into running them. This year, we have seen the evidence of this over and over as the various versions of the Code Red virus were propagated throughout the world. As you recall, the original version was time and date functional, with a programmed attack at a U.S. government agency's Web site. It was modified successfully by a number of different individuals, and led to a proliferation of attacks that

took some time to overcome. Why was this so successful? The possibilities for change are endless, and the methods numerous. For instance, you can modify the original code to create a new code signature, compress the file, encrypt the file, protect it with a password, or otherwise modify it to help escape detection. This allows you to move past the virus scanners, firewalls, and IDS systems, because it is a new signature that is not yet recognized as a threat.

Tools & Traps…

Want to Check that Firewall?

There are an incredible number of freeware tools available to you for beginning your checks of vulnerability. Basic tools, of course, include the basic Transmission Control Protocol/Internet Protocol (TCP/IP) tools included with the protocol: ping, tracert, pathping, Telnet, and nslookup can all give you a quick look at vulnerabilities. Along with these, I have a couple of favorites that allow for quick probes and checks of information about various IP addresses:

- SuperScan, from Foundstone Corporation: www.foundstone.com/knowledge/free_tools.html (click on SCANNER).
- Sam Spade, from SamSpade.org: www.samspade.org.

These two tools, among many other very functional tools, will allow you to at least see some of the vulnerabilities that may exist where you are.

Firewalls Cannot Protect You 100 Percent from Attack

Firewalls can protect a network from certain types of attacks, and they provide some useful logging. However, much like anti-virus software, firewalls will never provide 100 percent protection. In fact, they often provide much less than that.

First of all, even if a firewall were 100 percent effective at stopping all attacks that tried to pass through it, one has to realize that not all avenues of attack go through the firewall. Malicious employees, physical security, modems, and infected floppies are all still threats, just to name a few. For purposes of this discussion, we'll leave threats that don't pass through the firewall alone.

Firewalls are devices and/or software designed to selectively separate two or more networks. They are designed to permit some types of traffic while denying others. What they permit or deny is usually under the control of the person who manages the firewall. What is permitted or denied should reflect a written security policy that exists somewhere within the organization.

As long as something is allowed through, there is potential for attack. For example, most firewalls permit some sort of Web access, either from the inside out or to Web servers being protected by the firewall. The simplest of these is port filtering, which can be done by a router with access lists. A simple and basic filter for Internet Control Message Protocol (ICMP) traffic blocking it at the outside interface will stop responses from your system to another when an outsider pings your interface. If you want to see this condition, ping or use tracert on www.microsoft.com. You'll time out on the connection. Is Microsoft down? Hardly—they just block ICMP traffic, among other things, in their defense setup. There are a few levels of protection a firewall *can* give for Web access. Simply configure the router to allow inside hosts to reach any machine on the Internet at TCP port 80, and any machine on the Internet to send replies from port 80 to any inside machine. A more careful firewall may actually understand the Hypertext Transfer Protocol (HTTP), perhaps only allowing legal HTTP commands. It may be able to compare the site being visited against a list of not-allowed sites. It might be able to hand over any files being downloaded to a virus-scanning program to check.

Let's look at the most paranoid example of an HTTP firewall. You'll be the firewall administrator. You've configured the firewall to allow only legal HTTP commands. You're allowing your users to visit a list of only 20 approved sites. You've configured your firewall to strip out Java, JavaScript,

and ActiveX. You've configured the firewall to allow only retrieving HTML, .gif, and .jpg files.

Can your users sitting behind your firewall still get into trouble? Of course they can. I'll be the evil hacker (or perhaps the security-ignorant Webmaster) trying to get my software through your firewall. How do I get around the fact that you only allow certain file types? I put up a Web page that tells your users to right-click on a .jpg to download it and then rename it to evil.exe once it's on their hard drive. How do I get past the anti-virus software? Instead of telling your users to rename the file to .exe, I tell them to rename it to .zip, and unzip it using the password "hacker." Your anti-virus software will never be able to check my password-protected zip file. But that's okay, right? You won't let your users get to my site anyway. No problem. All I have to do is break into one of your approved sites. However, instead of the usual obvious defacement, I leave it as is, with the small addition of a little JavaScript. By the time anyone notices that it has had a subtle change, I'll be in.

Won't the firewall vendors fix these problems? Possibly, but there will be others. The hackers and firewall vendors are playing a never-ending game of catch-up. Since the firewall vendors have to wait for the hackers to produce a new attack before they can fix it, they will always be behind.

