Making Everything Easier!™

3rd Edition

Hacking FOR DUMMIES®

Learn to:

- **Use the latest ethical hacking methods and tools**
- **Test your Windows® or Linux® systems**
- **Hack databases, VoIP systems, and Web applications**
- **Report vulnerabilities and improve information security**

Kevin Beaver, CISSP

Information Security Consultant

Hacking For Dummies *3rd Edition*

Chapter 4 Hacking Methodology

ISBN: 978-0-470-55093-9

WILEY

Chapter 4
Hacking Methodology

In This Chapter

- Examining steps for successful ethical hacking
- Gleaning information about your organization from the Internet
- Scanning your network
- Looking for vulnerabilities

Before you dive in head first with your ethical hacking, it's critical to have at least a basic methodology to work from. Ethical hacking involves more than just penetrating and patching a system or network. Proven techniques can help guide you along the hacking highway and ensure that you end up at the right destination. Using a methodology that supports your ethical hacking goals separates the professionals from the amateurs and helps ensure that you make the most of your time and effort.

Setting the Stage for Testing

In the past a lot of ethical hacking involved manual processes. Now, tools can automate various tasks. These tools allow you to focus on performing the tests and less on the specific steps involved. However, following a general methodology and understanding what's going on behind the scenes will help you.

Ethical hacking is similar to beta testing software. Think logically — like a programmer, a radiologist, or a home inspector — to dissect and interact with all the system components to see how they work. You gather information, often in many small pieces, and assemble the pieces of the puzzle. You start at point A with several goals in mind, run your tests (repeating many steps along the way), and move closer until you discover security vulnerabilities at point B.

The process used for ethical hacking is basically the same as the one a malicious attacker would use — the primary differences lie in the goals and how you achieve them. Another key difference is that you, as an ethical hacker, will eventually attempt to assess *all* your information systems for vulnerabilities and properly address them, rather than run a single exploit or attack a small number of systems. Today's attacks can come from any angle against any system, not just from the perimeter of your network and the Internet as you might have been taught in the past. Test every possible entry point, including partner, vendor, and client networks, as well as home users, wireless LANs, and laptop computers. Any human being, computer system, or physical component that protects your computer systems — both inside and outside your buildings — is fair game.

TIP

When you start rolling with your ethical hacking, keep a log of the tests you perform, the tools you use, the systems you test, and your results. This information can help you do the following:

- Track what worked in previous tests and why.
- Help prove that you didn't maliciously hack the systems.
- Correlate your testing with intrusion detection systems and other log files if trouble or questions arise.
- Document your final report.

TIP

In addition to taking general notes, taking screen captures of your results whenever possible is also helpful. These shots come in handy later should you need to show proof of what occurred, and they also will be useful as you generate your final report. Also, depending on the tools you use, these screen captures might be your only evidence of vulnerabilities or exploits when it comes time to write your final report. Chapter 3 lists the general steps involved in creating and documenting an ethical hacking plan.

Your main task is to simulate the information gathering and system compromises carried out by someone with malicious intent. This task can be a partial attack on one computer or it can constitute a comprehensive attack against the entire network. Generally, you look for weaknesses that malicious users and external attackers might exploit. You want to assess internal systems (processes and procedures that involve computers, networks, people, and physical infrastructures). Look for vulnerabilities; check how all your systems interconnect and how private systems and information are (or aren't) protected from untrusted elements.

These steps don't include specific information on the low-tech hacking methods that you use for social engineering and assessing physical security, but the techniques are basically the same. I cover these methods in more detail in Chapters 5 and 6.

TIP

If you're performing ethical hacking for a client, you may go the blind assessment route and start with just the company name and no other information. This blind assessment approach allows you to start from the ground up and gives you a better sense of the information and systems that malicious attackers can access publicly. However, keep in mind that this way of testing can take longer, and you may have an increased chance of missing some security vulnerabilities.

