

A hand holding a key against a background of binary code. The key is dark and metallic, with a simple, functional design. The hand is positioned as if holding the key, with the thumb and index finger visible. The background is a dark blue gradient with a pattern of white binary digits (0s and 1s) scattered across it. The overall aesthetic is technical and digital.

Introduction

Welcome to the course

Ethical Hacking and penetration testing

Teachers:

Hans Jones hjo@du.se

Computer attacks in general 1

- Computers are constantly under attacks (check the logs!)
 - AV companies use “Honey Monkey” computers as Windows XP SP0 / IE6
 - Example: F-Secure – 250k attacks/day – 20k fresh samples/day (2014)
- Who are they?
- Outsiders
 - Individuals
 - Organized crime
 - States/state supported actors
 - The competition
 - Hacktivists
 - Hired guns
 - Terrorists
 - ...



Computer attacks in general 2

- Who are they cont...?

- Insiders

- Dissatisfied / abusive, sloppy / ignorant (former) employees
- Customers, suppliers and business partners
- Consultants, temporary staff, visitors, etc.

- Skills and capacities?

- From "script kiddies"
- People with moderate skill
- Elite hackers and security consultants
- To organizations with unlimited resources!

- Never underestimate your adversary online!

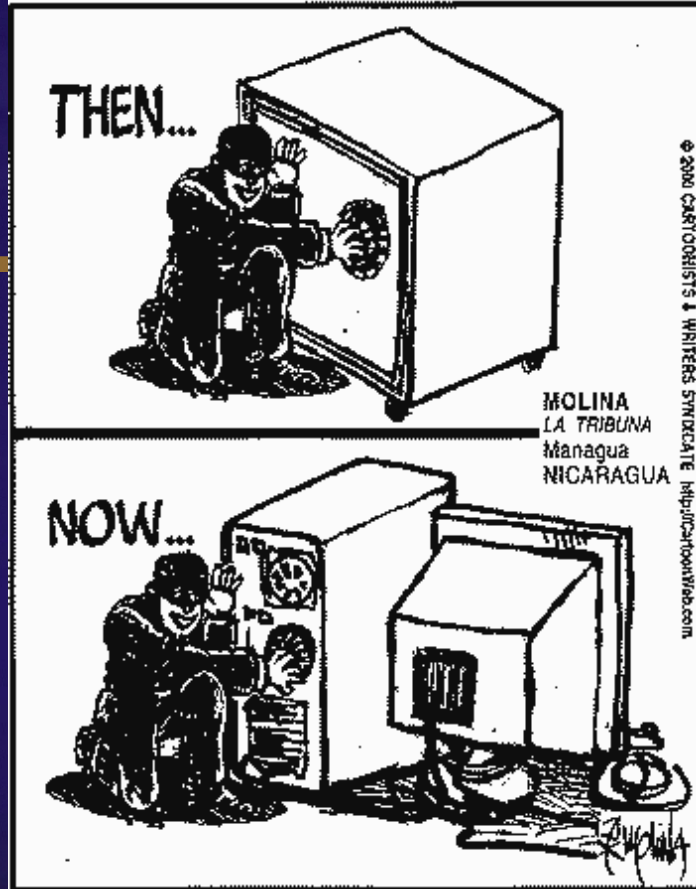


]HackingTeam[

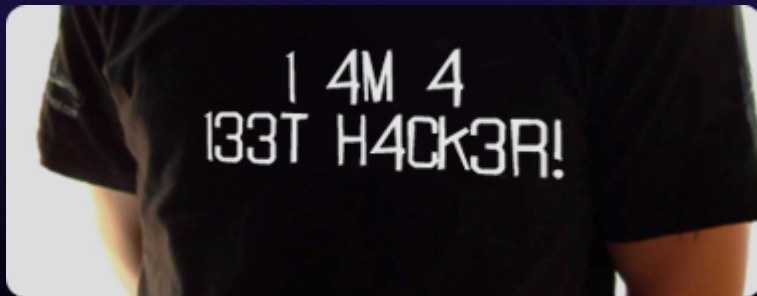
<http://www.hackingteam.it/index.php/remote-control-system>

Why are they doing it?

- Fun, excitement and fame
- Today, most of it goes on making money or damage various systems
 - This is where the money is, and with the right knowledge you can earn big money!
 - Computing power = money (crypto-currencies)
- Usurping valuable / confidential information



Then



Fame

Now



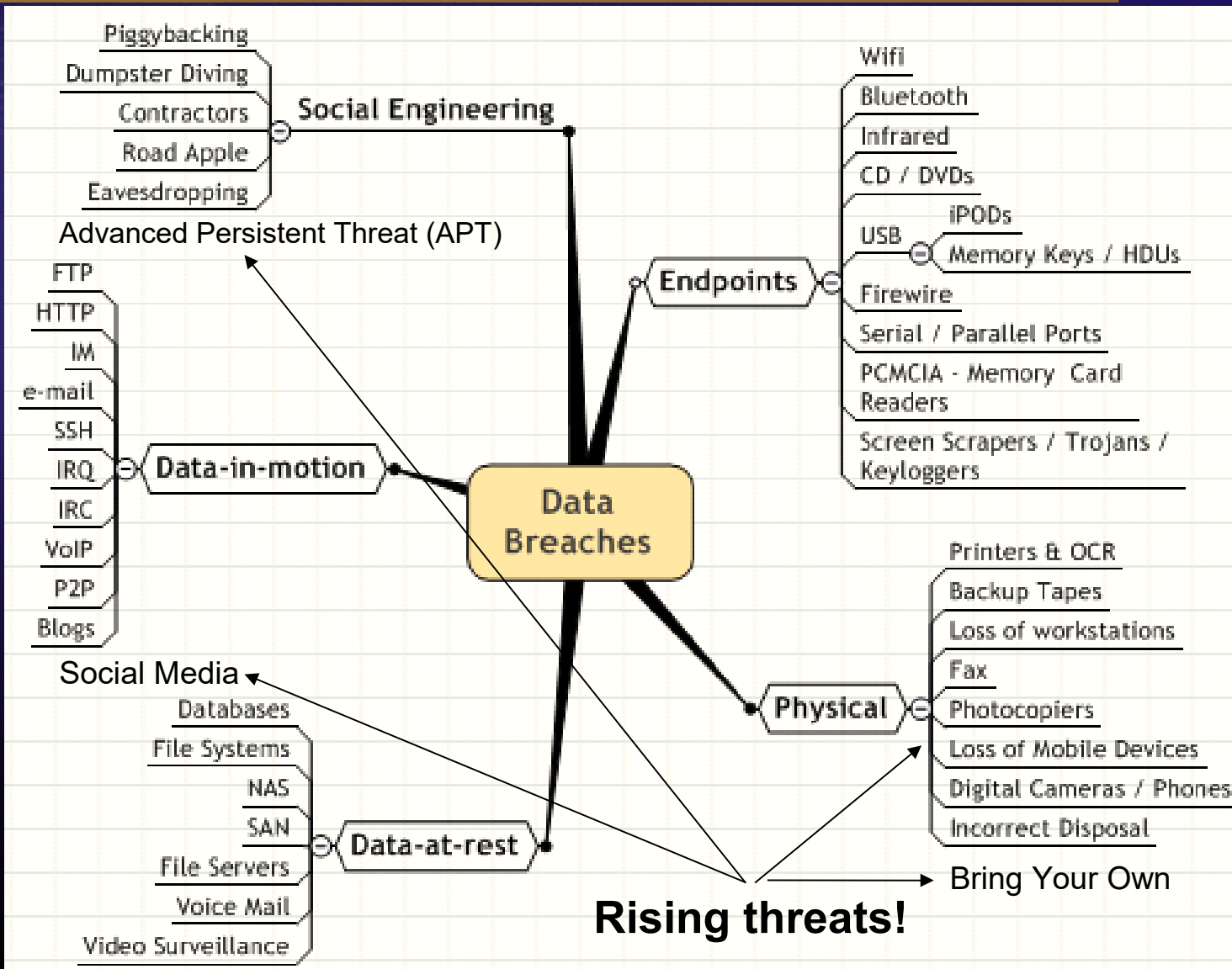
Money

Cybercrime over the past 10 years

- 1st Generation – Because I can and propaganda
 - Worms, defacement of web sites
- 2nd Generation – I can make money
 - Botnets appear, denial of service attacks, seeking payment to stop attacks
- 3rd Generation – Organized crime
 - Large scale management of attacks, coordinated use of tools and techniques, trojans, worms
Phishing, targeted attacks
- 4th Generation – Selling the tools
 - Tools to perform attacks become “vended” with 24/7 support available, Botnet rentals, sophisticated Id theft services, Licensed Malware appears, Exploit knowledge is sold. Social Networks just for cybercriminals appear. Cybercrime supply chains are formalized and fine tuned
- 5th Generation - Our new reality is zero-day, Advanced Persistent Threats (APT) and state-sponsored attacks as for example the Stuxnet worm
- Security is like the Cold War - the faster we implement protections, the faster the cybercriminals innovate



Who got everything covered?



Basic Security Terminology 1

- CIA (Confidentiality, Integrity, Availability) security goals
- Confidentiality
 - Confidentiality means that people cannot read sensitive information, either while it is on a computer or while it is traveling across a network.
- Integrity
 - Integrity means that attackers cannot change or destroy information, either while it is on a computer or while it is traveling across a network. Or, at least, if information is changed or destroyed, then the receiver can detect the change or restore destroyed data.
- Availability
 - Availability means that people who are authorized to use information are not prevented from doing so



Basic Security Terminology 2

- Compromises
 - Successful attacks
 - Also called incidents
 - Also called breaches (not breeches)
- Countermeasures
 - Tools used to thwart attacks
 - Also called safeguards, protections, and controls
 - Types of countermeasures
 - Preventative – keep attacks from succeeding
 - Detective – identify when a threat is attacking and if it was successful
 - Corrective – get back on track after a compromise



How are information stolen (intrusion)?

