MICHAEL GREGG
OMAR SANTOS

Cert Guide

Learn, prepare, and practice for exam success

CEH

Certified Ethical Hacker

Version 10

PEARSON IT
CERTIFICATION

Third Edition

Certified Ethical Hacker (CEH) Version 10 Cert Guide

Third Edition

Michael Gregg
Omar Santos

Pearson

ISBN-13: 978-0-7897-6052-4

ISBN-10: 0-7897-6052-5

Library of Congress Control Number: 2019940687

ScoutAutomatedPrintCode

Trademarks

Warning and Disclaimer

Special Sales

Publisher
Mark L. Taub

Product Line Manager
Brett Bartow

Acquisitions Editor
Paul Carlstroem

Development Editor
Rick Kughen

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
MediaMix Productions, LLC

Indexer
Tim Wright

Proofreader
Abigail Manheim

Technical Editors
Michael Angelo
Ron Taylor

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

Contents at a Glance

Table of Contents

About the Authors

Michael Gregg (CISSP, SSCP, CISA, MCSE, MCT, CTT+, A+, N+, Security+, CCNA, CASP, CISA, CISM, CEH, CHFI, and GSEC) directs the cyber security operations for a multinational organization that operates facilities worldwide. As the CISO, Michael is responsible for securing the organization's assets on a global scale. Michael is responsible for developing cost-effective and innovative technology solutions for security issues and for evaluating emerging technologies.

He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to coauthoring the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or coauthored 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (Wiley, 2008); *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (Syngress, 2006); *Certified Ethical Hacker Exam Prep 2* (Que, 2006); and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (Sams, 2005).

Michael has testified before a U.S congressional committee, has been quoted in newspapers such as the *New York Times*, and was featured on various television and radio shows, including NPR, ABC, CBS, Fox News, and others, discussing cyber security and ethical hacking. He has created more than a dozen IT security training classes. He has created and performed video instruction on many security topics, such as cyber security, CISSP, CISA, Security+, and others.

When not working, speaking at security events, or writing, Michael enjoys 1960s muscle cars and has a slot in his garage for a new project car.

You can reach Michael by email at MikeG@thesolutionfirm.com.

Omar Santos is an active member of the security community, where he leads several industry-wide initiatives and standard bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants that are dedicated to increasing the security of the critical infrastructure.

Omar is the author of more than 20 books and video courses and numerous white papers, articles, and security configuration guidelines and best practices. Omar is a principal engineer of the Cisco Product Security Incident Response Team (PSIRT), where he mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar has been quoted by numerous media outlets, such as The Register, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune, Ars Technica, and more. Additional information about Omar can be obtained from h4cker.org and omarsantos.io. You can follow Omar on Twitter at @santosomar.

Dedications

Michael:

To my parents, Betty and Curly, who always stood behind me, encouraged me, and prayed that all my dreams would come true.

Omar:

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book. I also dedicate this book to my father, Jose, and to the memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

Acknowledgments

Michael:

I would like to say thanks to Grace, Michael, Paul, Tonya, and all the team at Pearson for helping make this book a reality.

Omar:

This book is a result of concerted efforts of various individuals whose help brought this book to reality. I would like to thank the technical reviewers, Ron Taylor and Michael F. Angelo, for their significant contributions and expert guidance. I would also like to express our gratitude to the team at Pearson, especially to Rick Kughen, Paul Carlstroem, Tonya Simpson, and Barbara Hacha for their help and continuous support throughout the development of this book.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Introduction

The EC-Council Certified Ethical Hacker (CEH) exam has become one of the leading ethical hacking and cybersecurity certifications available today. CEH is recognized by the industry as providing candidates with a solid foundation of hands-on security testing skills and knowledge. The CEH exam covers a broad range of security concepts to prepare candidates for the technologies that they are likely to be working with if they move into a role that requires hands-on security testing.

Let's talk some about what this book is. It offers you the information for what you need to know to pass the CEH exam. It's highly recommended that you spend time with the tools and software discussed in the book. You should also complete a number of practice tests to become more comfortable with the type of questions you will see on the exam and get used to completing 125 questions in four hours. Depending on your personal study habits or learning style, you might benefit from buying this book *and* taking a class.

NOTE After completing the CEH exam, candidates may elect to attempt the CEH Practical exam. Individuals who possess the CEH credential will be able to sit for the CEH Practical exam. This exam will test their limits in unearthing vulnerabilities across major operating systems, databases, and networks. The CEH Practical exam is a six-hour, hands-on exam that requires you to demonstrate the application of ethical hacking techniques, such as threat vector identification, network scanning, OS detection, vulnerability analysis, system hacking, and web app hacking.

Cert Guides are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the actual certification exam. The instructional design implemented in the Cert Guides reflects the nature of the CEH certification exam. The Cert Guides provide you with the factual knowledge base you need for the exams, and then take it to the next level with exercises and exam questions that require you to engage in the analytic thinking needed to pass the CEH exam.

EC-Council recommends that typical candidates for this exam have a minimum of 2 years of experience in IT security. In addition, EC-Council recommends that candidates have preexisting knowledge of networking, TCP/IP, and basic computer knowledge.