As an ethical hacker, you might not have to worry about covering your tracks or evading intrusion detection systems because everything you do is legitimate. But you might want to test systems stealthily. I discuss techniques that hackers use to conceal their actions in this book and outline some countermeasures for them, as well.

Seeing What Others See

Getting an outside look can turn up a ton of information about your organization and systems that others can see, through a process often called *footprinting.* Here's how to gather the information:

- Use a Web browser to search for information about your organization. Search engines, such as Google and Bing, are great places to start.
- Run network scans, probe open ports, and assess vulnerabilities to determine specific information about your systems. As an insider, you can use port scanners and Windows share-finder tools, such as GFI LANguard, to see what's accessible.

TIP

Whether you search generally or probe more technically, limit the amount of information you gather based on what's reasonable for you. You might spend an hour, a day, or a week gathering this information — how much time you spend depends on the size of the organization and the complexity of its information systems.

Gathering public information

The amount of information you can gather about an organization's business and information systems is staggering and widely available on the Internet. Your job is to find out what's out there. This information allows malicious attackers and employees to target specific areas of the organization, including departments and key individuals.

The following techniques can be used to gather information about your organization.

Web search

Performing a Web search or simply browsing your organization's Web site can turn up the following information:

- Employee names and contact info
- Important company dates
- Incorporation filings (for private companies)
- SEC filings (for public companies)
- Press releases about moves, organizational changes, and new products
- Mergers and acquisitions
- Patents and trademarks
- Presentations, articles, and Webcasts or Webinars

TIP

Microsoft is making headway into the search arena with Bing (`www.bing.com`). However, my favorite tool (and the favorite of many hackers) is still Google (`www.google.com`). This search engine ferrets out information — from word processing documents to graphics files — on any publicly accessible computer. And it's free. Entire books have been written about using Google, so expect any hacker (ethical or otherwise) to be very well versed on this useful tool. (See Chapter 14 for more about Google hacking.)

With Google, you can search the Internet in several ways:

- **By typing keywords:** This kind of search often reveals hundreds and sometimes millions of pages of information — such as files, phone numbers, and addresses — that you never guessed were available.
- **By performing advanced Web searches:** Google's advanced search options can find sites that link back to your company's Web site. This type of search often reveals a lot of information about partners, vendors, clients, and other affiliations.
- **By using switches to dig deeper into a Web site:** For example, if you want to find a certain word or file on your Web site, simply enter a line like one of the following into Google:

  ```
  site:www.your_domain.com keyword
  site:www.your_domain.com filename
  ```

You can even do a generic filetype search across the entire Internet to see what turns up, such as:

```
filetype:swf company_name
```

Use this search for Flash .swf files, which can be downloaded and decompiled to reveal sensitive information that can be used against your business, as I cover in detail in Chapter 14.

```
filetype:pdf company_name confidential
```

Use this search for PDF documents that might contain sensitive information that can be used against your business.

Web crawling

Web-crawling utilities, such as HTTrack Website Copier, can mirror your Web site by downloading every publicly accessible file from it. You can then inspect that copy of the Web site offline, digging into the following:

- The Web site layout and configuration
- Directories and files that might not otherwise be obvious or readily accessible
- The HTML and script source code of Web pages
- Comment fields

Comment fields often contain useful information such as names and e-mail addresses of the developers and internal IT personnel, server names, software versions, internal IP addressing schemes, and general comments about how the code works.

Web sites

The following Web sites may provide specific information about an organization and its employees:

- Government and business Web sites:
    - www.hoovers.com and http://finance.yahoo.com give detailed information about public companies.
    - www.sec.gov/edgar.shtml shows SEC filings of public companies.
    - www.uspto.gov offers patent and trademark registrations.
    - The Web site for your state's Secretary of State or similar organization can offer incorporation and corporate officer information.
- Background checks and other personal information:
    - ChoicePoint (www.choicepoint.com)
    - USSearch (www.ussearch.com)
    - ZabaSearch (www.zabasearch.com)

Mapping the network

When you map your network, you can search public databases and resources to see what other people know about your network.