On various firewall mailing lists, there have been many philosophical debates about exactly which parts of a network security perimeter comprise "the firewall," but those discussions are not of use for our immediate purposes. For our purposes, firewalls are the commercial products sold as firewalls, various pieces of software that claim to do network filtering, filtering routers, and so on. Basically, our concern is *how do we get our information past a firewall?*

It turns out that there is plenty of opportunity to get attacks past firewalls. Ideally, firewalls would implement a security policy perfectly. In reality, someone has to create the firewall, so they are far from perfect. One of the major problems with firewalls is that firewall administrators can't very easily limit traffic to exactly the type they would like. For example, the policy may state that Web access (HTTP) is okay, but RealAudio use is not. The firewall admin should just shut off the ports for RealAudio, right? Problem is, the folks who wrote RealAudio are aware that this might

happen, so they give the user the option to pull down RealAudio files via HTTP. In fact, unless you configure it away, most versions of RealAudio will go through several checks to see how they can access RealAudio content from a Web site, and it will automatically select HTTP if it needs to do so. The real problem here is that any protocol can be tunneled over any other one, as long as timing is not critical (that is, if tunneling won't make it run too slowly). RealAudio does buffering to deal with the timing problem.

The designers of various Internet "toys" are keenly aware of which protocols are typically allowed and which aren't. Many programs are designed to use HTTP as either a primary or backup transport to get information through.

There are probably many ways to attack a company with a firewall without even touching the firewall. These include modems, diskettes, bribery, breaking and entering, and so on. For the moment, we'll focus on attacks that must traverse the firewall.

Social Engineering

One of the first and most obvious ways to traverse a firewall is trickery. E-mail has become a very popular mechanism for attempting to trick people into doing stupid things; the "Melissa" and "I Love You" viruses are prime examples. Other examples may include programs designed to exhibit malicious behavior when they are run (Trojans) or legitimate programs that have been "infected" or wrapped in some way (Trojans/viruses). As with most mass-mail campaigns, a low response rate is enough to be successful. This could be especially damaging if it were a custom program, so that the anti-virus programs would have no chance to catch it. For information about what can be done with a virus or Trojan.

Attacking Exposed Servers

Another way to get past firewalls is to attack exposed. Many firewalls include a demilitarized zone (DMZ) where various Web servers, mail servers and so on are placed. There is some debate as to whether a classic DMZ is a network completely outside the firewall (and therefore not pro-

tected by the firewall) or whether it's some in-between network. Currently in most cases, Web servers and the like are on a third interface of the firewall that protects them from the outside, allowing the inside not to trust them either and not to let them in.

The problem for firewall admins is that firewalls aren't all that intelligent. They can do filtering, they can require authentication, and they can do logging, but they can't really tell a good allowed request from a bad allowed request. For example, I know of no firewall that can tell a legitimate request for a Web page from an attack on a Common Gateway Interface (CGI) script. Sure, some firewalls can be programmed to look for certain CGI scripts being attempted (phf, for example), but if you've got a CGI script you *want* people to use, the firewall isn't going to able to tell those people apart from the attacker who has found a hole in it. Much of the same goes for Simple Mail Transfer Protocol (SMTP), File Transfer Protocol (FTP), and many other commonly offered services. They are all attackable.

For the sake of discussion, let's say that you've found a way into a server on the DMZ. You've gained root or administrator access on that box. That doesn't get you inside, does it? Not directly, no. Recall that our definition of DMZ included the concept that DMZ machines can't get to the inside. Well, that's usually not strictly true. Very few organizations are willing to administer their servers or add new content by going to the console of the machine. For an FTP server, for example, would they be willing to let the world access the FTP ports, but not themselves? For administration purposes, most traffic will be initiated from the inside to the DMZ. Most firewalls have the ability to act as diodes, allowing traffic to be initiated from one side but not from the other. That type of traffic would be difficult but not impossible to exploit. The main problem is that you have to wait for something to happen. If you catch an FTP transfer starting, or the admin opening an X window back inside, you may have an opportunity.

More likely, you'll want to look for allowed ports. Many sites include services that require DMZ machines to be able to initiate contact back to the inside machine. This includes mail (mail has to be delivered inside), database lookups (for e-commerce Web sites, for example), and possibly

reporting mechanisms (perhaps syslog). Those are more helpful because you get to determine when the attempt is made. Let's look at a few cases:

Suppose you were able to successfully break into the DMZ mail server via some hole in the mail server daemon. Chances are good that you'll be able to talk to an internal mail server from the DMZ mail server. Chances are also good that the inside mail server is running the same mail daemon you just broke into, or even something less well protected (after all, it's an inside machine that isn't exposed to the Internet, right?)

Attacking the Firewall Directly

You may find in a few cases that the firewall itself can be compromised. This may be true for both homegrown firewalls (which require a certain amount of expertise on the part of the firewall admin) and commercial firewalls (which can sometimes give a false sense of security, as they need a certain amount of expertise too, but some people assume that's not the case). In other cases, a consultant may have done a good job of setting up the firewall, but now no one is left who knows how to maintain it. New attacks get published all the time, and if people aren't paying attention to the sources that publish this stuff, they won't know to apply the patches.

The method used to attack a firewall is highly dependent on the exact type of the firewall. Probably the best sources of information on firewall vulnerabilities are the various security mailing lists. A particularly malicious attacker would do as much research about a firewall to be attacked as possible, and then lie in wait for some vulnerability to be posted.