Verizon 2016 Data Breach Investigation Report

<http://www.verizonenterprise.com/DBIR>

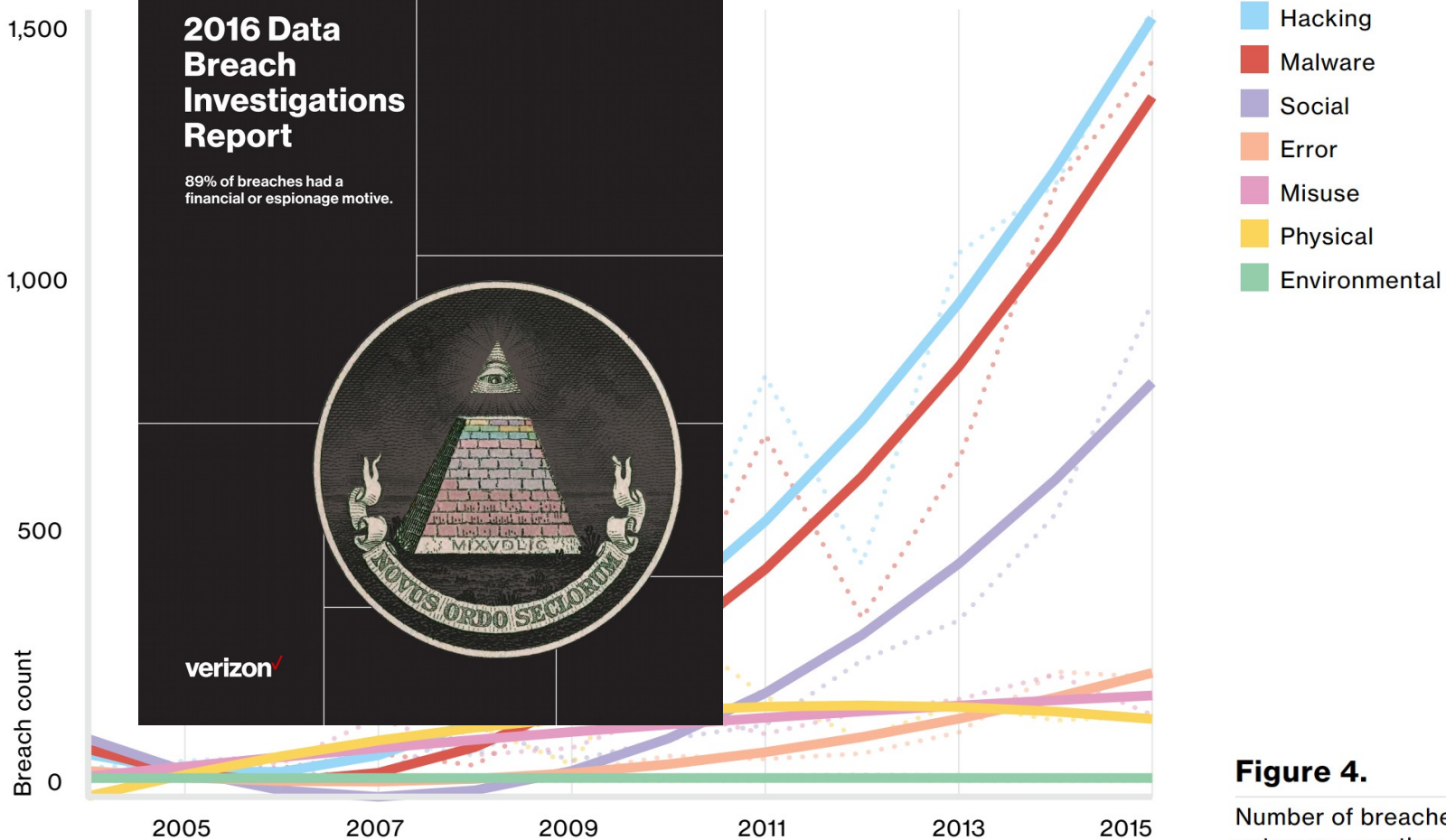


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

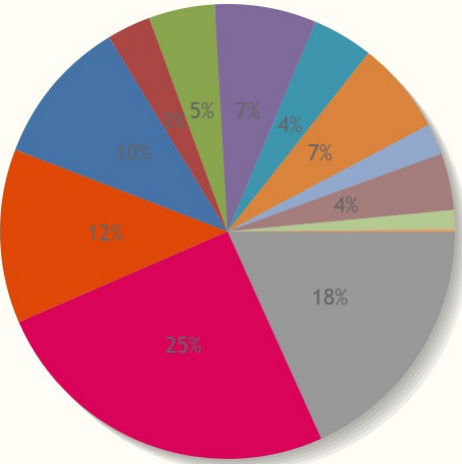
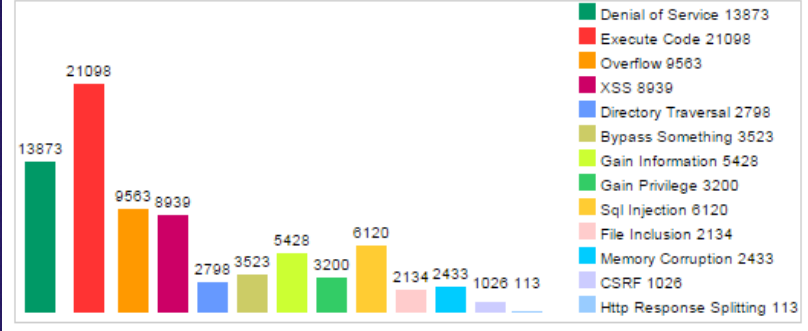
CVE Details

The ultimate security vulnerability datasource

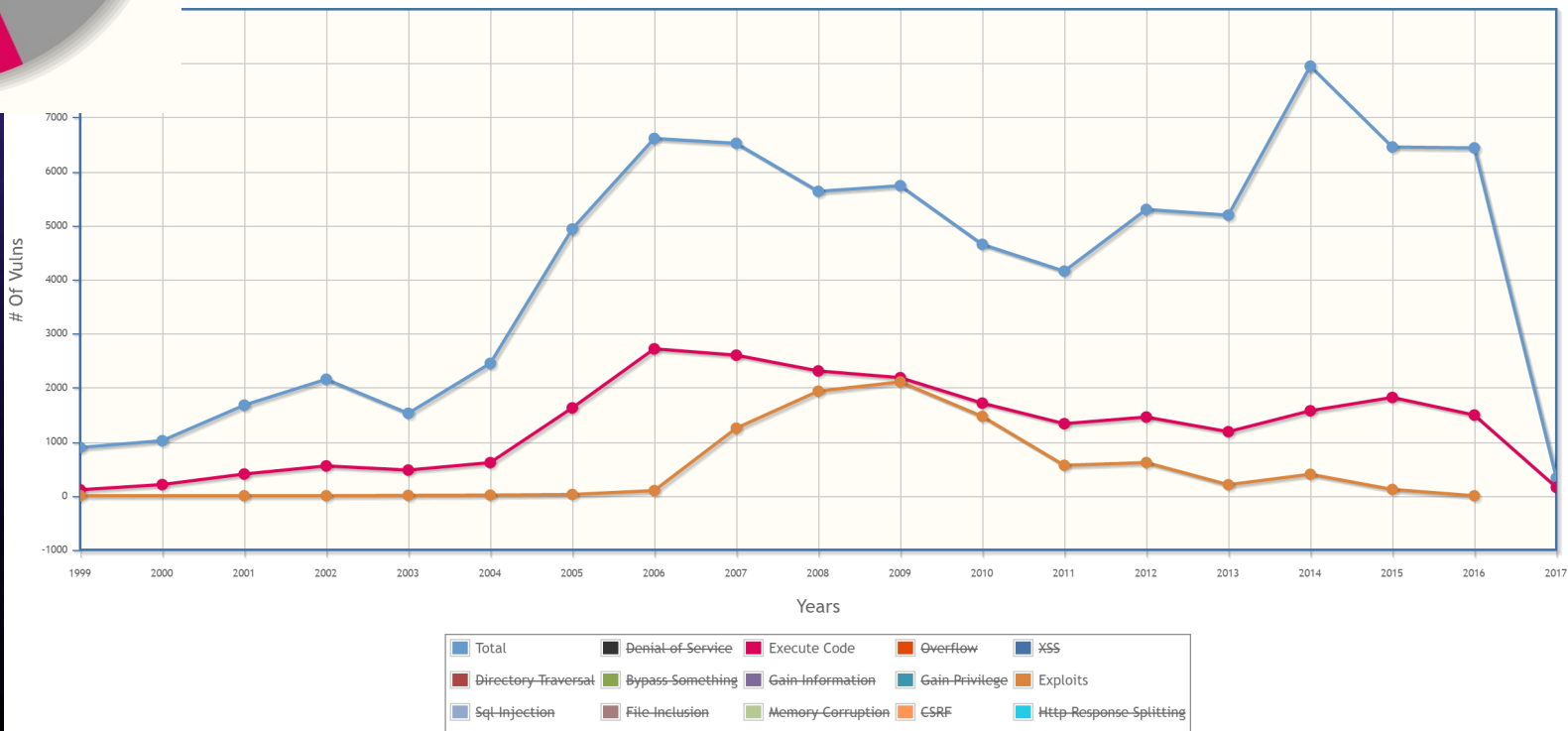
<http://www.cvedetails.com/>

2017-01

Vulnerabilities By Type



Vulnerabilities by type & year

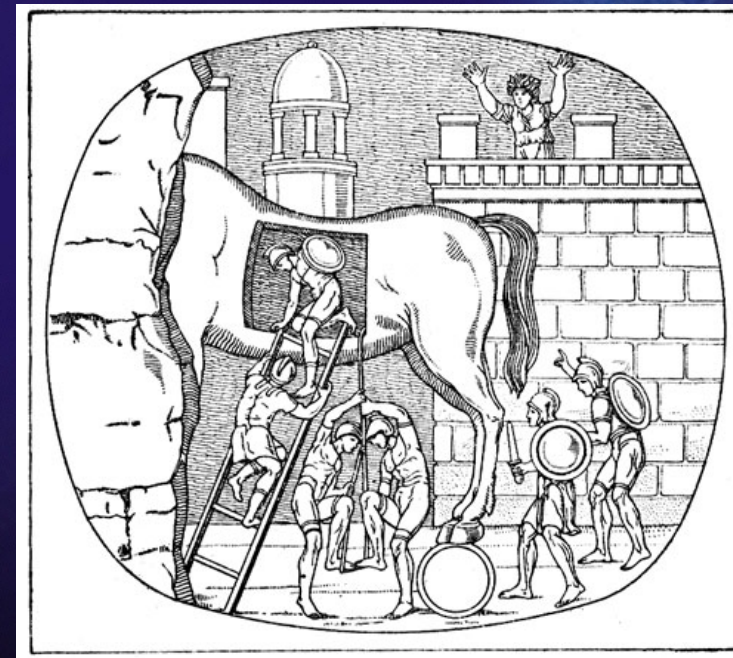


- Denial of Service
- Execute Code
- Overflow
- XSS
- Directory Traversal
- Bypass Something
- Gain Information
- Gain Privilege
- Sql Injection
- File Inclusion
- Memory Corruption
- CSRF
- Http Response Splitting

- Total
- Denial-of-Service
- Execute Code
- Overflow
- XSS
- Directory Traversal
- Bypass-Something
- Gain-Information
- Gain-Privilege
- Exploits
- Sql-Injection
- File-Inclusion
- Memory-Corruption
- CSRF
- Http-Response-Splitting