Now, let's briefly discuss what this book is not. It is not a book designed to teach you advanced hacking techniques or the latest hack. This book's goal is to prepare you for the CEH 312-50 exam, and it is targeted to those with some networking, OS, and systems knowledge. It provides basics to get you started in the world of ethical

hacking and prepare you for the exam. Those wanting to become experts in this field should be prepared for additional reading, training, and practical experience.

How to Use This Book

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization; instead, it is designed to help you truly learn and understand the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don't know, and be well prepared for the exam. These tools include the following:

- **"Do I Know This Already?" Quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter. The answers are provided in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."
- **Foundation Topics:** These are the core sections of each chapter. They explain the tools and hacking concepts, and explain the configuration of both for the topics in that chapter.
- **Exam Preparation Tasks:** This section lists a series of study activities that you should complete after reading the "Foundation Topics" section. Each chapter includes the activities that make the most sense for studying the topics in that chapter. The activities include the following:
  - **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic. Review these topics carefully.
  - **Define Key Terms:** Although certification exams might be unlikely to ask a question such as "Define this term," the CEH 312-50 exam requires you to learn and know a lot of tools and how they are used. This section lists some of the most important terms from the chapter, asking you to write a short definition and compare your answer to the Glossary.

- **Exercises:** One or more sample exercises at the end of many chapters list a series of tasks for you to practice, which apply the lessons from the chapter in a real-world setting.
- **Review Questions:** Each chapter includes review questions to help you confirm that you understand the content you just covered. The answers are provided in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Credit

Cover image © Chainarong06/Shutterstock.

Chapter opener images © Charlie Edwards/Photodisc/Getty Images.

Chapter 1, quote from the Electronic Communication Privacy Act from U.S. Code Sections 2510 and 2701.

Chapter 1, section "Payment Card Industry Data Security Standard (PCI-DSS)," list of PCI-DSS requirements from PCI-DSS.

Chapter 2, section "NIST SP 800-15," four stages of security assessment, from "Technical Guide to Information Security Testing and Assessment," https://www.nist.gov/publications/technical-guide-information-security-testing-and-assessment.

Chapter 2, section "Open Source Security Testing Methodology Manual," OSSTMM list of key points from OSSTMM.org.

Figure 2-3, screenshot of Wireshark © Wireshark Foundation.

Figure 2-10, screenshot of Wireshark © Wireshark Foundation.

Figure 2-11, screenshot of Wireshark © Wireshark Foundation.

Figure 3-1, screenshot of Microsoft excel © Microsoft 2019.

Figure 3-2, screenshot of home page Zabasearch © 2019 Zabasearch.

Figure 3-3, screenshot of home page pipl © 2006–2019 pipl.

Figure 3-4, screenshot of Google web page © Google.

Figure 3-5, screenshot of FOCA © Telefónica Digital España.

Figure 3-7, screenshot of LoriotPro © LUTEUS SARL.

Figure 3-8, screenshot of Ping Capture © LUTEUS SARL.

Figure 3-11, screenshot of Zenmap © Nmap.

Figure 3-12, screenshot of Winfingerprint © Kirby Kuehl.

Figure 3-13, screenshot of Wireshark © Wireshark Foundation.

Figure 4-2, screenshot of DumpSec © Microsoft.

Figure 4-3, screenshot of Have I Been Pwned? © Superlative Enterprises Pty Ltd.

Figure 4-4, screenshot of Cain & Abel © Cain & Abel.

Figure 5-3, screenshot of SET © David Kennedy.

Figure 5-4, screenshot of SET © David Kennedy.

Figure 5-5, screenshot of SET © David Kennedy.

Figure 5-6, screenshot of SET © David Kennedy.

Figure 5-7, screenshot of SET © David Kennedy.

Figure 5-8, screenshot of SET © David Kennedy.

Figure 5-9, screenshot of SET © David Kennedy.

Figure 5-10, screenshot of SET © David Kennedy.

Figure 5-14, screenshot of WannaCry Ransomware © AO Kaspersky Lab.

Figure 5-17, screenshot of Wireshark © Wireshark Foundation.

Figure 5-19, screenshot of Talos © Cisco Systems, Inc.

Figure 5-20, screenshot of Process Explorer © Microsoft.

Figure 6-3, screenshot of MAC Address © MAC flooding.

Figure 6-5, screenshot of DNS Spoofing attack © Cain & Abel.

Figure 6-6, screenshot of Wireshark © Wireshark Foundation.

Figure 6-10, screenshot of Booter Sites © Google.

Figure 7-6, screenshot of Netcraft tool Copyright © 1995–2019 Netcraft Ltd.

Figure 7-7, screenshot of Wikto © Gareth Phillips.

Figure 7-8, screenshot of ExploitDB.com © ExploitDB.com.

Figure 7-11, screenshot of Damn Vulnerable Web Application © DVWA.

Figure 7-12, screenshot of Damn Vulnerable Web Application © DVWA.

Figure 7-13, screenshot of Damn Vulnerable Web Application © DVWA.

Figure 7-14, screenshot of Burp Suite professional © 2019 PortSwigger Ltd.

Figure 7-15, screenshot of OWASP ZAP © WASP.

Figure 7-16, screenshot of SQL statement © 1999–2019 by Refsnes Data.

Figure 7-18, screenshot of SQL injection © OWASP.

Figure 7-19, screenshot of SQL injection © OWASP.