Client-Side Holes

One of the best ways to get past firewalls is client-side holes. Aside from Web browser vulnerabilities, other programs with likely holes include AOL Instant Messenger, MSN Chat, ICQ, IRC clients, and even Telnet and ftp clients. Exploiting these holes can require some research, patience, and a little luck. You'll have to find a user in the organization you want to attack that appears to be running one of these programs, but many of the chat programs include a mechanism for finding people, and it's not uncommon for people to post their ICQ number on their homepage. You could do a

search for victim.com and ICQ. Then you could wait until business hours when you presume the person will be at work, and execute your exploit using the ICQ number. If it's a serious hole, then you now probably have code running behind the firewall that can do as you like.

Any IDS Can Be Evaded

And you ask, "What the heck is an IDS?" IDS stands for *intrusion detection system*. At the time of this writing, there are hundreds of vendors providing combined hardware and software products for intrusion detection, either in combination with firewall and virus protection products or as freestanding systems. IDSs have a job that is slightly different from that of firewalls. Firewalls are designed to stop bad traffic. IDSs are designed to spot bad traffic, but not necessarily to stop it (though a number of IDSs will cooperate with a firewall to stop the traffic, too). These IDSs can spot suspicious traffic through a number of mechanisms. One is to match it against known bad patterns, much like the signature database of an anti-virus program. Another is to check for compliance against written standards and flag deviations. Still another is to profile normal traffic and flag traffic that varies from the statistical norm. Because they are constantly monitoring the network, IDSs help to detect attacks and abnormal conditions both internally and externally in the network, and provide another level of security from inside attack.

As with firewalls and client-side security methods, IDSs can be evaded and worked around. One of the reasons that this is true is because we still have users working hands-on on machines within our network, and as we saw with client-side security, this makes the system vulnerable. Another cause in the case of firewalls and IDS systems is that although they are relatively tight when first installed, the maintenance and care of the systems deteriorates with time, and vigilance declines. This leads to many misconfigured and improperly maintained systems, which allows the evasion to occur.

The problem with IDSs for attackers is that they don't know when one is present. Unlike firewalls, which are fairly obvious when you hit them, IDSs can be completely passive and therefore not directly detectable. They

can spot suspicious activity and alert the security admin for the site being attacked, unbeknownst to the attacker. This may result in greater risk of prosecution for the attacker. Consider getting an IDS. Free ones are starting to become available and viable, allowing you to experiment with the various methods of detection that are offered by the IDS developers. Make sure you audit your logs, because no system will ever achieve the same level of insight as a well-informed person. Make absolutely sure that you keep up-to-date on new patches and vulnerabilities. Subscribe to the various mailing lists and read them. From the attack standpoint, remember that the attacker can get the same information that you have. This allows the attacker to find out what the various IDS systems detect and, more importantly, *how* the detection occurs. Variations of the attack code can then be created that are not detectable by the original IDS flags or settings.

In recent months, IDSs have been key in collecting information about new attacks. This is problematic for attackers, because the more quickly their attack is known and published, the less well it will work as it's patched away. In effect, any new research that an attacker has done will be valuable for a shorter period of time. I believe that in a few years, an IDS system will be standard equipment for every organization's Internet connections, much as firewalls are now.

Secret Cryptographic Algorithms Are Not Secure

This particular "law" is not, strictly speaking, a law. It's theoretically possible that a privately, secretly developed cryptographic algorithm *could* be secure. It turns out, however, that it just doesn't happen that way. It takes lots of public review and lots of really good cryptographers trying to break an algorithm (and failing) before it can begin to be considered secure.

Bruce Schneier has often stated that anyone can produce a cryptographic algorithm without being able to break it. Programmers and writers know this as well. Programmers cannot effectively beta-test their own software, just as writers cannot effectively proofread their own writing. Put another way, to produce a secure algorithm, a cryptographer must know all possible attacks and be able to recognize when they apply to his or her

algorithm. This includes currently known attacks as well as those that may be made public in the future. Clearly no cryptographer can predict the future, but some of them have the ability to produce algorithms that are resistant to new things because they are able to anticipate or guess some possible future attacks.

This has been demonstrated many times in the past. A cryptographer, or someone who thinks he or she is one, produces a new algorithm. It looks fine to this person, who can't see any problem. The "cryptographer" may do one of several things: use it privately, publish the details, or produce a commercial product. With very few exceptions, if it's published, it gets broken, and often quickly. What about the other two scenarios? If the algorithm isn't secure when it's published, it isn't secure at any time. What does that do to the author's private security or to the security of his customers?

Why do almost all new algorithms fail? One answer is that good crypto is hard. Another is the lack of adequate review. For all the decent cryptographers who can break someone else's algorithm, there are many more people who would like to try writing one. Crypto authors need lots of practice to learn to write good crypto. This means they need to have their new algorithms broken over and over again, so they can learn from the mistakes. If they can't find people to break their crypto, the process gets harder. Even worse, some authors may take the fact that no one broke their algorithm (probably due to lack of time or interest) to mean that it must be secure!