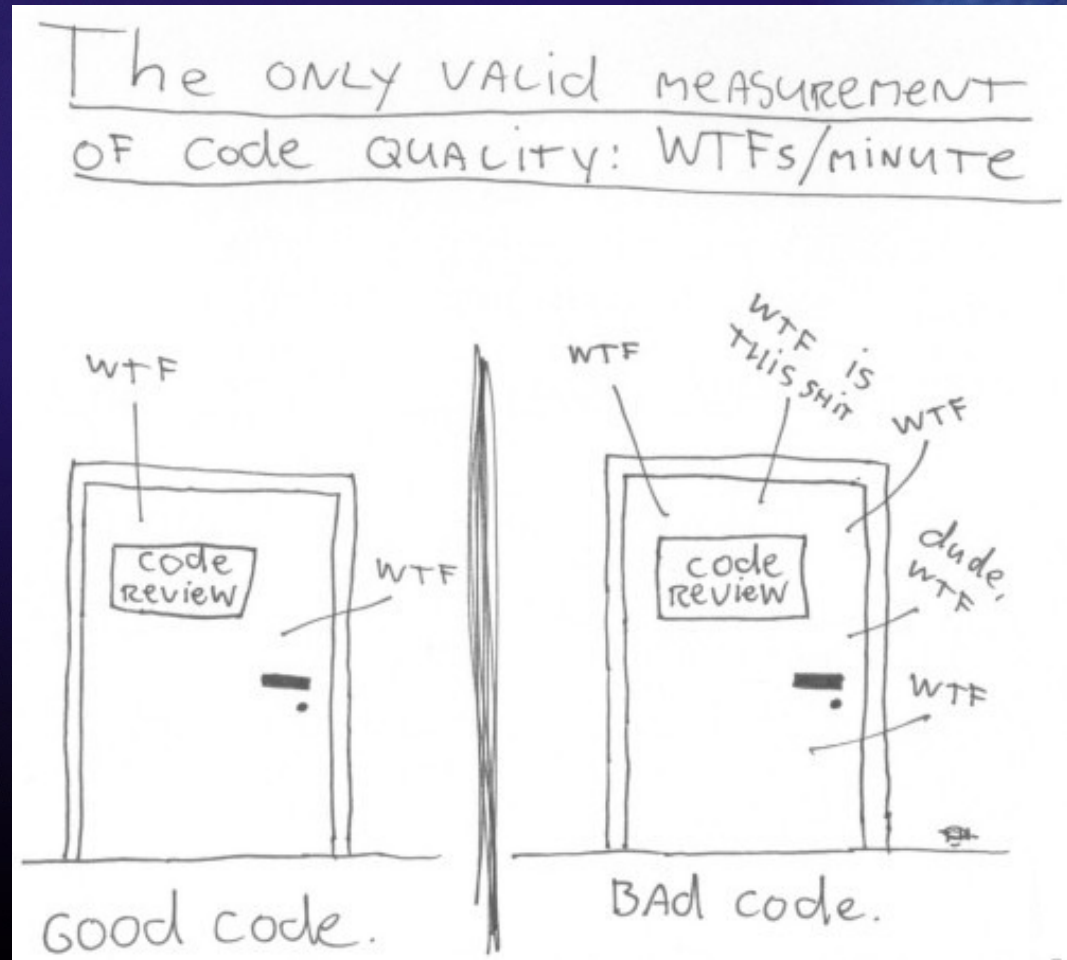
Why does this happen I?

- Lots of configuration mistakes, program errors and information leakage
 - Awareness is the main issue
 - Trojan attack for example
- Configuration mistakes
 - Default accounts and passwords
 - File system permissions
 - Unused services enabled
 - Bad or low security settings/policy
 - Can be misused with normal applications



Why does this happen II?

- Programming errors
 - Buffer overflows
 - Overwrite memory
 - Web applications
 - Accessible and able to manipulate
 - SQL-injection
 - Change strings (SQL)
 - Misuse often requires 'exploits'



Why does this happen III?

- Information leakage
 - Clear text passwords / information in network traffic : encryption < 15%
 - Stale documents on web servers
 - Passwords on post-it notes stored inside or on the computer
 - User credentials in programming comments
 - Bad or low security settings/policy
 - Can be misused with normal applications

I seek what you leak.

DATA LEAKAGE

Ensure sensitive information on laptops, mobiles and removable media is encrypted.

Check email recipients before sending and be mindful of information you post online.

Copyright 2009. www.Security.com. All Rights Reserved.

Why does this happen IV?

- Some contributing factors
 - Computer security has not been a priority in IT solutions
 - Programmers have not learned security
 - Few security audits
 - Unsafe program languages
 - Programmers are lazy
 - Consumers do not care about security
 - Security may make things harder to use
 - Security is difficult, expensive and takes time to implement



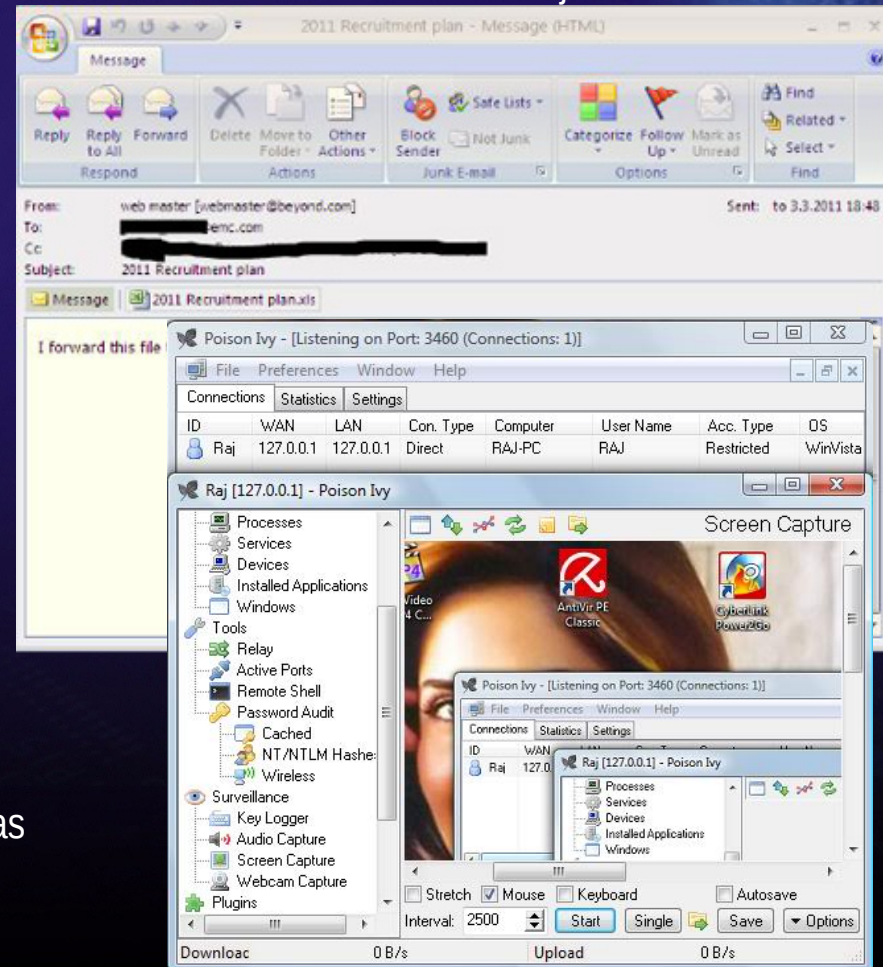
Very hard to fix
all 3 corners!



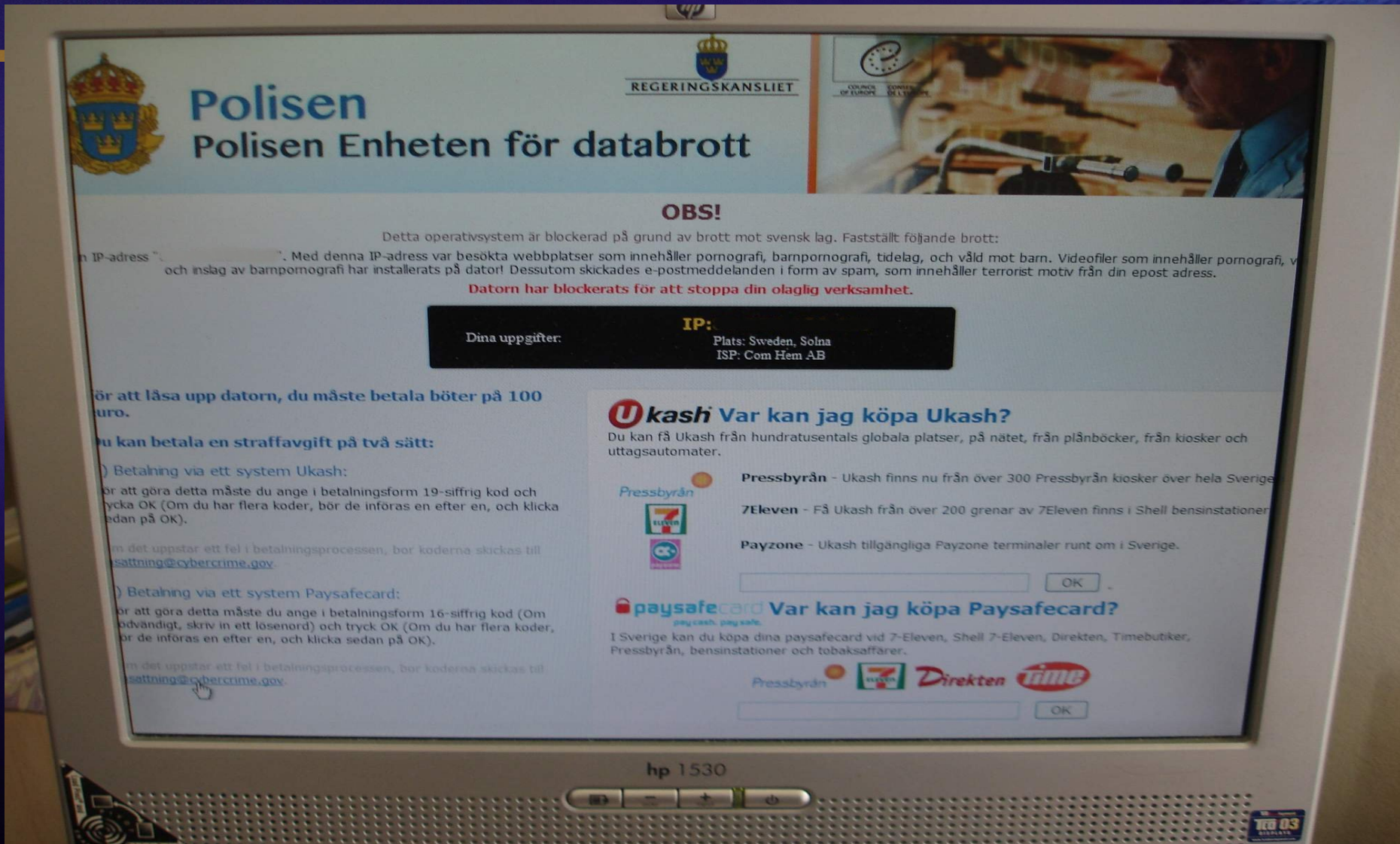
RSA attack 2011-03



- RSAs two-factor authentication to generate temporary codes for increased security.
- It all started with a well crafted phishing email to a non-technical staff member with the subject line “2011 recruitment plan”.
- Attached to the email was an excel spreadsheet that contained an exploit for a known vulnerability in Adobe Flash.
- The exploit installed a hard-to-detect remote administration tool named Poison Ivy on at least one RSA computer. The end result was that an attacker gained access to the RSA network.
- The attackers moved from system to system harvesting accounts until they came across those users who had highly privileged access to sensitive systems and data.
- An internal staging system was “created” to collect, encrypt and transmit back up lists of usernames/passwords to systems.
- Confidential material related to SecurID technology was FTPed to a remote site.
- The attackers have not been identified.