Figure 7-20, screenshot of Webgoat © OWASP.

Figure 7-21, screenshot of Blind SQL Injection © OWASP.

Chapter 7, section “iOS,” the quote “...eliminates security layers designed to protect your personal information and your iOS device and is a violation of the iOS end-user software license agreement and is grounds for Apple to deny service for the device” © Apple, Inc.

Figure 8-6, screenshot of airmon-ng © Thomas d’Otreppe de Bouvette.

Figure 8-7, screenshot of airodump-ng © Thomas d’Otreppe de Bouvette.

Figure 8-8, screenshot of aireplay-ng © Thomas d’Otreppe de Bouvette.

Figure 8-11, screenshot of airodump-ng © Thomas d’Otreppe de Bouvette.

Figure 8-12, screenshot of aireplay-ng © Thomas d’Otreppe de Bouvette.

Figure 8-13, screenshot of airodump-ng © Thomas d’Otreppe de Bouvette.

Figure 8-14, screenshot of aircrack-ng © Thomas d’Otreppe de Bouvette.

Figure 9-3, screenshot of Snort Alerts © Squert.

Figure 9-4, screenshot of Snort Alerts © Kibana.

Figure 9-7, screenshot of Router password crack © ifm Network Experts.

Figure 10-8, screenshot of S-Tools © Naman Dwivedi.

Figure 10-9, screenshot of S-Tools © Naman Dwivedi.

Figure 10-14, screenshot of Yellowpipe Internet services © Yellowpipe.com.

Figure 11-5, screenshot of Citadel © 2019 Malwarebytes.

Chapter 11, section “Cloud Computing,” list of the advantages of using a cloud-based service from Eric Simmon, “DRAFT - Evaluation of Cloud Computing Services.”

Chapter 11, section “Cloud Computing,” list of the essential characteristics of cloud computing from Eric Simmon, “DRAFT - Evaluation of Cloud Computing Services.”

Footprinting and Scanning

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 3-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 3-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Overview of the Seven-Step Information-Gathering Process	1, 4, 6
Determining the Network Range	5
Identifying Active Machines	2, 3
Finding Open Ports and Access Points	10
Fingerprinting Services	7
Mapping the Network Attack Surface	8, 9

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Where should an ethical hacker start the information-gathering process?
   a. Interview with company
   b. Dumpster diving
   c. Company's website
   d. Interview employees

2. What is the common Windows and Linux tool that is used for port scanning?
   a. Hping
   b. Amap
   c. Nmap
   d. SuperScan

3. What does the Nmap **-sT** switch do?
   a. UDP scan
   b. ICMP scan
   c. TCP full connect scan
   d. TCP ACK scan

4. Which of the following would be considered outside the scope of footprinting and information gathering?
   a. Finding physical addresses
   b. Attacking targets
   c. Identifying potential targets
   d. Reviewing company website

5. During a security assessment you are asked to help with a footprinting activity. Which of the following might be used to determine network range?
   a. ARIN
   b. DIG
   c. Traceroute
   d. Ping host

6. You have been asked to gather some specific information during a penetration test. The **"intitle"** string is used for what activity?
   a. Traceroute
   b. Google search
   c. Website query
   d. Host scanning

7. During a footprinting exercise, you have been asked to gather information from APNIC and LACNIC. What are these examples of?
   a. IPv6 options
   b. DHCP servers
   c. DNS servers
   d. RIRs

8. CNAMEs are associated with which of the following?
   a. ARP
   b. DNS
   c. DHCP
   d. Google hacking

9. LoriotPro is used for which of the following?
   a. Active OS fingerprinting
   b. Passive OS fingerprinting
   c. Mapping
   d. Traceroute

10. What scan is also known as a zombie scan?
    a. IDLE scan
    b. SYN scan
    c. FIN scan
    d. Stealth scan

Foundation Topics

Overview of the Seven-Step Information-Gathering Process

Footprinting is the first step of the hacking methodology, and it is all about gathering information. Most organizations share a tremendous amount of information and data through various channels, including their websites and social media pages, their employees, and even their help desks. Footprinting is about information gathering and is both passive and active. Reviewing the company's website is an example of passive footprinting, whereas calling the help desk and attempting to social engineer them out of privileged information is an example of active information gathering. Port scanning entails determining network ranges and looking for open ports on individual systems. The EC-Council divides footprinting and scanning into seven basic steps, as follows:

Key Topic

1. Information gathering
2. Determining the network range
3. Identifying active machines
4. Finding open ports and access points
5. OS fingerprinting
6. Fingerprinting services
7. Mapping the network attack surface

Many times, students ask for a step-by-step method of information gathering. Realize that these are just general steps and that ethical hacking is really the process of discovery. Although the material in this book is covered in an ordered approach, real life sometimes varies. When performing these activities, you might find that you are led in a different direction from what you originally envisioned.

Information Gathering

The information-gathering steps of footprinting and scanning are of utmost importance. Good information gathering can make the difference between a successful pen test and one that has failed to provide maximum benefit to the client. This information can be found on the organization's website, published trade papers,

Usenet, financial databases, or even from disgruntled employees. Some potential sources are discussed, but first, let's review documentation.