For an example of this future thinking, let's look at DES. In 1990, Eli Biham and Adi Shamir, two world-famous cryptographers, "discovered" what they called differential cryptanalysis. This was some time after DES had been produced and made standard. Naturally, they tried their new technique on DES. They were able to make an improvement over a simple brute-force attack, but there was no devastating reduction in the amount of time it took to crack DES. It turns out that the structure of the s-boxes in DES was nearly ideal for defending against differential cryptanalysis. It seems that someone who worked on the DES design knew of, or had suspicions about, differential cryptanalysis.

Very few cryptographers are able to produce algorithms of this quality. They are also the ones who usually are able to break the good algorithms. I've heard that a few cryptographers advocate breaking other people's algorithms as a way to learn how to write good ones. These world-class cryptographers produce algorithms that get broken, so they put their work out into the cryptographic world for peer review. Even then, it often takes time for the algorithms to get the proper review. Some new algorithms use innovative methods to perform their work. Those types may require innovative attack techniques, which may take time to develop. In addition, most of these cryptographers are in high demand and are quite busy, so they don't have time to review every algorithm that gets published. In some cases, an algorithm would have to appear to be becoming popular in order to justify the time spent looking at it. All of these steps take time—sometimes years. Therefore, even the best cryptographers will sometimes recommend that you not trust their own new algorithms until they've been around for a long time. Even the world's best cryptographers produce breakable crypto from time to time.

The U.S. government has now decided to replace DES with a new standard cryptographic algorithm. This new one is to be called Advanced Encryption Standard (AES), and the NIST (National Institute of Standards and Technology) has selected Rijndael as the proposed AES algorithm. Most of the world's top cryptographers submitted work for consideration during a several-day conference. A few of the algorithms were broken during the conference by the other cryptographers.

We can't teach you how to break real crypto. That's okay, though. We've still got some crypto fun for you. There are lots of people out there who think they are good cryptographers and are willing to sell products based on that belief. In other cases, developers may realize that they can't use any real cryptography because of the lack of a separate key, so they may opt for something simple to make it less obvious what they are doing. In those cases, the crypto will be much easier to break

Again, the point of this law is not to perform an action based on it, but rather to develop suspicion. You should use this law to evaluate the quality of a product that contains crypto. The obvious solution here is to use well-established crypto algorithms. This includes checking as much as possible

that the algorithms are used intelligently. For example, what good does 3DES do you if you're using only a seven-character password? Most passwords that people choose are only worth a few bits of randomness per letter. Seven characters, then, is much less than 56 bits.

If a Key Is Not Required, You Do Not Have Encryption—You Have Encoding

This one is universal—no exceptions. Just be certain that you know whether or not there is a key and how well it's managed. As Scott Culp mentions in his law #7, "*Encrypted data is only as secure as the decryption key.*"

The key in encryption is used to provide variance when everyone is using the same small set of algorithms. Creating good crypto algorithms is hard, which is why only a handful of them are used for many different things. New crypto algorithms aren't often needed, as the ones we have now can be used in a number of different ways (message signing, block encrypting, and so on). If the best-known (and foreseeable) attack on an algorithm is brute force, and brute force will take sufficiently long, there is not much reason to change. New algorithms should be suspect, as we mentioned previously.

In the early history of cryptography, most schemes depended on the communicating parties using the same system to scramble their messages to each other. There was usually no key or pass-phrase of any sort. The two parties would agree on a scheme, such as moving each letter up the alphabet by three letters, and they would send their messages.

Later, more complicated systems were put into use that depended on a word or phrase to set the mechanism to begin with, and then the message would be run through. This allowed for the system to be known about and used by multiple parties, and they could still have some degree of security if they all used different phrases.

These two types highlight the conceptual difference between what encoding and encrypting are. Encoding uses no key, and if the parties involved want their encoded communications to be secret, then their encoding scheme must be secret. Encrypting uses a key (or keys) of some

sort that both parties must know. The algorithm can be known, but if an attacker doesn't have the keys, that shouldn't help.

Of course, the problem is that encoding schemes can rarely be kept secret. Everyone will get a copy of the algorithm. If there were no key, everyone who had a copy of the program would be able to decrypt anything encrypted with it. That wouldn't bode well for mass-market crypto products. A key enables the known good algorithms to be used in many places. So what do you do when you're faced with a product that says it uses Triple-DES encryption with no remembering of passwords required? Run away! DES and variants (like 3DES) depend on the secrecy of the key for their strength. If the key is known, the secrets can obviously be decrypted. Where is the product getting a key to work with if not from you? Off the hard drive, somewhere.

Is this better than if it just used a bad algorithm? This is probably slightly better if the files are to leave the machine, perhaps across a network. If they are intercepted there, they may still be safe. However, if the threat model includes people who have access to the machine itself it's pretty useless, since they can get the key as well. Cryptographers have become very good at determining what encoding scheme is being used and then decoding the messages. If you're talking about an encoding scheme that is embedded in some sort of mass-market product, forget the possibility of keeping it secret. Attackers will have all the opportunity they need to determine what the encoding scheme is.

If you run across a product that doesn't appear to require the exchange of keys of some sort and claims to have encrypted communications, think very hard about what you have. Ask the vendor a lot of questions of about exactly how it works. Think back to our earlier discussion about exchanging keys securely. If your vendor glosses over the key exchange portion of a product, and can't explain in painstaking detail how exactly the key exchange problem was solved, then you probably have an insecure product. In most cases, you should expect to have to program keys manually on the various communication endpoints.