Ransomware - trojan attack 2012-03



- Blog: <http://blog.perhellqvist.se/blog/2012/03/14/ny-elaking-laser-datorn-och-kraver-losensumma/>
- Technical paper: http://sophosnews.files.wordpress.com/2012/03/blackhole_paper_mar2012.pdf

The Digital Arms Race



- A, B and C exists, now is the time for the D weapons!
 - The Internet will play a crucial role for war in the future in order to paralyze computer networks and infrastructure
- NSA and GCHQ's mass surveillance is just the beginning
 - Documents from Edward Snowden shows that the intelligence services of arming themselves for the future of digital warfare
 - Sweden, will according to an article (2015-03-18) DN acquire similar capabilities
 - <http://www.dn.se/nyheter/sverige/ministern-vi-ska-kunna-genomfora-egna-cyberattacker/>
- The NSA is also building an autonomous online defense system "Monsters Mind", which can not only crush the digital attacks against the US, it can also fire digital reprisals automatically!



Flame / sKyWIper – 2011/2012 (post Stuxnet)

'FLAME' WARS HOW ESPIONAGE WENT VIRAL

The Flame virus has been dubbed the world's most sophisticated piece of malware. How does it work?

1 Infection begins with a computer in a high-security network. How it gets there is unknown; the virus could be delivered by USB stick, via an email or through an internet hack attack.



CONTROL AND COMMAND

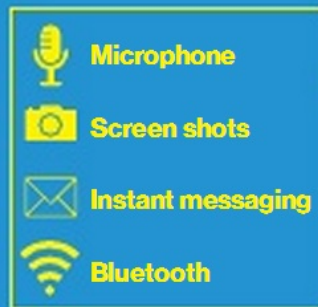


2 Virus scans for other networks and accounts to infect. Rather than being virulent, it carefully chooses its targets and communicates with 'control and command' for advice.



Hidden servers are used by cyber attackers to talk with virus and access the data.

3 Flame is masterful in sweeping for data, listening in to microphones, monitoring instant messenger chats, taking screen shots and hacking connected Bluetooth devices.



DROPBOX



4 Gathered information is broken down into small pieces and smuggled out in normal network traffic. It is reassembled and placed in a 'drop box' on the internet.

GRAPHIC: JOHN BRADLEY

COUNTRIES INVOLVED

IRAN

The country with the largest number of infections, though they have also been found in Sudan, Syria, Lebanon and Egypt. President Mahmoud Ahmadinejad (right) has warned of the dangerous new threat.

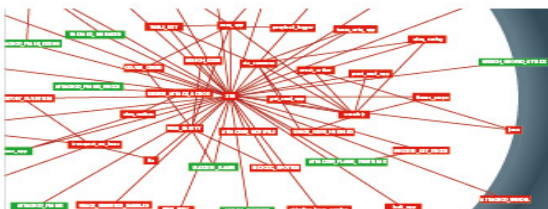


ISRAEL

The government of Benjamin Netanyahu (right) hinted they might be behind the virus, even though computers also infected in Israel.



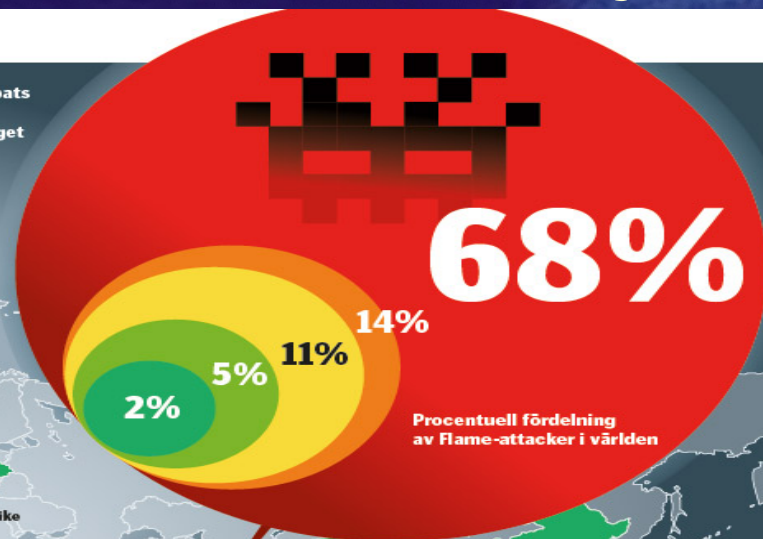
Flame / sKyWIper – Worm / rootkit / trojan



Flame består av många moduler med olika funktioner som angriparn kan lägga till, ta bort eller uppdatera efter behov över nätet.

Antalet datorer i världen som drabbats av Flame uppgår i dag till cirka 10 000, enligt datasekerhetsföretaget Kaspersky.

Trojanen har också upptäckts i Paris och nu i Stockholm.



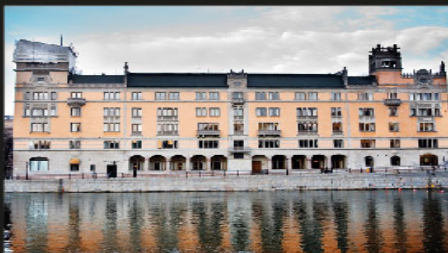
Procentuell fördelning av Flame-attacker i världen

Så kan du skydda dig:

- Uppdatera antivirusprogrammen så ofta som möjligt.
- Installera programfixar för Windows som Microsoft släpper ut.

- Analysera trafiken från arbetsplatsen nattetid. Isolera viktiga datorer från det interna nätverket.
- Använd inte usb-minnen på jobbdatorn.

Målen för Flame



Spionera på politiska beslutsfattare och regeringstjänstemän.

Foto Jörgen Appelgran



Samla information om landets försvarssystem.

Foto Scanpix



Leta och kartlägga sårbarheter i system för att skaffa sig förmåga att angripa samhällsviktig infrastruktur.

Foto Scanpix



Bedriva klassiskt industrispionage i syfte att skaffa underättelseinformation om företag inom high-tech.

Foto Scanpix

Källa: Kaspersky Lab
Grafik: Jonas Åskergrén/Anders Vikhult

- Wiki: [http://en.wikipedia.org/wiki/Flame_\(malware\)](http://en.wikipedia.org/wiki/Flame_(malware))
- Technical paper: <http://www.crysys.hu/skywiper/skywiper.pdf>

CPU/GPU development

Google for



<https://www.google.se/search?q=286755fad04869ca523320acce0dc6a4>



TEGRA X1 MOBILE SUPERCHIP

256-core Maxwell GPU | 8-core 64-bit CPU | 4Kp60 10-bit H.265/VP9

2013 – 25 GPU cards at 2-3 TeraFlop each, clustered together with software as Virtual OpenCL can achieve around 350 billion-guess-per-second speed

2017 – GPU cards are now at 8 - 10 TF

2015 – 1 TeraFlop at 10 W

2000 – 1 TeraFlop needed a super computer with 10 000 CPUs consuming 1 MW



The internet of things

THE INTERNET OF THINGS

AN EXPLOSION OF CONNECTED POSSIBILITY

THE INTERNET OF EVERYTHING IS HERE.
As the Internet evolves, so will we.

37 billion new things will be connected by 2020.

MoE #TomorrowStartsHere

CISCO

Today, there are twice as many things connected to the Internet as human beings on the planet.

2012
8.7 BILLION

Just three years old and the U.S. National Intelligence Council has recognized IoT on their list of the six most "disruptive" technologies — with impacts that will last through 2025.

2009
IoT INCEPTION

CISCO estimates the IoT was born sometime in 2008-2009.

2003
0.5 BILLION

A 43,000% increase in connected devices in just 12 years.

1992
1,000,000

About the equivalent of the population of San Jose.

2014
14.4 BILLION



2016
22.9 BILLION

Sensors that are already emerging will become more prevalent — traffic light cameras, parking spot sensors, entertainment facilities and smart utility meters are all sharing to other machines via broadband.



2015
18.2 BILLION



2017
28.4 BILLION



2018
34.8 BILLION



2019
42.1 BILLION



2020
50.1 BILLION

Taking population predictions into account, there will be about 6.6 devices per human on the planet.



HACKERS AHEAD

BILLIONS OF DEVICES

YEAR

ICS and SCADA systems



SCADA is used around the world to control all kinds of industrial processes — SCADA can help you increase efficiency, lower costs and increase the profitability of your operations.

SCADA (Supervisory Control and Data Acquisition) is not a specific technology, but a type of application. Any application that gets data about a system in order to control that system is a SCADA application.

Many old ICS (Industrial Control Systems) are now connected to internet.

<http://www.dpstelecom.com/white-papers/scada/offer.php>

SHODAN

<https://www.shodan.io/>

Like living on the edge? Try out the beta website for Shodan.

Shodan Exploits Scanhub Maps Blog Membership Register Login

SHODAN Search

EXPOSE ONLINE DEVICES.

WEBCAMS. ROUTERS.
POWER PLANTS. IPHONES. WIND TURBINES.
REFRIGERATORS. VOIP PHONES.