Whois

The best starting point is to perform a Whois lookup by using any one of the Whois tools available on the Internet. You may have used Whois to check whether a particular Internet domain name is available.

For ethical hacking, Whois provides the following information that can give a hacker a leg up to start a social engineering attack or to scan a network:

- Internet domain name registration information, such as contact names, phone numbers, and mailing addresses
- DNS servers responsible for your domain

You can look up Whois information at one of the following places:

- Whois.net (`www.whois.net`)
- A domain registrar's site, such as `www.godaddy.com`
- Your ISP's tech support site

My favorite Whois tool is DNSstuff.com (`www.dnsstuff.com`). Although this tool is no longer free and is used to sell many services, it's still a good resource.

You can run DNS queries directly from the site to

- Display general domain-registration information
- Show which host handles e-mail (the Mail Exchanger or MX record) for a domain
- Map the location of specific hosts
- Determine whether the host is listed on certain spam blacklists

A free site you can use for more basic Internet domain queries is `www.dnstools.com`.

The following list shows various lookup sites for other categories:

- **Government:** `www.dotgov.gov`
- **Military:** `www.nic.mil`
- **AfriNIC:** `www.afrinic.net` (emerging Regional Internet Registry for Africa)

- **APNIC:** www.apnic.net (Regional Internet Registry for the Asia Pacific Region)
- **ARIN:** https://ws.arin.net/whois/index.html (Regional Internet Registry for North America, a portion of the Caribbean, and subequatorial Africa)
- **LACNIC:** www.lacnic.net/en (Latin American and Caribbean Internet Addresses Registry)
- **RIPE Network Coordination Centre:** www.db.ripe.net/whois (Europe, Central Asia, African countries north of the equator, and the Middle East)

If you're not sure where to look for a specific country, https://www.arin.net/knowledge/rirs/countries.html has a reference guide.

Google Groups

Google Groups (http://groups.google.com) can reveal surprising public network information. Search for such information as your fully qualified domain names (FQDNs), IP addresses, and usernames. You can search millions of Usenet posts that date back to 1981 for public and often very private information.

You might find some information that you didn't realize was made public, such as the following:

- A tech-support or message board post that divulges too much information about your systems. Many people who post messages like these don't realize that their messages are shared with the world or how long they are kept.
- Confidential company information posted by disgruntled employees or clients.

If you discover that confidential information about your company is posted online, you may be able to get it removed. Check out the Google Groups help page at http://groups.google.com/support for details.

Privacy policies

Check your Web site's privacy policy. A good practice is to let your site's users know what information is collected and how it's being protected, but nothing more.

Make sure that the people who write your privacy policies (often nontechnical lawyers or marketing managers) don't divulge details about your information security infrastructure. Be careful to avoid the example of an Internet start-up businessman who once contacted me about a business opportunity. During the conversation, he bragged about his company's security systems that ensured the privacy of client information (or so he thought). I went to his

Web site to check out his privacy policy. He had posted the brand and model of firewall he was using, along with other technical information about his network. This type of information could certainly be used against him by bad guys. Not a good idea.

Scanning Systems

Active information gathering produces more details about your network and helps you see your systems from an attacker's perspective. For instance, you can

- Use the information provided by your Whois searches to test other closely related IP addresses and hostnames. When you map out and gather information about a network, you see how its systems are laid out. This information includes determining IP addresses, hostnames (typically external but occasionally internal), running protocols, open ports, available shares, and running services and applications.
- Scan internal hosts when and where they are within the scope of your testing. (*Hint:* They really ought to be.) These hosts might not be visible to outsiders (at least you hope they're not), but you absolutely need to test them to see what rogue employees and other insiders can access. A worst-case situation is that the hacker has set up shop on the inside. Just to be safe, examine your internal systems for weaknesses.