Passwords Cannot Be Securely Stored on the Client Unless There Is Another Password to Protect Them

This statement about passwords specifically refers to programs that store some form of the password on the client machine in a client-server relationship. Remember that the client is always under the complete control of the person sitting in front of it. Therefore, there is generally no such thing as secure storage on client machines. What usually differentiates a server is that the user/attacker is forced to interact with it across a network, via what should be a limited interface. The one possible exception to all client storage being attackable is if encryption is used. This law is really a specific case of the previous one: "If a key isn't required, then you don't have encryption—you have encoding." Clearly, this applies to passwords just as it would to any other sort of information. It's mentioned as a separate case because passwords are often of particular interest in security applications. Every time an application asks you for a password, you should think to yourself, "How is it stored?" Some programs don't store the password after it's been used because they don't need it any longer—at least not until next time. For example, many Telnet and ftp clients don't remember passwords at all; they just pass them straight to the server. Other programs will offer to "remember" passwords for you. They may give you an icon to click on and not have to type the password.

How securely do these programs store your password? It turns out that in most cases, they can't store your password securely. As covered in the previous law, since they have no key to encrypt with, all they can do is encode. It may be a very complicated encoding, but it's encoding nonetheless, because the program has to be able to decode the password to use it. If the program can do it, so can someone else.

This one is also universal, though there can be apparent exceptions. For example, Windows will offer to save dial-up passwords. You click the icon and it logs into your ISP for you. Therefore, the password is encoded on the hard drive somewhere and it's fully decodable, right? Not necessarily. Microsoft has designed the storage of this password around the Windows

login. If you have such a saved password, try clicking **Cancel** instead of typing your login password the next time you boot Windows. You'll find that your saved dial-up password isn't available, because Windows uses the login password to unlock the dial-up password. All of this is stored in a .pwl file in your Windows directory.

Occasionally, for a variety of reasons, a software application will want to store some amount of information on a client machine. For Web browsers, this includes cookies and, sometimes, passwords. (The latest versions of Internet Explorer will offer to remember your names and passwords.). For programs intended to access servers with an authentication component, such as Telnet clients and mail readers, this is often a password. What's the purpose of storing your password? So that you don't have to type it every time.

Obviously, this feature isn't really a good idea. If you've got an icon on your machine that you can simply click to access a server, and it automatically supplies your username and password, then anyone who walks up can do the same. Can they do anything worse than this? As we'll see, the answer is yes.

Let's take the example of an e-mail client that is helpfully remembering your password for you. You make the mistake of leaving me alone in your office for a moment, with your computer. What can I do? Clearly, I can read your mail easily, but I'll want to arrange it so I can have permanent access to it, not just the one chance. Since most mail passwords pass in the clear (and let's assume that in this case that's true), if I had a packet capture program I could load onto your computer quickly, or if I had my laptop ready to go, I could grab your password off the wire. This is a bit more practical than the typical monitoring attack, since I now have a way to make your computer send your password at will.

However, I may not have time for such elaborate preparations. I may only have time to slip a diskette out of my shirt and copy a file. Perhaps I might send the file across your network link instead, if I'm confident I won't show up in a log somewhere and be noticed. Of course, I'd have to have an idea what file(s) I was after. This would require some preparation or research. I'd have to know what mail program you typically use. But if I'm in your office, chances are good that I would have had an opportunity

to exchange mail with you at some point, and every e-mail you send to me tells me in the message headers what e-mail program you use.

What's in this file I steal? Your stored password, of course. Some programs will simply store the password in the clear, enabling me to read it directly. That sounds bad, but as we'll see, programs that do that are simply being honest. In this instance, you should try to turn off any features that allow for local password storage if possible. Try to encourage vendors not to put in these sorts of "features."

Let's assume for a moment that's not the case. I look at the file and I don't see anything that looks like a password. What do I do? I get a copy of the same program, use your file, and click **Connect**. Bingo, I've got (your) mail. If I'm still curious, in addition to being able to get your mail I can now set up the packet capture and find your password at my leisure.

It gets worse yet. For expediency's sake, maybe there's a reason I don't want to (or can't) just hit **Connect** and watch the password fly by. Perhaps I can't reach your mail server at the moment, because it's on a private network. And perhaps you were using a protocol that doesn't send the password in the clear after all. Can I still do anything with your file I've stolen? Of course.

Consider this: without any assistance, your mail program knows how to decode the password and send it (or some form of it). How does it do that? Obviously it knows something you don't, at least not yet. It either knows the algorithm to reverse the encoding, which is the same for every copy of that program, or it knows the secret key to decrypt the password, which must be stored on your computer.

In either case, if I've been careful about stealing the right files, I've got what I need to figure out your password without ever trying to use it. If it's a simple decode, I can figure out the algorithm by doing some experimentation and trying to guess the algorithm, or I can disassemble the portion of the program that does that and figure it out that way. It may take some time, but if I'm persistent, I have everything I need to do so. Then I can share it with the world so everyone else can do it easily.