[TAKE A TOUR](#) [FREE SIGN UP](#)

Popular Search Queries:



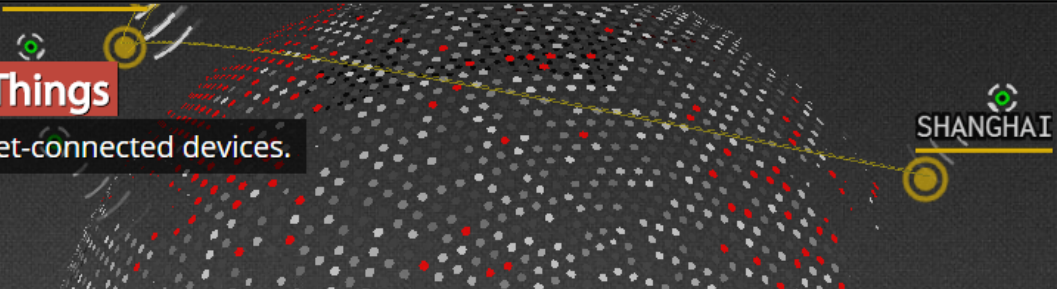
Shodan Scanhub Developers View All...

SHODAN Explore Contact Us Blog New to Shodan? [Login or Register](#)

The search engine for the Internet of Things

Shodan is the world's first search engine for Internet-connected devices.

[Create a Free Account](#) [Getting Started](#)



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

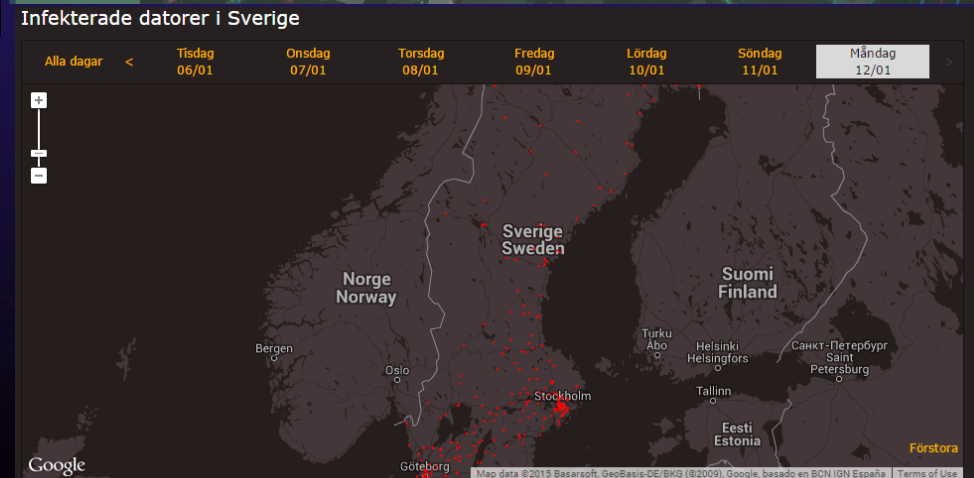
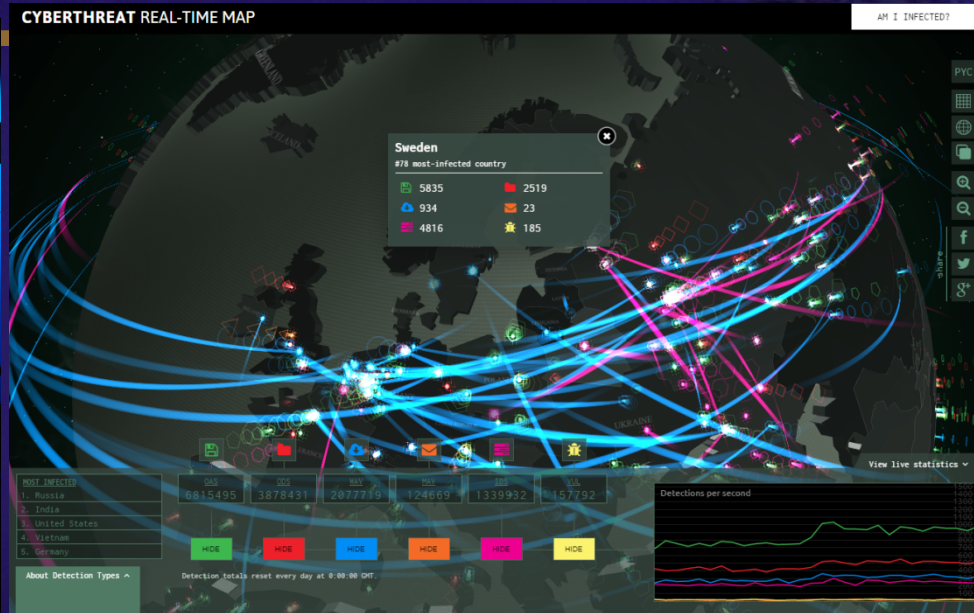
Cyber threat real-time maps



<http://worldmap3.f-secure.com/>

<http://cybermap.kaspersky.com/>

<https://cert.se/megamap/>



Städer	Organisationstyper				
Stad	IP-adresser	Träffar	Organisationstyp	IP-adresser	Träffar
Stockholm	3244	18407	Webbhotell	11626	66485
Göteborg	1669	7301	ISP	9152	56882

WiFi Drones and Virtual Assistants



Parrot AR.Drone 2.0 GPS Edition Quadricopter

- Record HD Movies
- Return Home Mode
- €300

Network attacks/id-collect/surveillance

- Ukraine Maidan protests - SMS
- Hong Kong umbrella protests

<https://www.youtube.com/user/ARdrone>
<http://www.parrot.com/>

Virtual Assistant Jeopardy

See how four digital helpers performed when asked trivia from the official 'Jeopardy' practice test:



Virtual Assistant (Score out of 20)	Alexa (5)	Siri (17)	Cortana (16)	Google Now (16)
"What is atomic number 98?"	Says: "Hmmm, I can't find the answer to the question I heard."	Shows a periodic table illustration of Californium.	Bing search results include Californium Wikipedia entry, if you scroll down a screen. No point scored.	Says: "...Californium is a radioactive metallic chemical element with symbol Cf and atomic number 98."
"What was the name of Mozart's last symphony?"	Gives the wrong answer: "Symphony No. 49 in D Major."	Shows search results, the first of which is "Mozart's Last Symphony: The Giant 'Jupiter.'"	Shows search results, the first of which is "Mozart's Last Symphony: The Giant 'Jupiter.'"	Says: "...the work is nicknamed the Jupiter Symphony."
"Who played Daisy in the movie 'The Curious Case of Benjamin Button'?"	Says: "Benjamin Button's actors are Brad Pitt and Cate Blanchett."	Says: "The Curious Case of Benjamin Button' stars Brad Pitt, Cate Blanchett and Taraji Henson."	Bing search results includes Cate Blanchett link...way way down the list. No point scored.	Says: "...Cate Blanchett, who plays Daisy, Benjamin's great love."

NSA - Edward Snowden



- Movies: Citizenfour (2014) and Snowden (2016)
- ES warns about loss of privacy in Christmas message
- <http://www.theguardian.com/world/video/2013/dec/25/edward-snowden-christmas-message-video>
- ES Hong Kong interview part 1 and 2
- <http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>
- <http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video>



What is This Course About?

- Learn how attacks are performed
- Learn how to prevent attacks and/or limit their consequences
 - No silver bullet; man-made complex systems will have errors; errors may be exploited
 - Large number of ways to attack
 - Large collection of specific methods for specific purposes
- Learn to think about security when doing things
- Learn to understand and apply security principles



Required skills and other practical stuff

- This is a practical course!
 - Windows or any OS which supports Virtual Machines
 - Basic Linux
 - Network technology
 - Basic crypto
 - Programming (C/C++, C#/Java or JS/PHP/Python/Perl)
- You need (beside 20h work per week)
 - Vmware/VirtualBox or/and USB-media
 - Kali Linux (32 bit version is the safe bet for labs!)
 - Disk space – virtual OS images
 - Network environment with at least two devices on the network
 - Wireless access point



Course contents I

- Introduction to Ethical Hacking
- Overview of network and operating systems
- Foot printing or reconnaissance
- Scanning
- Enumeration and information gathering
- Accelerated hash/crypto attacks with OpenCL (parallel prog.)
- Wireless networks attacks
- Exploits as buffer overflows
- Metasploit Framework and modules
- Web application vulnerabilities
- SQL-injection



Course contents II

- Denial of Service (DoS) attacks
- Network attacks as spoofing, sniffing and session hijacking
- Malware - rootkits, trojans and backdoors
- Covert channels
- Viruses and worms
- Vulnerability scan and analysis
- Secure communication
- Other area not decided yet? (renew the course)
- Static and dynamic file analysis
- Pen-test methods and frameworks/standards?
- Note! Changes may occur during the course!



Goals and grade (see English syllabus)

- Efter genomgången kurs ska de studerande kunna
 - redogöra för de grundläggande principerna och teknikerna om hur attackerare kan ta sig in i datasystem.
 - tillämpa förvärvat kunskap praktiskt genom att utföra etiska penetrationstester (pen-test) och dölja intrång
 - utföra analys av dataintrång och granskningar av informationstekniska säkerhetsrisker
 - bedöma olika informationstekniska lösningars styrkor och svagheter vad gäller datasäkerhet
 - självständigt presentera och utföra demonstrationer av pen-test i undervisande syfte
 - värdera hacknings samhällseliga roll utifrån såväl ett socialt, etiskt som ekonomiskt perspektiv.
- Grade (U - VG)
 - Labs is worth 4,5 hp
 - Own project for examination seminar is worth 3 hp

Lab 1

■ Kali Linux

- Create persistent pen-test USB memory stick (optional)
- Most (> 90%) of the course may be done in a virtual environment (recommended) as VMware or VirtualBox

■ Get used to the lab environment

■ GNU/Linux

■ Extra

- Wireshark



Lab 2

- Information gathering
 - DNS, SNMP and SMTP
- Scanning and IP filter determination
- Break password hashes or crypto
 - Rainbow tables and parallel computing intro
- Extra
 - Netbios information gathering



Lab 3 and lab 4

- 3. Wireless attacks and parallel crypto attacks
 - Analyze packet captures
 - Vulnerability scanning
 - Nessus, Nikto2, Wikto
- 4. Application attacks
 - Simple buffer misuse (bad programming)
 - Buffer overflows (stack based)
 - Metasploit Framework
 - Metasploit module
 - Extra, more buffer overflow



Lab 5 and lab 6

- 5. Web application and network attacks
 - Web application attacks
 - SQL-injection
 - Secure communication and PKI certificates
 - Network, MITM, sniffing and spoofing attacks
 - Extra, DoS attacks
- 6. Malicious code/malware attacks and backdoors
 - Process analysis training
 - Rootkits, malicious code and covert channels
 - Static and dynamic analysis of binary files
 - Extra, patch and rootkit scanning, simulators and trojans