Documentation

One important aspect of information gathering is documentation. Most people don't like paperwork, but it's a requirement that you cannot ignore. The best way to get off to a good start is to develop a systematic method to profile a target and record the results. Create a matrix with fields to record domain name, IP address, DNS servers, employee information, email addresses, IP address range, open ports, and banner details. Figure 3-1 gives an example of what your information matrix might look like when you start the documentation process.

	A	B	C	D	E
1	**Obtained Thru Search Engine**	**Results**	**Social Network Sites**	**Results**	**Website Footprinting**
2	Employees		Profile		OS's
3	Login pages		News		Scripting
4	Portal URL's		Education		Job requests
5	Technologies		Family		Other
6	**Email Footprinting**	**Results**	**People Search Sites**	**Results**	**Google Hacking**
7	IP address		Date of birth		Files containing passwords
8	Email Address		Email		Error messages
9	Geo location		Photos		Other findings
10	**Whois Footprinting**	**Results**	**Network footprinting**	**Results**	**DNS footprinting**
11	Domain name		Network range		DNS servers
12	Contact details		Subnet mask		Zone transfer (Y/N)
13	Domain creation date		Traceroute findings		Types of Servers
14	Hosting company		Other data		DNSSEC (Y/N)

FIGURE 3-1 Documentation

Building this type of information early on will help in mapping the network and planning the best method of attack.

The Organization's Website

With the initial documentation out of the way, it's time to get started. The best place to begin is the organization's website. Search for the company's URL with Google, Bing, Dogpile, Shodan, or your search engine of choice. You will want to look for the following:

- **Company URL:** Domain name.
- **Internal URLs:** As an example, not only xyz.com but also support.xyz.com.
- **Restricted URLs:** Any domains not accessible to the public.
- **Internal pages:** Company news, employment opportunities, addresses, and phone numbers. Overall, you want to look for all open source information, which is information freely provided to clients, customers, or the general public.

NOTE One great tool to find internal URLs is Netcraft's "What's that site running?" tool on its home page. You can find it at https://www.netcraft.com/.

Let's look at an example of a local web hosting company. A quick review of its site shows it has a news and updates section. Recent news states the following:

> We are proud to have just updated all of our servers to Plesk 10.0.1. Anyone logging in to these new servers as admin should use the username of the domain, for example, www.xyz.com. The passwords have been transferred from the old servers, so no password reset should be required. We used the existing domain administrator password. Our continued alliance with Extreme Networks has allowed us to complete our transition from Cisco equipment. These upgrades, along with our addition of a third connection to the Internet, give us a high degree of fault tolerance.

You might consider this good marketing information to provide potential clients. The problem is that this information is available to anyone who browses the website. This information allows attackers to know that the new systems are Linux based and that the network equipment is all Extreme Networks. If attackers were planning to launch a denial of service (DoS) attack against the organization, they now know that they must knock out three nodes to the Internet. Even a competitor would benefit from this knowledge because the company is telling the competition everything about its infrastructure.

In some cases, information may have been removed from a company website. That is when the Wayback Machine, at https://archive.org, is useful to browse archived web pages that date back to 1996. It's a useful tool for looking for information that no longer exists on a site.

NOTE Although the Wayback Machine is very useful for exploring old web pages, keep in mind that websites can be removed or blocked so that they are not listed.

Another big information leakage point is the company directories. These usually identify key employees or departments. By combining this information with a little social engineering, an attacker can call the help desk, pretend he works for one of these key employees, and demand that a password is reset or changed. He could also use biographical information about a key employee to perform other types of social engineering trickery. Kevin Mitnick used social engineering techniques.

During a pen test, you want to record any such findings and make sure to alert the organization as to what information is available and how it might be used in an attack.

One method to gain additional information about the organization's email server is to send an email that will bounce from the site. If the site is www.xyz.com, send a mail to badaddress@xyz.com. It will bounce back to you and give you information in its header, including the email server IP address and email server version. Another great reason for bouncing an email message is to find out whether the organization makes use of mail scrubbers. Whatever you find, you should copy the information from the headers and make a note of it as you continue to gather information.

Finally, keep in mind that it's not just logical information that you want to gather. Now is a good time to record all physical information about the targeted company. Location information is used to determine the physical location of the targeted company. Bing Maps and Google Earth are two tools that can be used to get physical layout information. Bing Maps is particularly interesting because it offers a 45-degree perspective, which gives a unique view of facilities and physical landmarks. This view enables you to identify objects such as entry points and points of ingress/egress.

In the Field: Free Speech and the Web

Although the Web has drastically enhanced the ability for people to communicate, not all countries allow free speech, and many restrict what their citizens can do or post online. Others even have plans to score citizens based on their online activity. The Chinese state is setting up one such system that will monitor the behavior of its population and rank them all based on their social credit.

This social credit system, which was first announced in 2014, is scheduled to be fully operational nationwide by 2020. However, it is already in place for millions of people across the country. The scheme will be mandatory.

The exact methodology is a secret—but examples of infractions include posting negative comments about the government, buying too many video games, and posting fake news online. You can read more at https://www.vox.com/the-goods/2018/11/2/18057450/china-social-credit-score-spend-frivolously-video-games.