If the program uses real encryption, it's still not safe if I've stolen the right file(s). Somewhere that program must have also stored the decryption

key; if it didn't it couldn't decode your password, and clearly it can. I just have to make sure I steal the decryption key as well.

Couldn't the program require the legitimate user to remember the decryption key? Sure, but then why store the client password in the first place? The point was to keep the user from having to type in a password all the time.

Notes from the Underground…

Vigilance is Required Always!

Much discussion has been raised recently about the number of attacks that occur and the rapid deployment and proliferation of malicious codes and attacks. Fortunately, most of the attacks are developed to attack vulnerabilities in operating system and application code that have been known for some time. As we saw this year, many of the Code Red attacks and the variants that developed from them were attacking long-known vulnerabilities in the targeted products. The sad thing (and this should be embarrassing both professionally and personally) was the obvious number of network administrators and technicians who had failed to follow the availability of fixes for these systems and keep them patched and up-to-date. No amount of teaching, and no amount of technical reference materials can protect your systems if you don't stay vigilant and on top of the repairs and fixes that are available.

In Order for a System to Begin to Be Considered Secure, It Must Undergo an Independent Security Audit

Writers know that they can't proofread their own work. Programmers ought to know that they can't bug-test their own programs. Most software companies realize this, and they employ software testers. These software

testers look for bugs in the programs that keep them from performing their stated functions. This is called *functional testing*.

Functional testing is vastly different from security testing, although on the surface, they sound similar. They're both looking for bugs, right? Yes and no. Security testing (which ought to be a large superset of functionality testing) requires much more in-depth analysis of a program, usually including an examination of the source code. Functionality testing is done to ensure that a large percentage of the users will be able to use the product without complaining. Defending against the average user accidentally stumbling across a problem is much easier than trying to keep a knowledgeable hacker from breaking a program any way he can.

Even without fully discussing what a security audit is, it should be becoming obvious why it's needed. How many commercial products undergo a security review? Almost none. Usually the only ones that have even a cursory security review are security products. Even then, it often becomes apparent later on that they didn't get a proper review.

Notice that this law contains the word "begin." A security audit is only one step in the process of producing secure systems. You only have to read the archives of any vulnerability reporting list to realize that software packages are full of holes. Not only that, but we see the same mistakes made over and over again by various software vendors. Clearly, those represent a category in which not even the most minimal amount of auditing was done.

Probably one of the most interesting examples of how auditing has produced a more secure software package is OpenBSD. Originally a branch-off from the NetBSD project, OpenBSD decided to emphasize security as its focus. The OpenBSD team spent a couple of years auditing the source code for bugs and fixing them. They fixed any bugs they found, whether they appeared to be security related or not. When they found a common bug, they would go back and search all the source code to see whether that type of error had been made anywhere else.

The end result is that OpenBSD is widely considered one of the most secure operating systems there is. Frequently, when a new bug is found in NetBSD or FreeBSD (another BSD variant), OpenBSD is found to be not vulnerable. Sometimes the reason it's not vulnerable is that the problem

was fixed (by accident) during the normal process of killing all bugs. In other cases, it was recognized that there was a hole, and it was fixed. In those cases, NetBSD and FreeBSD (if they have the same piece of code) were vulnerable because someone didn't check the OpenBSD database for new fixes (all the OpenBSD fixes are made public).

Security through Obscurity Does Not Work

Basically, "security through obscurity" (known as STO) is the idea that something is secure simply because it isn't obvious, advertised, or interesting. A good example is a new Web server. Suppose you're in the process of making a new Web server available to the Internet. You may think that because you haven't registered a Domain Name System (DNS) name yet, and because no links exist to the Web server, you can put off securing the machine until you're ready to go live.

The problem is, port scans have become a permanent fixture on the Internet. Depending on your luck, it will probably be only a matter of days or even hours before your Web server is discovered. Why are these port scans permitted to occur? They aren't illegal in most places, and most ISPs won't do anything when you report that you're being portscanned.

What can happen if you get portscanned? The vast majority of systems and software packages are insecure out of the box. In other words, if you attach a system to the Internet, you can be broken into relatively easily unless you actively take steps to make it more secure. Most attackers who are port scanning are looking for particular vulnerabilities. If you happen to have the particular vulnerability they are looking for, they have an exploit program that will compromise your Web server in seconds. If you're lucky, you'll notice it. If not, you could continue to "secure" the host, only to find out later that the attacker left a backdoor that you couldn't block, because you'd already been compromised.

Worse still, in the last year a number of worms have become permanent fixtures on the Internet. These worms are constantly scanning for new victims, such as a fresh, unsecured Web server. Even when the worms are in their quietest period, any host on the Internet will get a couple of

probes per day. When the worms are busiest, every host on the Internet gets probes every few minutes, which is about how long an unpatched Web server has to live. Never assume it's safe to leave a hole or to get sloppy simply because you think no one will find it. The minute a new hole is discovered that reveals program code, for example, you're exposed. An attacker doesn't have to do a lot of research ahead of time and wait patiently. Often the holes in programs are publicized very quickly, and lead to the vulnerability being attacked on vulnerable systems.