TIP

If you're not completely comfortable scanning your systems, consider first using a lab with test systems or a system running virtual machine software, such as VMware Workstation or the open source alternative VirtualBox (`www.virtualbox.org`).

Hosts

Scan and document specific hosts that are accessible from the Internet and your internal network. Start by pinging either specific host names or IP addresses with one of these tools:

- The basic ping utility that's built in to your operating system
- A third-party utility that allows you to ping multiple addresses at the same time, such as SuperScan version 3 (`www.foundstone.com/us/resources/proddesc/superscan3.htm`) and NetScanTools Pro (`www.netscantools.com`) for Windows and fping (`www.fping.com`) for UNIX

The site `www.whatismyip.com` shows how your gateway IP address appears on the Internet. Just browse to that site, and your public IP address (your firewall or router — preferably not your local computer) appears. This information gives you an idea of the outermost IP address that the world sees.

Open ports

Scan for open ports by using network scanning tools:

- Scan network ports with SuperScan or Nmap (`http://nmap.org`). See Chapter 8 for details.
- Listen to network traffic with a network analyzer, such as OmniPeek (`www.wildpackets.com`) and Wireshark (`www.wireshark.com`). I cover this topic in various chapters throughout this book.

Scanning *internally* is easy. Simply connect your PC to the network, load the software, and fire away. Scanning from *outside* your network takes a few more steps, but it can be done. The easiest way to connect and get an "outside-in" perspective is to assign your computer a public IP address and plug that workstation into a switch or hub on the public side of your firewall or router. Physically, the computer is not on the Internet looking in, but this type of connection works just the same as long as it's outside your firewall and router. You can also do this outside-in scan from home or a remote office location.

Determining What's Running on Open Ports

As an ethical hacker, you should glean as much information as possible after scanning your systems. You can often identify the following information:

- Protocols in use, such as IP, IPX, and NetBIOS
- Services running on the hosts, such as e-mail, Web servers, and database applications
- Available remote access services, such as Windows Terminal Services/ Remote Desktop, VNC, and Secure Shell (SSH)
- VPN services, such as PPTP, SSL, and IPSec
- Required authentication for network shares

You can look for the following sampling of open ports (your network-scanning program reports these as accessible or open):

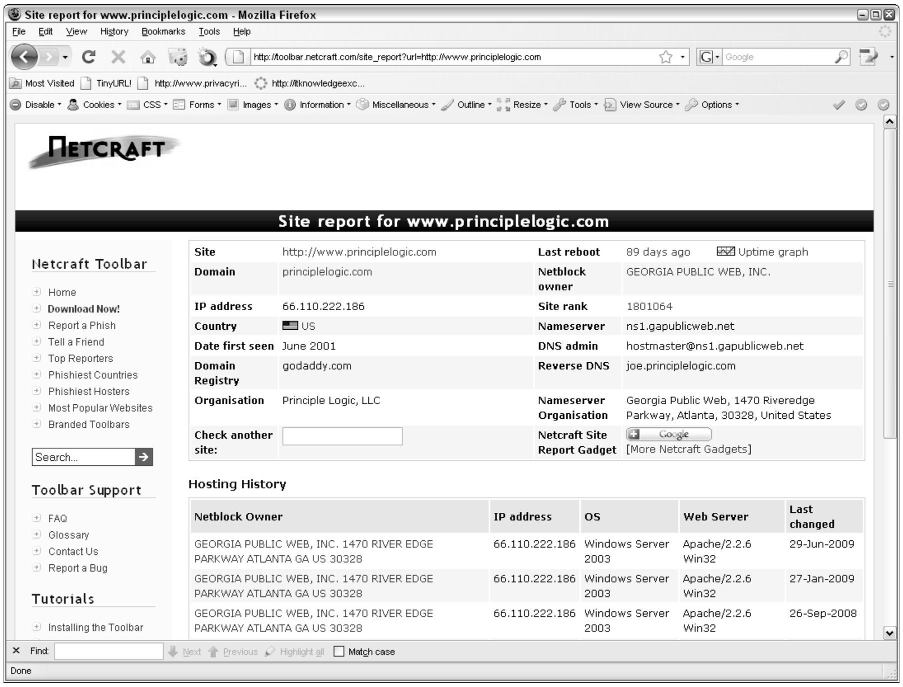
- Ping (ICMP echo) replies; ICMP traffic is allowed to and from the host
- TCP port 21, showing that FTP is running
- TCP port 23, showing that telnet is running
- TCP ports 25 or 465 (SMTP and SMPTS), 110 or 995 (POP3 and POP3S), or 143 or 993 (IMAP and IMAPS), showing that an e-mail server is running