Job Boards

If you're lucky, the company has a job posting board. Look this over carefully; you will be surprised at how much information is given here. If no job listings are posted

on the organization's website, get interactive and check out some of the major Internet job boards. Popular sites include the following:

- Careerbuilder.com
- Monster.com
- Dice.com
- Indeed.com

At the job posting site, query for the organization. Here's an example of the type of information usually found:

- Primary responsibilities for this position include management of a Windows 2019 Active Directory environment, including MS Exchange 2008, SQL 2016, and Citrix.
- Interact with the technical support supervisor to resolve issues and evaluate/maintain patch level and security updates.
- Experience necessary in Active Directory, Microsoft Clustering and Network Load Balancing, MS Exchange 2007, MS SQL 2016, Citrix MetaFrame XP, EMC CX-400 SAN-related or other enterprise-level SAN, Veritas Net Backup, BigBrother, and NetIQ Monitoring SW.
- Maintain, support, and troubleshoot a Windows 10 LAN.

Did this organization give away any information that might be valuable to an attacker? They actually have told attackers almost everything about their network. Just the knowledge that the organization is running Windows 10 is extremely valuable.

NOTE Discovering unsecured devices or infrastructure could be used to determine if a Bitcoin miner could successfully be placed on the victim's network without his knowledge.

One way to reduce the information leakage from job postings is to reduce the system-specific information in the job post or to use a company confidential job posting. Company confidential postings hide the true company's identity and make it harder for attackers to misuse this type of information.

Employee and People Searches

Security is not just about technical and physical controls. It's also about people. In many modern attacks, people are the initial target. All this really means is that an ethical hacker is also going to want to see what information is available about key personnel. Whereas websites, employee directories, and press releases may provide employee names, third-party sites have the potential to provide sensitive data an attacker might be able to leverage. We can categorize these sites as either data aggregation brokers or social networking.

A staggering number of data aggregation brokerage sites are on the Web. It is easy for an attacker to perform online searches about a person. These sites allow attackers to locate key individuals, identify home phone numbers, and even create maps to people's houses. Attackers can even see the surroundings of the company or the home they are targeting with great quality satellite pictures. Here are some of the sites:

- **Pipl:** https://pipl.com/
- **Spokeo:** http://www.spokeo.com/
- **BirthdayDatabase.com:** http://www.birthdatabase.com/
- **Whitepages:** http://www.whitepages.com/
- **People Search Now:** http://www.peoplesearchnow.com/
- **Zabasearch:** http://www.zabasearch.com/
- **Peoplefinders:** http://www.peoplefinders.com/
- **Justia email finder:** http://virtualchase.justia.com/content/finding-email-addresses

NOTE Keep in mind that the amount of information you gather will depend on what part of the world you are searching. Some countries have stronger laws regarding privacy than others. For example, the European Union has strict privacy laws. Citizens of the EU have the right to be forgotten.

What's interesting about these sites is that many sites promise everything from criminal background checks, to previous addresses, to marriage records, to family members. Figures 3-2 and 3-3 offer some examples of what these sites provide.