Own project work – can be started anytime

- Performed in solo (1 person) – deep dive into a subject
- Finished with a presentation / live demo of the performed work where the class and teachers are grading the performance
 - Report = lab/manual exercise (see example Windows Vista Security)
- Example of suitable subjects
 - Ethical hacking and the legal system
 - Pen-test methods and standards
 - Forensics (hacked computer), smart phone pen-tests, etc. new stuff...
 - Automated pen-testing - Remote advanced exploits
 - Reverse engineering - Virus - Malware - Rootkits
 - Kali Linux, there are *many* programs...
 - Vulnerable systems: DVL, pentesterlab.com, webgoat, metasploitable etc.
 - Your own proposal – must be approved!
 - See earlier work on [server]\pen-test\projects

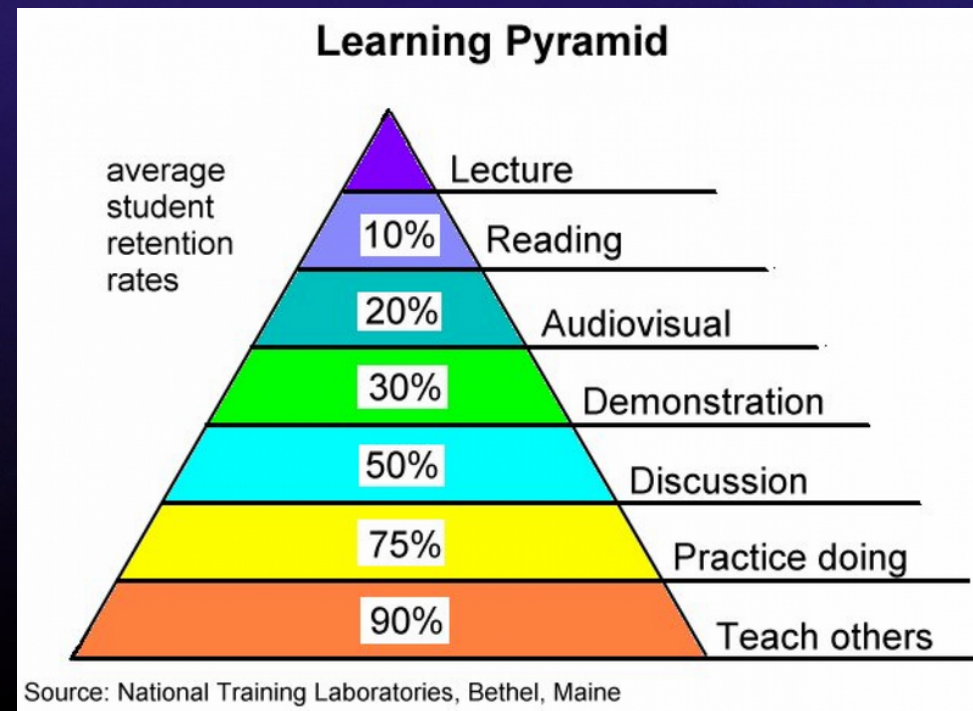
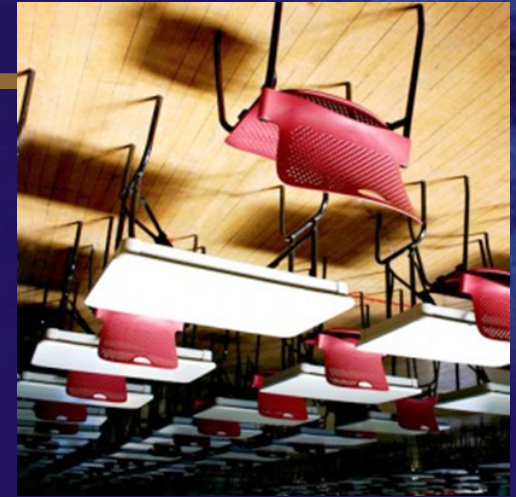


Preliminary schedule

- Around: 13-14 recorded lectures in Adobe Presenter format
- Three Adobe Connect sessions every week
- Practical advice!
 - Read labinstruktion.pdf
 - Browse thru the lab before you begin
 - Make sure to be in sync with the course!
 - Every lab have a "best before date"
 - All handins in Fronter are done in one compressed file
- The examination seminary project is reported during week 12
- See the studiehandledning document in Fronter for more info

Flipped classroom

- Recorded lectures and seminars (in our case labs) replace the traditional lectures
- Active learning
 - Engage the student
 - Student responsibility
 - Not only listen and read
- Relieve the teachers
 - Increase time and efficiency
 - Student discussion (and peer review) is desirable
 - Students can do labs in pair, but hand in is individual

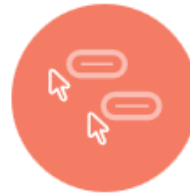


Screenhero

- Remote pair programming
 - Screenhero gives you low-lag screen sharing, multiple mouse cursors, and voice chat.
 - You each get your own mouse cursor, and you're both always in control.
 - It works with your favorite IDE, text editor, or app.
- To begin using Screenhero get an invite from the teachers
- <https://screenhero.com/>

Screenhero features

Screenhero is specifically tailored for effortless real-time collaboration



Multiple mouse cursors

You both have your own mouse cursor. Now both sides can switch seamlessly between driving and navigating, with zero cognitive overhead.

Voice chat

Effective collaboration requires being able to speak with your collaborator while you work together. Screenhero provides crisp, 48kHz audio with echo cancellation.



Lightning fast screen sharing

Screenhero provides the lowest latency screen sharing on the market, even at full resolutions. You feel like you are working at the same desk.

Cross platform

Screenhero is cross-platform, which means you can share between Mac and Windows (and any other future platforms). On Mac, we support: Mac OSX 10.8+, 10.9+. On Windows, we support: Windows 7



Slack

<https://slack.com/> > Sign in > Teamdomain (digitalbrott-du)
To begin using Screenhero and Slack get an invite from the teachers

The screenshot shows the Slack desktop application window titled "Digitalbrott och eSakerhet - Slack". The interface is in dark mode. On the left sidebar, the "Digitalbrott och ..." workspace is selected. Under "CHANNELS", the channel "#dt1062-utv_mob" is highlighted. Below it are "# general" and "# random", and a "Create a channel..." option. Under "DIRECT MESSAGES", "slackbot" is listed with a notification badge. Under "PRIVATE GROUPS", there is a "New private group..." option. At the bottom of the sidebar, it says "There's no one here yet" and "+ Invite People". The main content area shows the channel header "#dt1062-utv_mob" with 1 member. Below the header is a message from "hjo" at 12:34 PM stating "joined #dt1062-utv_mob". At the bottom, there is a text input field with a plus icon on the left and a search icon on the right.

The screenshot shows the Slack mobile application interface. At the top, the status bar shows the time as 14:18 and 77% battery. The app header shows the workspace name "Digitalbrott och..." and a search icon. Below the header is a navigation bar with icons for home, messages, mentions, and stars. A search bar labeled "Jump to..." is visible. The main content area shows a notification for "UNREAD" from "@slackbot" with a notification badge. Below the notification, the "CHANNELS" list is visible, including "# dt1062_utv_mob", "# general", and "# random". At the bottom right, there is a prominent red circular button with a white plus sign.

<https://digitalbrott-du.slack.com/>

Literature 1 (2006)

Updated Edition of the Best-Seller!