- TCP/UDP port 53, showing that a DNS server is running
- TCP ports 80, 443, and 8080, showing that a Web server or Web proxy server is running
- TCP/UDP ports 135, 137, 138, 139 and, especially, 445, showing that an unprotected Windows host is running

Thousands of ports can be open — 65,536 each for both TCP and UDP, to be exact. I cover many popular port numbers when describing hacks throughout this book. A continually updated listing of all well-known port numbers (ports 0–1023) and registered port numbers (ports 1024–49151), with their associated protocols and services, is located at `www.iana.org/assignments/port-numbers`. You can also perform a port-number lookup at `www.cotse.com/cgi-bin/port.cgi`.

If you detect a Web server running on the system that you test, you can check the software version by using one of the following methods:

- Type the site's name followed by a page that you know doesn't exist, such as *`www.your_domain.com`*`/1234.html`. Many Web servers return an error page showing detailed version information.
- Use Netcraft's *What's that site running?* search utility (`www.netcraft.com`), which connects to your server from the Internet and displays the Web server version and operating system, as shown in Figure 4-1.


Site report for www.principlelogic.com - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://toolbar.netcraft.com/site_report?url=http://www.principlelogic.com
Google
Most Visited TinyURL! http://www.privacyri... http://itknowledgeexc...
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source Options
NETCRAFT
Netcraft Toolbar
Home
Download Now!
Report a Phish
Tell a Friend
Top Reporters
Phishiest Countries
Phishiest Hosters
Most Popular Websites
Branded Toolbars
Search...
Toolbar Support
FAQ
Glossary
Contact Us
Report a Bug
Tutorials
Installing the Toolbar
Find: Next Previous Highlight all
☐ Match case
Done

Site report for www.principlelogic.com

Site	http://www.principlelogic.com	Last reboot	89 days ago Uptime graph
Domain	principlelogic.com	Netblock owner	GEORGIA PUBLIC WEB, INC.
IP address	66.110.222.186	Site rank	1801064
Country	US	Nameserver	ns1.gapublicweb.net
Date first seen	June 2001	DNS admin	hostmaster@ns1.gapublicweb.net
Domain Registry	godaddy.com	Reverse DNS	joe.principlelogic.com
Organisation	Principle Logic, LLC	Nameserver Organisation	Georgia Public Web, 1470 Riveredge Parkway, Atlanta, 30328, United States
Check another site:		Netcraft Site Report Gadget	Google [More Netcraft Gadgets]

Hosting History

Netblock Owner	IP address	OS	Web Server	Last changed
GEORGIA PUBLIC WEB, INC. 1470 RIVER EDGE PARKWAY ATLANTA GA US 30328	66.110.222.186	Windows Server 2003	Apache/2.2.6 Win32	29-Jun-2009
GEORGIA PUBLIC WEB, INC. 1470 RIVER EDGE PARKWAY ATLANTA GA US 30328	66.110.222.186	Windows Server 2003	Apache/2.2.6 Win32	27-Jan-2009
GEORGIA PUBLIC WEB, INC. 1470 RIVER EDGE PARKWAY ATLANTA GA US 30328	66.110.222.186	Windows Server 2003	Apache/2.2.6 Win32	26-Sep-2008

Figure 4-1: Netcraft's Web server version utility.