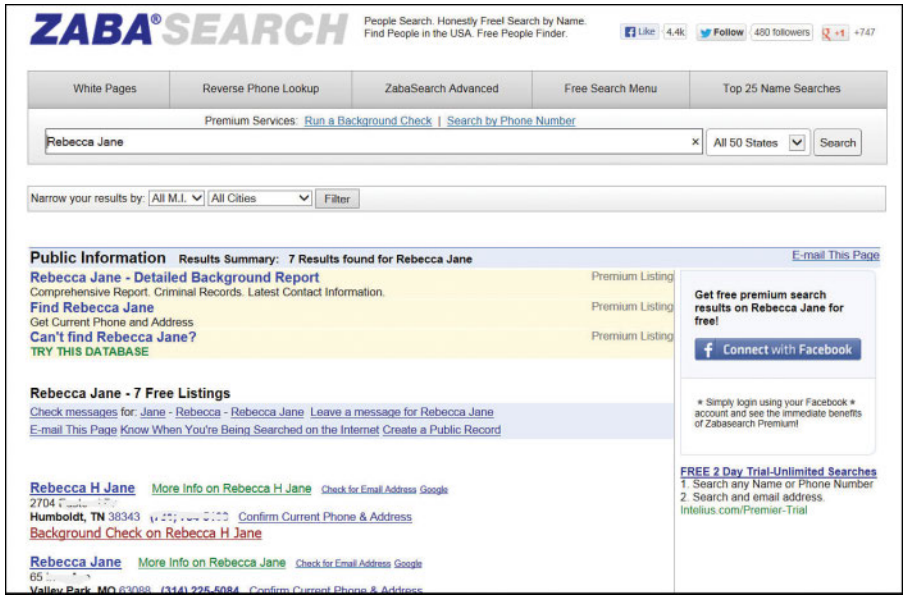

FIGURE 3-2 Zabasearch

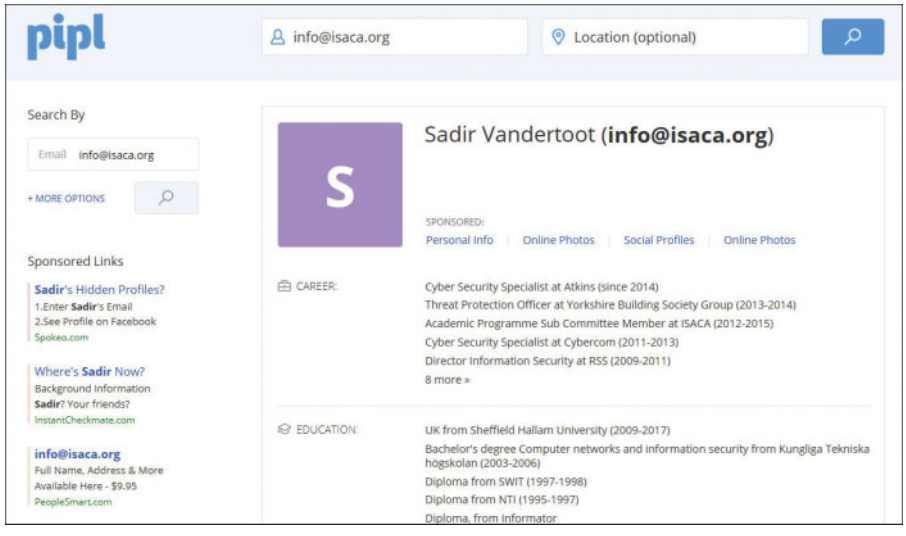

FIGURE 3-3 Pipl Email Lookup

NOTE According to the United States Federal Trade Commission, the American public has little rights over the control and dissemination of personal information except for medical records and some credit information. See https://tcf.org/content/report/data-protection-federalism/.

Social networks are another big target for attackers. Although social media has opened up great channels for communication and is very useful for marketers, it is fraught with potential security problems. Social networking sites are becoming one of the biggest threats to a user's security and will remain so for the foreseeable future. One reason is that users don't always think about security when using these sites. There is also the issue that these sites are designed to connect people. Security is not always the primary concern. Some sites that the ethical hacker may want to check include the following:

- Facebook
- Twitter
- LinkedIn
- Pinterest

TIP The three primary ways attackers use social networking include using social engineering to gather sensitive information, creating fake profiles, and using public information to gather information about a victim.

Although some organizations might be relatively secure, gaining the names, addresses, and locations of key employees can allow attackers to fly a drone over their homes, guess passwords, or even possibly backdoor the organization through an employee's unsecure credentials.

NOTE Ethical hackers can use tools like InSpy to perform enumeration on LinkedIn profiles and identify people based on company, job title, and email address.

TIP It's not just people that hackers are concerned with. Some attackers may scan the Web for competitive intelligence. It can be thought of as identifying, gathering, and analyzing information about a company's products or services.

The Dangers of Social Networks

Robin Sage is the name of a military exercise given to Army students before they receive their assignments to one of the Army's seven operational Special Forces groups. It is also the name that was recently given to a fictitious 25-year-old female pretending to be a cyberthreat analyst at the U.S. Navy's Network Warfare Command. The idea behind this ruse was to demonstrate the dangers of social networking. The results were startling.

Even though her fake Facebook profile was filled with inconsistencies, many people who should have known better tried to make contact, and passed potentially sensitive information. Her social network connections included senior military officers, a member from the Joint Chiefs of Staff, and someone from the National Reconnaissance Office (NRO); the NRO is responsible for launching and operating U.S. spy satellites.

The experiment was carried out by security consultant Thomas Ryan and revealed huge vulnerabilities in the use of social networking by people in the national security field. The results of this experiment were discussed by Mr. Ryan at the Black Hat security conference.

EDGAR Database

If the organization you are working for is publicly traded, you want to review the Security and Exchange Commission's EDGAR database. It's located at https://www.sec.gov/edgar/searchedgar/companysearch.html. A ton of information is available at this site. Hackers focus on the 10-Q and 10-K. These two documents contain yearly and quarterly reports.

NOTE The financial data found by using the EDGAR database can be used to determine whether a company should be targeted for attack or even ransomware.

Not only do these documents contain earnings and potential revenue, they also contain details about any acquisitions and mergers. Anytime there is a merger, or one firm acquires another, there is a rush to integrate the two networks. Having the networks integrated is more of an immediate concern than security. Therefore, you will be looking for entity names that are different from the parent organization. These findings might help you discover ways to jump from the subsidiary to the more secure parent company. You should record this information and have it

ready when you start to research the Internet Assigned Numbers Authority (IANA) and American Registry for Internet Numbers (ARIN) databases. Here are some other sites you can use to gather financial information about an organization:

- **Marketwatch:** http://www.marketwatch.com
- **Experian:** http://www.experian.com
- **Wall Street Consensus Monitor:** http://www.wallstreetconsensusmonitor.com/
- **Euromonitor:** http://www.euromonitor.com

Google Hacking

Most of us use Google or another search engine to locate information. What you might not know is that search engines, such as Google, can perform much more powerful searches than most people ever dream of. Not only can Google translate documents, perform news searches, and do image searches, but it can also be used by hackers and attackers to do something that has been termed *Google hacking*.

By using basic search techniques combined with advanced operators, Google can become a powerful vulnerability search tool. Table 3-2 describes some advanced operators.

Table 3-2 Google Search Terms

Operator	Description
Filetype	Directs Google to search only within the test of a particular type of file. Example: filetype:xls
Inurl	Directs Google to search only within the specified URL of a document. Example: inurl:search-text
Link	Directs Google to search within hyperlinks for a specific term. Example: link:www.domain.com
Intitle	Directs Google to search for a term within the title of a document. Example: intitle: “Index of.etc”

NOTE The CEH exam may ask you about specific Google search term strings.