Let me clarify a few points about STO: Keeping things obscure isn't necessarily bad. You don't want to give away any more information than you need to. You can take advantage of obscurity; just don't rely on it. Also, carefully consider whether you might have a better server in the long run by making source code available so that people can review it and make their own patches as needed. Be prepared, though, to have a round or two of holes before it becomes secure.

How obscure is obscure enough? One problem with the concept of STO is that there is no agreement about what constitutes obscurity and what can be treated like a bona fide secret. For example, whether your password is a secret or is simply "obscured" probably depends on how you handle it. If you've got it written down on a piece of paper under your keyboard and you're hoping no one will find it, I'd call that STO. (By the way, that's the first place I'd look. At one company where I worked, we used steel cables with padlocks to lock computers down to the desks. I'd often be called upon to move a computer, and the user would have neglected to provide the key as requested. I'd check for the key in this order: pencil holder, under the keyboard, top drawer. I had about a 50 percent success rate for finding the key.)

It comes down to a judgment call. My personal philosophy is that all security is STO. It doesn't matter whether you're talking about a house key under the mat or a 128-bit crypto key. The question is, does the attacker know what he needs, or can he discover it? Many systems and sites have long survived in obscurity, reinforcing their belief that there is no reason to target them. We'll have to see whether it's simply a matter of time before they are compromised.

Summary

In this Appendix, we have tried to provide you with an initial look at the basic laws of security that we work with on a regular basis. We've looked at a number of different topic areas to introduce our concepts and our list of the laws of security. These have included initial glances at some concepts that may be new to you, and that should inspire a fresh look at some of the areas of vulnerability as we begin to protect our networks. We've looked at physical control issues, encryption and the exchange of encryption keys. We've also begun to look at firewalls, virus detection programs, and intrusion detection systems (IDSs), as well as modification of code to bypass firewalls, viruses, and IDSs, cryptography, auditing, and security through obscurity. As you have seen, not all of the laws are absolutes, but rather an area of work that we use to try to define the needs for security, the vulnerabilities, and security problems that should be observed and repaired as we can. All of these areas are in need of constant evaluation and work as we continue to try to secure our systems against attack.

Solutions Fast Track

Knowing the Laws of Security

- ☑ Review the laws.
- ☑ Use the laws to make your system more secure.
- ☑ Remember that the laws change.

Client-Side Security Doesn't Work

- ☑ Client-side security is security enforced solely on the client.
- ☑ The user always has the opportunity to break the security, because he or she is in control of the machine.
- ☑ Client-side security will not provide security if time and resources are available to the attacker.

You Cannot Securely Exchange Encryption Keys

without a Shared Piece of Information

- ☑ Shared information is used to validate machines prior to session creation.
- ☑ You can exchange shared private keys or use Secure Sockets Layer (SSL) through your browser.
- ☑ Key exchanges are vulnerable to man-in-the-middle (MITM) attacks.

Malicious Code Cannot Be 100 Percent Protected against

- ☑ Software products are not perfect.
- ☑ Virus and Trojan detection software relies on signature files.
- ☑ Minor changes in the code signature can produce a non-detectable variation (until the next signature file is released).

Any Malicious Code Can Be Completely Morphed to Bypass Signature Detection

- ☑ Attackers can change the identity or signature of a file quickly.
- ☑ Attackers can use compression, encryption, and passwords to change the look of code.
- ☑ You can't protect against every possible modification.

Firewalls Cannot Protect You 100 Percent from Attack

- ☑ Firewalls can be software or hardware, or both.
- ☑ The primary function of a firewall is to filter incoming and outgoing packets.
- ☑ Successful attacks are possible as a result of improper rules, policies, and maintenance problems.

Any IDS Can Be Evaded

- ☑ Intrusion detection systems (IDSs) are often passive designs.
- ☑ It is difficult for an attacker to detect the presence of IDS systems when probing.
- ☑ An IDS is subject to improper configuration and lack of maintenance. These conditions may provide opportunity for attack.

Secret Cryptographic Algorithms Are Not Secure

- ☑ Crypto is hard.
- ☑ Most crypto doesn't get reviewed and tested enough prior to launch.
- ☑ Common algorithms are in use in multiple areas. They are difficult, but not impossible, to attack.

If a Key Is Not Required, You Do Not Have Encryption—You Have Encoding

- ☑ This law is universal; there are no exceptions.
- ☑ Encryption is used to protect the encoding. If no key is present, you can't encrypt.
- ☑ Keys must be kept secret, or no security is present.

Passwords Cannot Be Securely Stored on the Client Unless There Is Another Password to Protect Them

- ☑ It is easy to detect password information stored on client machines.
- ☑ If a password is unencrypted or unwrapped when it is stored, it is not secure.
- ☑ Password security on client machines requires a second mechanism to provide security.