The Radia Perlman Series in Computer Networking and Security

PRENTICE
HALL

COUNTER HACK RELOADED

A Step-by-Step Guide to
Computer Attacks and Effective Defenses



Ed Skoudis with Tom Liston

Second Edition

PRENTICE HALL SERIES IN COMPUTER NETWORKING AND DISTRIBUTED SYSTEMS

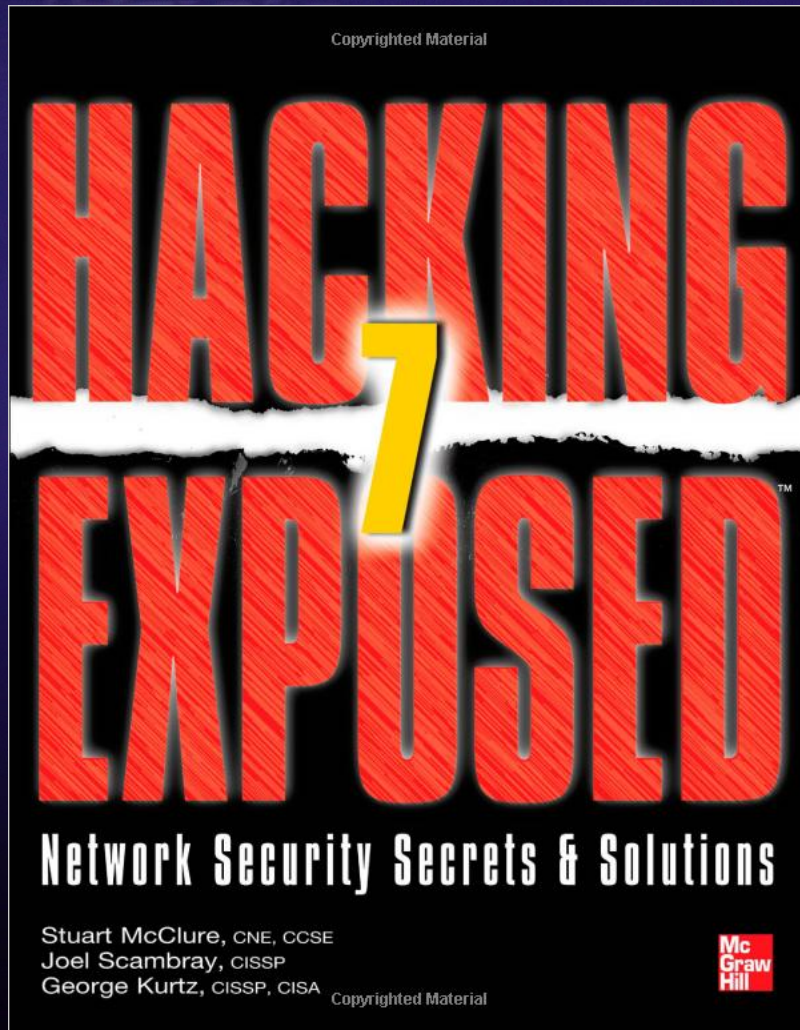
MALWARE Fighting Malicious Code



Ed Skoudis
With Lenny Zeltser

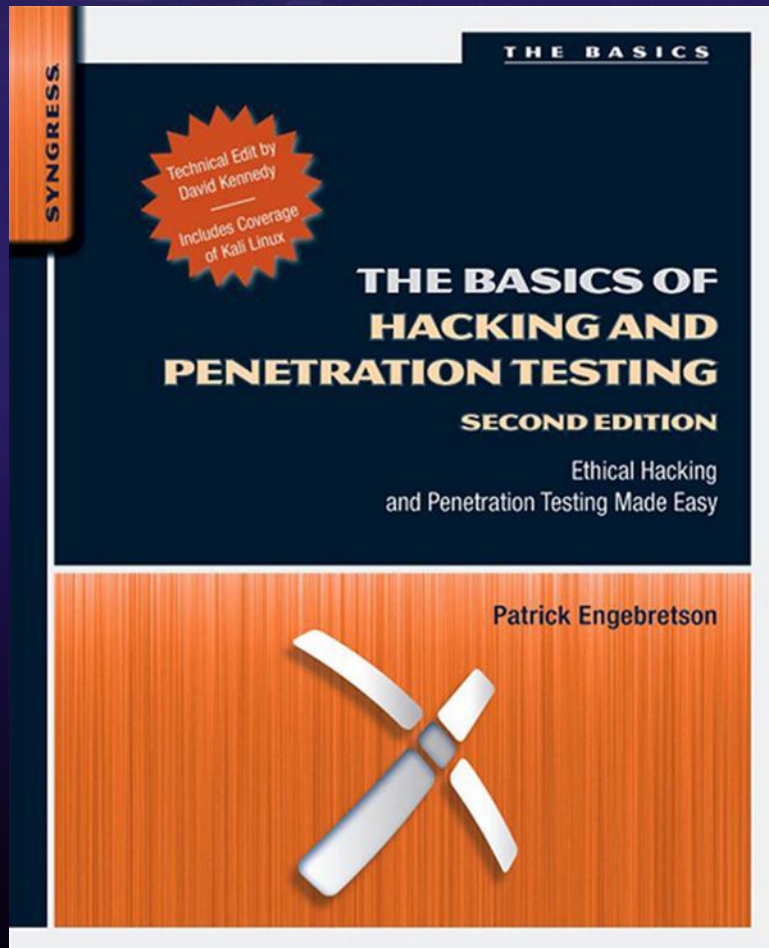
- ISBN-10: 0121631044
- <http://www.counterhack.net>

Literature 2 (2012)



- 3 types of books identified
 - Theoretical
 - In between
 - Practical
- Well reviewed book
- Dictionary for hacking (practical)
- ISBN-10: 0071613749
- <http://www.hackingexposed7.com/>

Literature 3 (2013) rev 2



- Short, cheap and new intro to pen-test
 - In between
- Well reviewed book
- Hands on examples
- Uses Kali tools
- ISBN-10: 0124116442

E-material etc.

- Additional books and magazines

- Valuable for the individual project

- Fronter links

- How to be a CEH (Certified Ethical

Hacker) http://www.ethicalhacker.net/component/option,com_smf/Itemid,54/topic,2114.msg8727/#msg8727

- Tools, papers etc.

- Labs

- \\projects\digitalbrott

- <http://users.du.se/~hjo/cs/>

- Blogs and security related web sites

- ...



<http://hakin9.org/>



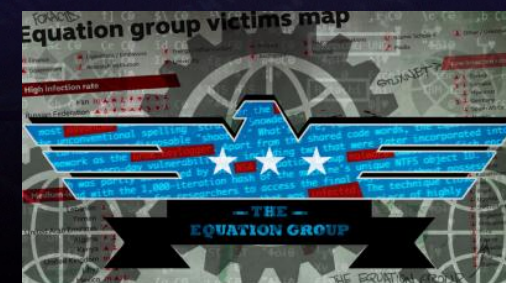
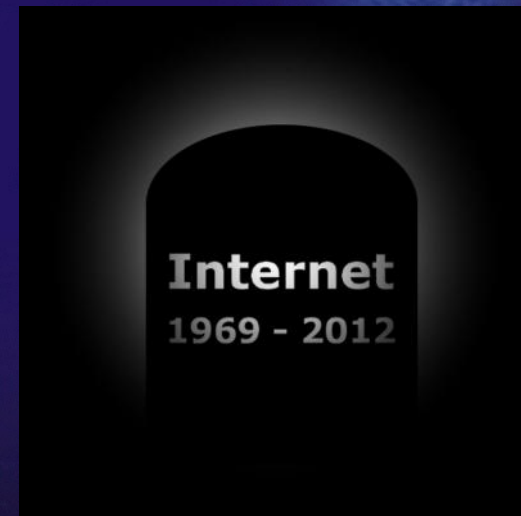
Virtuella Maskiner och OS

- I kursen behöver man använda en eller flera virtuella maskiner
 - En virtuell maskin är en emulation av ett datasystem
 - Via en programvara som körs i en fysisk maskin kan mjukvara och hårdvara emuleras
- Det finns färdiga maskiner ("virtual appliance") att ladda hem som tex. Kali Linux
- Skapa egna genom att ladda ner OS via DreamSpark Premium
 - http://wiki.du.se/%C3%84mnen_-_Subjects/Datateknik_-_Computer_Engineering/Distance_access_to_software
- Hämta VMware Workstation Player (Windows och Linux) från DreamSpark ovan eller: <https://www.vmware.com/> > Downloads > Workstation Player
- VirtualBox från: <https://www.virtualbox.org/>

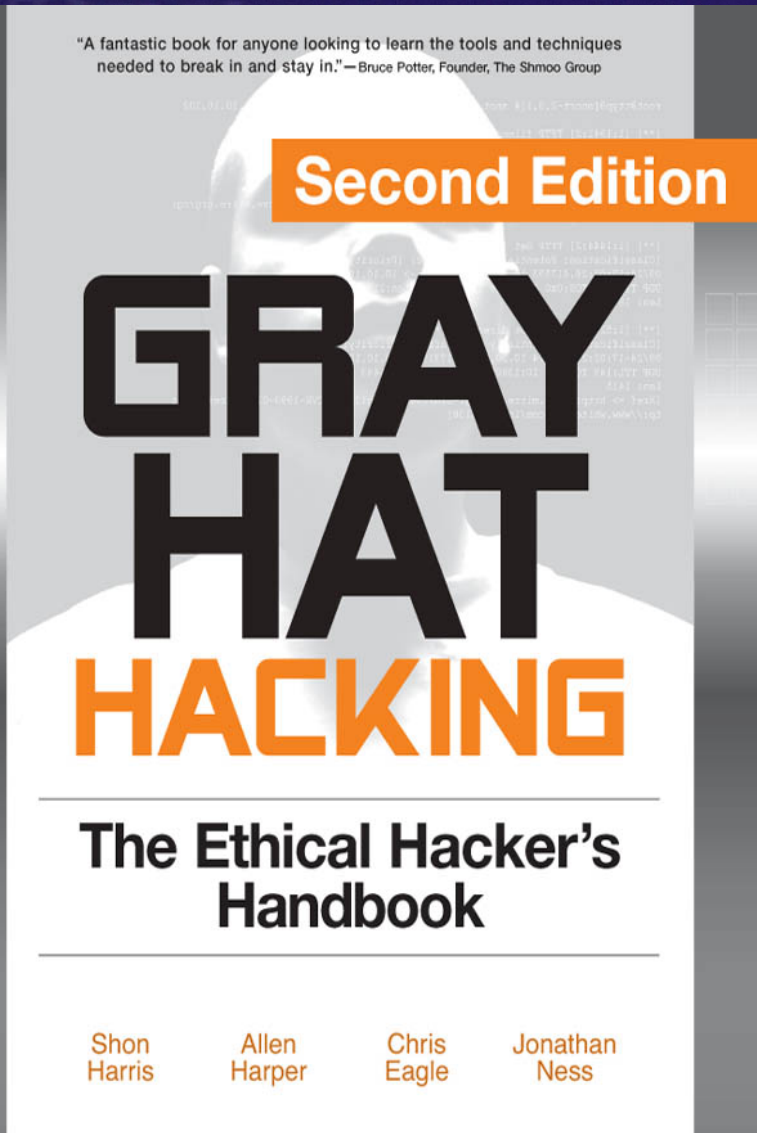


Interesting links and resources

- DN granskar: Det sårbara digitala samhället
 - <http://www.dn.se/stories/dn-granskar-det-sarbara-digitala-samhallet/>
- Brottsförebyggande rådets prel. statistik för 2014 visar att datorbedrägerier ökar kraftigt
 - <http://www.bra.se/bra/brott-och-statistik/statistik/anmalda-brott.html>
- Säkerhetsexperten Mikko Hypponen, F-Secure
 - <http://www.npr.org/2014/01/31/265386281/why-should-you-be-worried-about-nsa-surveillance>
 - R.I.P. Internet: <https://www.youtube.com/watch?v=u93kdtAUn7g>
- Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance
 - <https://freedom.press/encryption-works>
- The “Equation Group” is probably the most sophisticated computer attack group in the world, with almost superhuman technical skills and unlimited resources
 - <http://arstechnica.com/security/2015/02/how-omnipotent-hackers-tied-to-the-nsa-hid-for-14-years-and-were-found-at-last/>

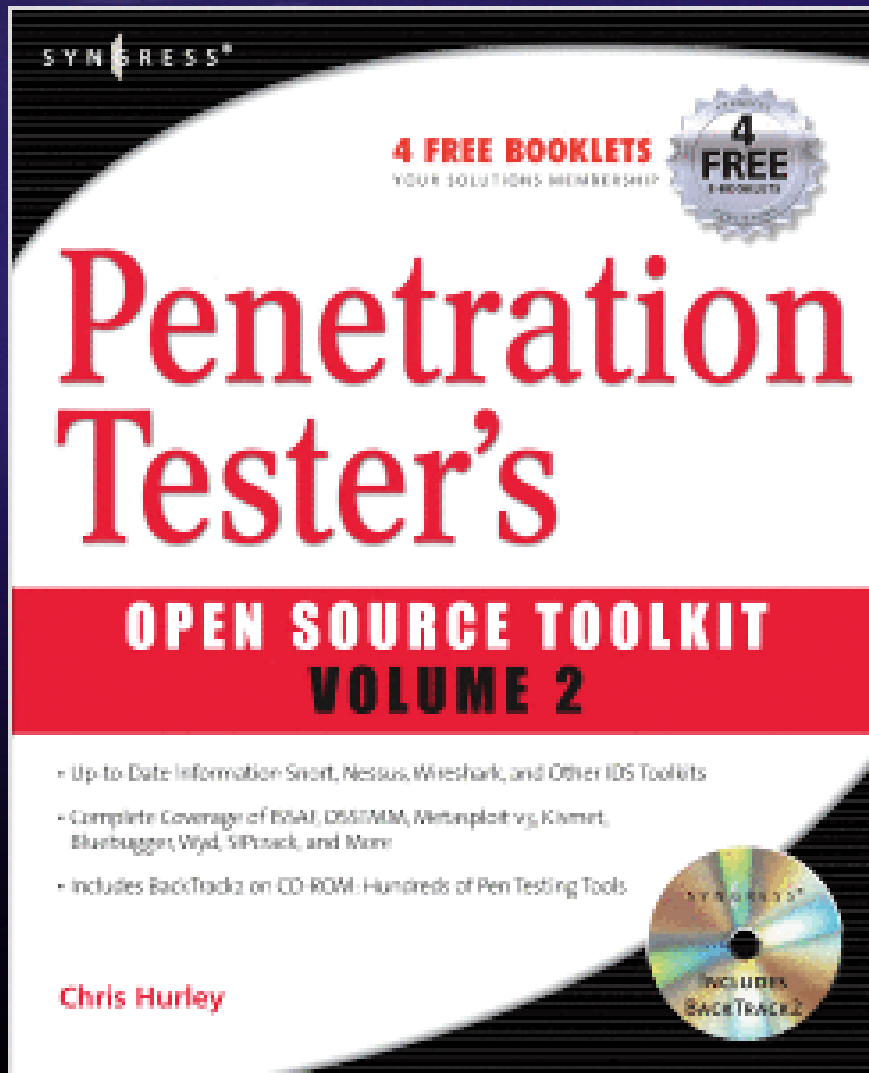


Literature beyond "Hacking Exposed" etc.