By using the advanced operators shown in Table 3-2 in combination with key terms, Google can be used to uncover many pieces of sensitive information that shouldn't be revealed. A term even exists for the people who blindly post this information on the Internet; they are called Google dorks. To see how this works, enter the following phrase into Google:

```
intext:JSESSIONID OR intext:PHPSESSID inurl:access.log ext:log
```

This query searches in a URL for the session IDs that could be used to potentially impersonate users. The search found more than 100 sites that store sensitive session IDs in logs that were publicly accessible. If these IDs have not timed out, they could be used to gain access to restricted resources. You can use advanced operators to search for many types of data. Figure 3-4 shows a search where Social Security numbers (SSNs) were queried. Although this type of information should not be listed on the Web, it might have been placed there inadvertently or by someone who did not understand the security implications.

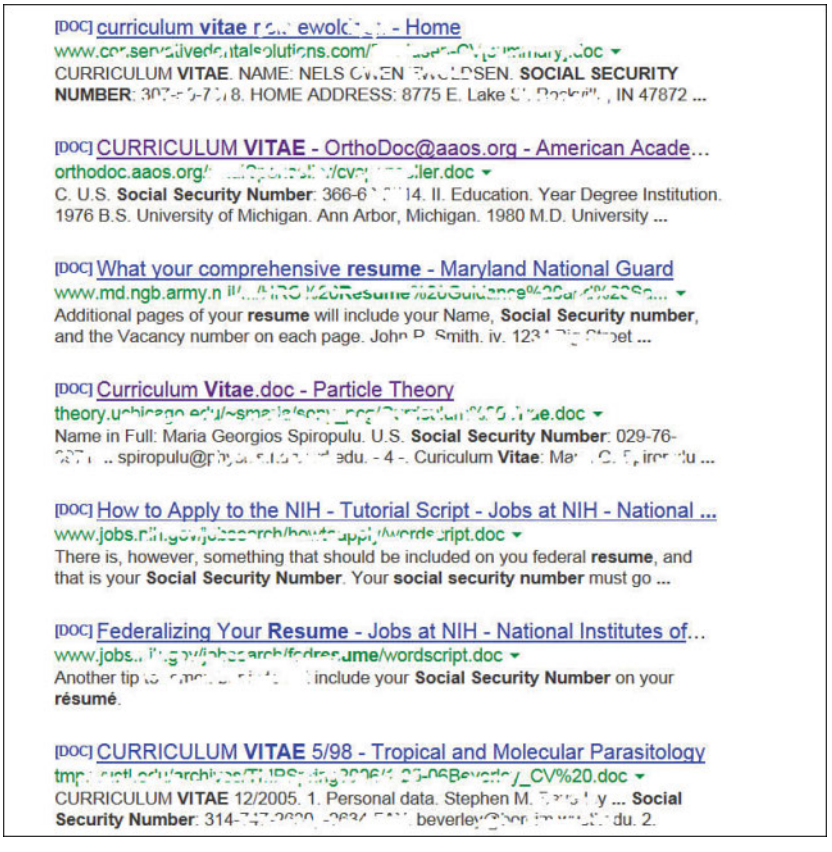

FIGURE 3-4 Google Hacking Social Security Numbers

Finally, don't forget that finding a vulnerability using Google is not unethical, but using that vulnerability can be unethical unless you have written permission from the domain owner. For example, here is a link to the Google hack for Shellshock (a Bash vulnerability introduced later in the chapter): https://www.exploit-db.com/exploits/34895/. Notice how it took only a few minutes for an attacker to gather this type of information. Security professionals should always be concerned about what kind of information is posted on the Web and who can access it.

Now that we have discussed some basic Google search techniques, let's look at advanced Google hacking. If you have never visited the Google Hacking Database (GHDB) repositories, I suggest that you visit http://www.hackersforcharity.org/ghdb/ and https://www.exploit-db.com/google-hacking-database/. These sites have the following search categories:

- Footholds
- Files containing usernames
- Sensitive directories
- Web server detection
- Vulnerable files
- Vulnerable servers
- Error messages
- Files containing juicy info
- Files containing passwords
- Sensitive online shopping info
- Network or vulnerability data
- Pages containing login portals
- Various online devices
- Advisories and vulnerabilities

Johnny Long, Bill Gardner, and Justin Brown have written an excellent book on the subject, *Google Hacking for Penetration Testers*, Third Edition. Using these techniques, you can find all sorts of information on services, files, and even people. Figure 3-4 shows an example of some of the more unbelievable things found by Google hacking.

A tool such as the GHDB has made using Google easier, but it's not your only option. Maltego, FOCA, Recon Dog, and Shodan are others worth discussion. Maltego is an open source intelligence and forensics application. It is a tool-based approach to mining and gathering Internet data that can be compiled in an easy-to-understand format. Maltego offers plenty of data on websites and their services. FOCA is another example of an open source information-gathering tool. Figure 3-5 shows an example of FOCA being used to extract metadata from documents to determine such details as software version. Similar to FOCA is Recon Dog, which is another example of an all-in-one information-gathering tool.