In Order for a System to Begin to Be Considered Secure, It Must Undergo an Independent Security

Audit

- ☑ Auditing is the start of a good security systems analysis.
- ☑ Security systems are often not reviewed properly or completely, leading to holes.
- ☑ Outside checking is critical to defense; lack of it is an invitation to attack.

Security through Obscurity Does Not Work

- ☑ Hiding it doesn't secure it.
- ☑ Proactive protection is needed.
- ☑ The use of obscurity alone invites compromise.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form. You will also gain access to thousands of other FAQs at ITFAQnet.com.

Q: How much effort should I spend trying to apply these laws to a particular system that I'm interested in reviewing?

A: That depends on what your reason for review is. If you're doing so for purposes of determining how secure a system is so that you can feel comfortable using it yourself, then you need to weigh your time against your threat model. If you're expecting to use the package, it's directly reachable by the Internet at large, and it's widely available, you should probably spend a lot of time checking it. If it will be used in some sort of back-end system, if it's custom designed, or if the system it's on is protected in some other way, you may want to spend more time elsewhere.

Similarly, if you're performing some sort of penetration test, you will have to weigh your chances of success using one particular avenue of attack versus another. It may be appropriate to visit each system that you can attack in

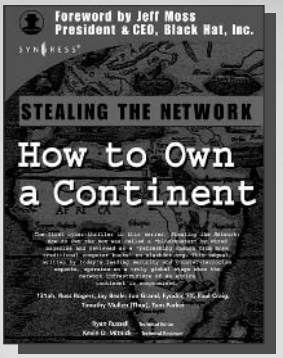
turn, and return to those that look more promising. Most attackers would favor a system they could replicate in their own lab, returning to the actual target later with a working exploit.

Q: How secure am I likely to be after reviewing a system myself?

A: This depends partially on how much effort you expend. In addition, you have to assume that you didn't find all the holes. However, if you spend a reasonable amount of time, you've probably spotted the low-hanging fruit—the easy holes. This puts you ahead of the game. The script kiddies will be looking for the easy holes. Even if you become the target of a talented attacker, the attacker may try the easy holes, so you should have some way of burglar-alarming them. Since you're likely to find something when you look, and you'll probably publish your findings, everyone will know about the holes. Keep in mind that you're protected against the ones you know about, but not against the ones you don't know about. One way to help

Syngress: *The Definition of a Serious Security Library*

Syn·gress (sin-gres): *noun*, *sing*. Freedom from risk or danger; safety. See *security*.



AVAILABLE NOW
order @
www.syngress.com

Stealing the Network: How to Own a Continent

131ah, Russ Rogers, Jay Beale, Joe Grand, Fyodor, FX, Paul Craig, Timothy Mullen (Thor), Tom Parker, Ryan Russell, Kevin D. Mitnick

The first book in the "*Stealing the Network*" series was called a "blockbuster" by Wired magazine, a "refreshing change from more traditional computer books" by Slashdot.org, and "an entertaining and informative look at the weapons and tactics employed by those who attack and defend digital systems" by Amazon.com. This follow-on book once again combines a set of fictional stories with real technology to show readers the danger that lurks in the shadows of the information security industry... Could hackers take over a continent?

ISBN: 1-931836-05-1

Price: $49.95 US $69.95 CAN

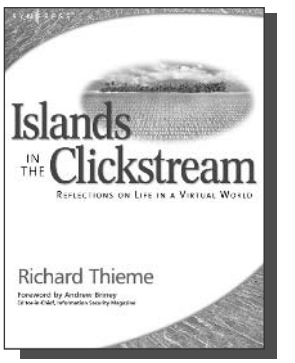
AVAILABLE NOW
order @
www.syngress.com

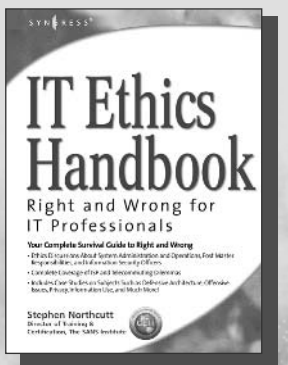
Richard Thieme's Islands in the Clickstream: Reflections on Life in a Virtual World

Richard Thieme is one of the most visible commentators on technology and society, appearing regularly on CNN radio, TechTV, and various other national media outlets. He is also in great demand as a public speaker, delivering his "Human Dimension of Technology" talk to over 50,000 live audience members each year. *Islands in the Clickstream* is a single volume "best of Richard Thieme."

ISBN: 1-931836-22-1

Price: $29.95 US $43.95 CAN





AVAILABLE NOW
order @
www.syngress.com

IT Ethics Handbook: Right and Wrong for IT Professionals

Stephen Northcutt

The final word on ethics and IT management from world-renowned security expert Stephen Northcutt, former Chief for Information Warfare at the Ballistic Missile Defense Organization and current Director of Training and Certification for the SANS Institute. This is not a textbook. Rather, it provides specific guidelines to system administrators, security consultants, and programmers on how to apply ethical standards to day-to-day operations.

ISBN: 1-931836-14-0

Price: $49.95 US $69.95 CAN

SYNGRESS®

TEAM LinG - Live, Informative, Non-cost and Genuine!