- 2008
- ISBN-10: 0071495681
- <http://www.grayhathackingbook.com/>

Literature, very practical



■ 2008

■ ISBN-10: 1597492132

Literature - web application

The Web Application Hacker's Handbook

Finding and Exploiting
Security Flaws

2

Second
Edition



■ Dafydd Stuttard ■ Marcus Pinto

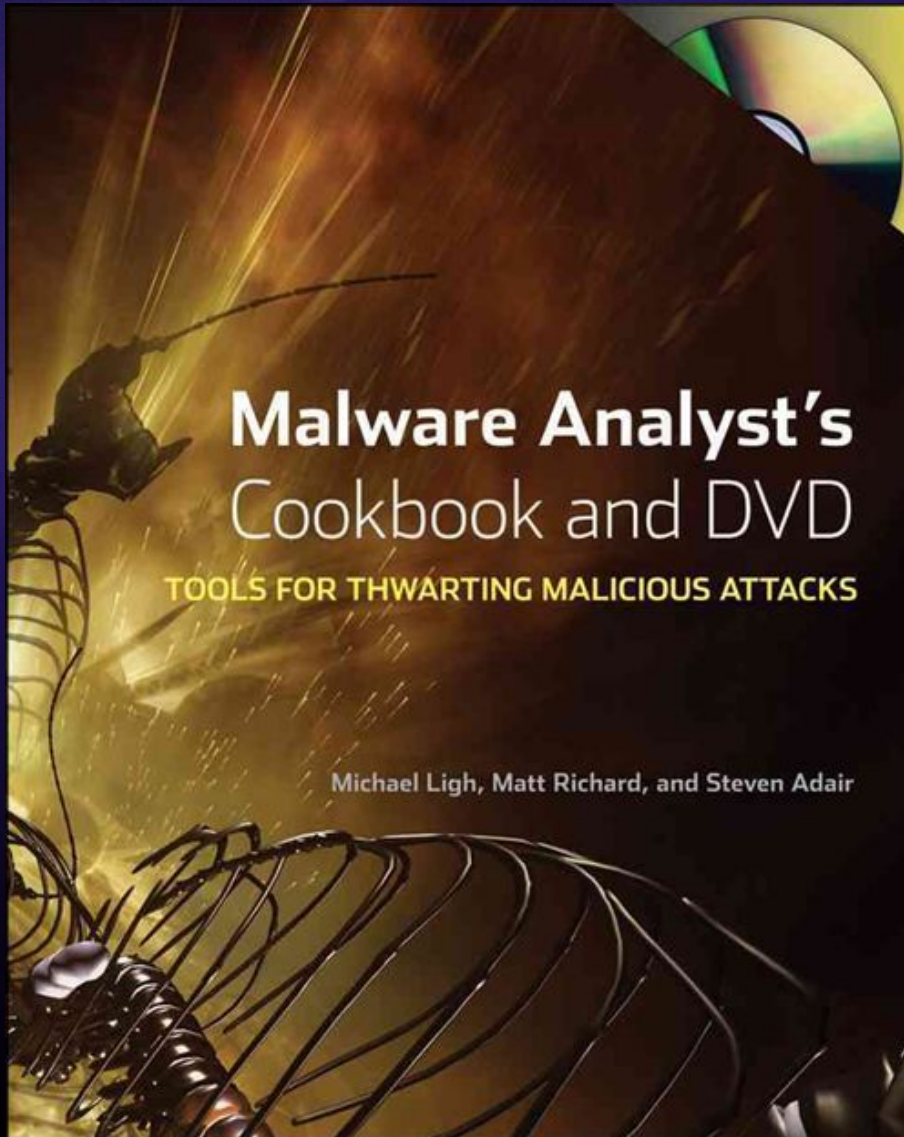
Best book for web security!

Late 2011

ISBN: 1118026470 / 978-
1118026472

<http://portswigger.net/wahh/>

Literature - Malware



The best!

DVD on digitalbrott share

Password - infected

ISBN: 0470613033 / 978-
0470613030

<http://www.malwarecookbook.com/>

MASTER THE PROFESSIONAL HACKER'S PYTHON TOOLKIT

Grey Hat Python 2009

Python is fast becoming the programming language of choice for hackers, reverse engineers, and software testers because it's easy to write quickly, and it has the low-level support and libraries that make hackers happy. But until now, there has been no real manual on how to use Python for a variety of hacking tasks. You had to dig through forum posts and man pages, endlessly tweaking your own code to get everything working. Not anymore.

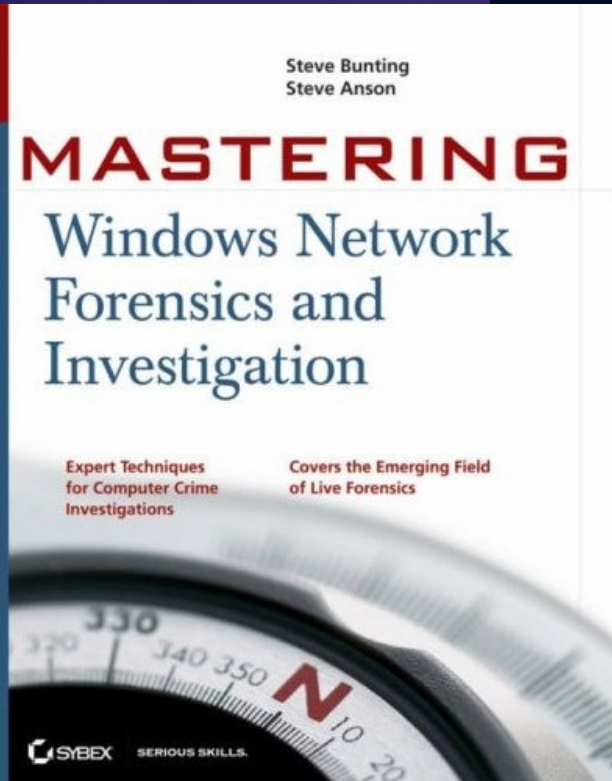
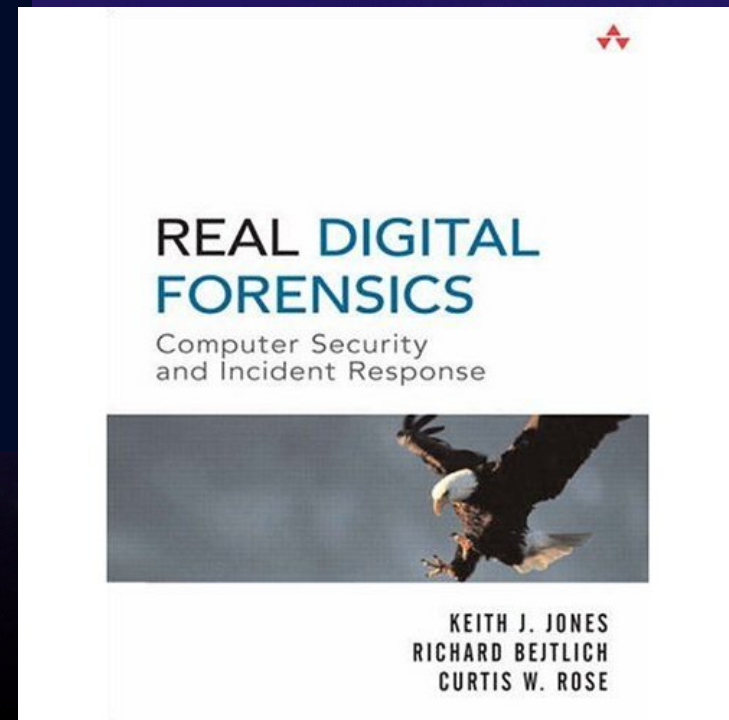
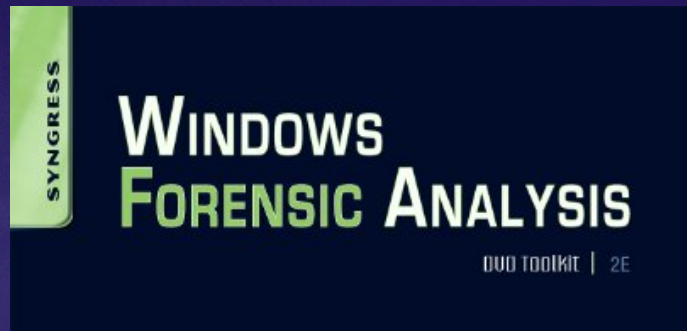
Gray Hat Python explains the concepts behind hacking tools and techniques like debuggers, trojans, fuzzers, and emulators. But author Justin Seitz goes beyond theory, showing you how to harness existing Python-based security tools—and how to build your own when the pre-built ones won't cut it.

You'll learn how to:

- > Automate tedious reversing and security tasks
- > Design and program your own debugger
- > Learn how to fuzz Windows drivers and create powerful fuzzers from scratch
- > Have fun with code and library injection, soft and hard hooking techniques, and other software trickery
- > Sniff secure traffic out of an encrypted web browser session
- > Use PyDBG, Immunity Debugger, Sulley, IDAPython, PyEMU, and more

The world's best hackers are using Python to do their handiwork. Shouldn't you?

Literature, forensic



Literature free

 WILEY

Security Engineering

A Guide to Building
Dependable
Distributed
Systems

Ross Anderson

- Can be downloaded!
- <http://www.cl.cam.ac.uk/~rja14/book.html>

More literature...