You can dig deeper for more specific information on your hosts:

- NMapWin (http://sourceforge.net/projects/nmapwin) can determine the system OS version.
- An enumeration utility (such as DumpSec at www.systemtools.com/somarsoft/?somarsoft.com) can extract users, groups, and file and share permissions directly from Windows.
- Many systems return useful banner information when you connect to a service or application running on a port. For example, if you telnet to an e-mail server on port 25 by entering `telnet mail.your_domain.com 25` at a command prompt, you may see something like this:

  ```
  220 mail.your_domain.com ESMTP all_the_version_info_
  you_need_to_hack Ready
  ```

  Most e-mail servers return detailed information, such as the version and the current service pack installed. After you have this information, you (and the bad guys) can determine the vulnerabilities of the system from some of the Web sites listed in the next section.
- A share-finder tool, such as the one built in to GFI LANguard, can find open Windows shares.
- An e-mail to an invalid address might return with detailed e-mail header information. A bounced message often discloses information that can be used against you, including internal IP addresses and software versions. On certain Windows systems, you can use this information to establish unauthenticated connections and sometimes even map drives. I cover these issues in Chapter 13.

Assessing Vulnerabilities

After finding potential security holes, the next step is to confirm whether they are vulnerabilities in your system or network. Before you test, perform some manual searching. You can research hacker message boards, Web sites, and vulnerability databases, such as these:

- Common Vulnerabilities and Exposures (http://cve.mitre.org/cve)
- US-CERT Vulnerability Notes Database (www.kb.cert.org/vuls)
- NIST National Vulnerability Database (http://nvd.nist.gov)

These sites list known vulnerabilities — at least the formally classified ones. As I cover in this book, you see that many other vulnerabilities are more generic in nature and can't easily be classified. If you can't find a vulnerability documented on one of these sites, search the vendor's site. You can also find a list of commonly exploited vulnerabilities at www.sans.org/top20. This site contains the SANS Top 20 Vulnerabilities consensus list, which is compiled and updated by the SANS organization.

If you don't want to research your potential vulnerabilities and can jump right into testing, you have a couple of options:

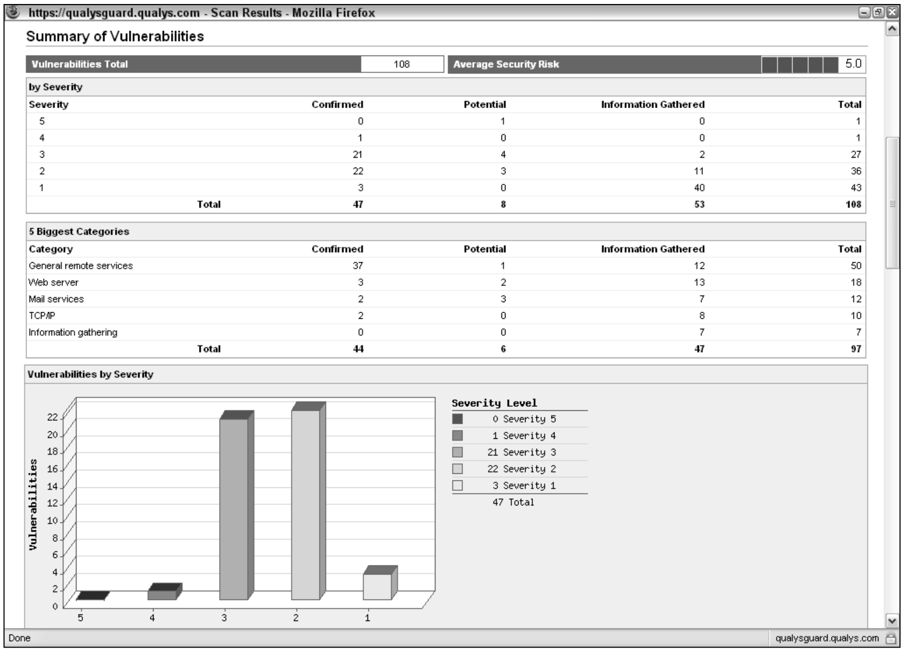
- **Manual assessment:** You can assess the potential vulnerabilities by connecting to the ports that are exposing the service or application and poking around in these ports. You should manually assess certain systems (such as Web applications). The vulnerability reports in the preceding databases often disclose how to do this — at least generally. If you have a lot of free time, performing these tests manually might work for you.
- **Automated assessment:** Manual assessments are a great way to learn, but people usually don't have the time for most manual steps. If you're like me, you scan for vulnerabilities automatically when you can.

Many great vulnerability assessment tools test for vulnerabilities on specific platforms (such as Windows and UNIX) and types of networks (either wired or wireless). They test for specific system vulnerabilities and some even focus on the SANS Top 20 list. Versions of these tools can map the business logic within a Web application; others can help software developers test for code flaws. The drawback to these tools is that they find only individual vulnerabilities; they often don't correlate vulnerabilities across an entire network. However, the advent of event-correlation and vulnerability management applications is allowing these tools to correlate these vulnerabilities.

One of my favorite ethical hacking tools is a vulnerability scanner called QualysGuard Suite by Qualys (`www.qualys.com`). It's both a port scanner and vulnerability assessment tool, and it offers a great deal of help for vulnerability management. You don't even need a computer to run it because QualysGuard is a Software as a Service (SaaS) commercial tool. Just browse to the Qualys Web site, log in to your account, and enter the IP address of the systems you want to test. Qualys also has an appliance that you can install on your network that allows you to scan internal systems. You simply schedule the assessment, and then the system runs tests and generates excellent reports, such as these:

- An executive report containing general information from the results of the scan, as shown in Figure 4-2.
- A technical report of detailed explanations of the vulnerabilities and specific countermeasures.

Like most good security tools, you pay for QualysGuard — it isn't the *least* expensive tool, but you get what you pay for. With QualysGuard, you buy a block of scans based on the number of scans you run.


https://qualysguard.qualys.com - Scan Results - Mozilla Firefox
Done
qualysguard.qualys.com

Summary of Vulnerabilities

Vulnerabilities Total	108	Average Security Risk	5.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	1	0	1
4	1	0	0	1
3	21	4	2	27
2	22	3	11	36
1	3	0	40	43
Total	47	8	53	108

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
General remote services	37	1	12	50
Web server	3	2	13	18
Mail services	2	3	7	12
TCP/IP	2	0	8	10
Information gathering	0	0	7	7
Total	44	6	47	97

Vulnerabilities by Severity

Figure 4-2: Executive summary data in a QualysGuard vulnerability assessment report.

Assessing vulnerabilities with a tool like QualysGuard requires follow-up expertise. You can't rely on the scan results alone. You have to validate the vulnerabilities it reports. Study the reports to base your recommendations on the context and criticality of the tested systems.

Penetrating the System

You can use identified critical security holes to do the following:

- Gain further information about the host and its data.
- Obtain a remote command prompt.
- Start or stop certain services or applications.
- Access other systems.
- Disable logging or other security controls.
- Capture screen shots.
- Access sensitive files.
- Send an e-mail as the administrator.

- Perform SQL injection attacks.
- Launch another type of DoS attack.
- Upload a file proving your victory.

Metasploit (`www.metasploit.com/framework`) is great for exploiting many of the vulnerabilities you find and allows you to obtain complete system penetration. Ideally, you've already made your decision on whether to fully exploit the vulnerabilities you find. You might want to leave well enough alone by just demonstrating the existence of the vulnerabilities and not actually exploiting them.

If you want to delve into the methodology component even further, I recommend you check out the Open Source Security Testing Methodology Manual (`www.isecom.org/osstmm`) for more information.

Contents at a Glance

Table of Contents

Part VII: The Part of Tens