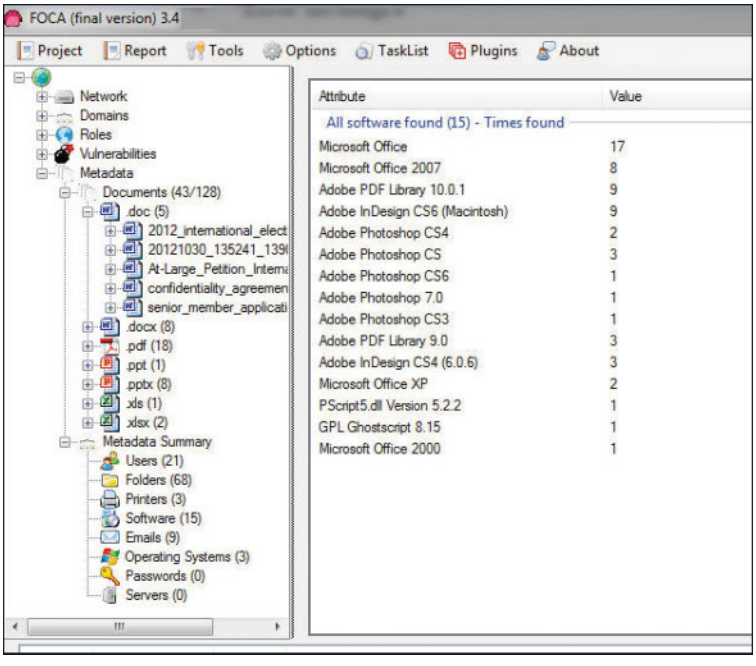

FIGURE 3-5 FOCA Extracting Metadata

Shodan offers the ability to search for the servers, webcams, printers, routers, and even SCADA devices connected to the Internet. SCADA devices are industrial controls with embedded computers that can be connected to the Internet.

Tools such as Shodan and Censys can be used to find network-connected devices, such as routers, servers, IoT devices, and even printers. Using a variety of filters, these search engines allow you to query hosts and networks for specific information.

In the Field: The Shodan Computer Search Engine

The Shodan Computer Search Engine is a powerful database of prescanned networked devices connected to the Internet. It consists of banners collected from port scans of public IP addresses, with fingerprints of services like Telnet, FTP, HTTP, and other applications.

Shodan creates risk by providing both attackers and defenders a prescanned inventory of devices connected to public IP addresses on the Internet. For example, when a new vulnerability is discovered and published, an attacker can quickly and easily search Shodan for vulnerable versions and then launch an attack. Attackers can also search the Shodan database for devices with poor configurations or other weaknesses, all without actively scanning.

Using Shodan search filters, one can really narrow down search results, by country code or CIDR netblock, for example. Shodan application programming interfaces (APIs) and some basic scripting can enable many search queries and subsequent actions (for example, a weekly query of newly discovered IPs scanned by Shodan on your CIDR netblock that runs automatically and is emailed to the security team).

Remember that public IP addresses are constantly probed and scanned already; by using Shodan, you are not scanning, because Shodan has already scanned these IPs. Shodan is a tool, and it can be used for good or evil. To mitigate risk, you can take tangible steps like registering for a free Shodan account, searching for your organization's public IPs, and informing the right network and security people of the risks of your organization's Shodan exposure. You can learn more at https://www.shodanhq.com.

This In the Field note was contributed by Shawn Merdinger, security researcher and founder of the MedSec LinkedIn group.

You might be wondering who is using all these web search tools. It's not just hackers. In 2013, documents made public by the National Security Agency (NSA) following a Freedom of Information Act (FOIA) request uncovered a PDF book titled *Untangling the Web: A Guide to Internet Research*. Although it is somewhat dated, its 643 pages contain many pages dedicated to showing federal agents how to "Google hack" and search directly for documents published online, such as Excel spreadsheets, Word documents, and PDFs. Although much of this document deals with manual ways to footprint, more modern tools like OSRFramework make the job much easier. OSRFamework is just a set of libraries that can be used to search for usernames, DNS data, phone numbers, and so on.

Usenet

Usenet is a user's network, which is nothing more than a collection of the thousands of discussion groups that reside on the Internet. Each discussion group contains

information and messages centered on a specific topic. Messages are posted and responded to by readers either as public or private emails. Even without direct access to Usenet, a convenient way to browse the content is by using Google Groups. Google Groups allows any Internet user a way to post and read Usenet messages. During a penetration test, you will want to review Google Groups for postings from the target company.

One way to search is to use individuals' names you might have uncovered; another is to do a simple search of the company. Searching for @company.com will work. Many times, this will reveal useful information. One company that I performed some work for had listings from the network administrator. He had been asked to set up a new router and was having trouble getting it configured properly. The administrator had not only asked the group for help but had also posted the router configuration to see whether someone could help figure out what was wrong. The problem was that the configuration file had not been sanitized and not only contained IP addresses but also the following information:

```
enable secret 5 $1$2RKf$OMOAcvzpb7j9uhfw6C5Uj1

enable password 7 583132656321654949
```

For those of you who might not be Cisco gurus, those are encrypted passwords. The first one is MD5 and the second is a type 7. According to Cisco, type 7 passwords were not designed to prevent a determined or targeted attack. Type 7 password encryption is only a basic protection mechanism based on a reversible algorithm. Because of the weak encryption algorithm, the Cisco position is that customers should treat configuration files as sensitive information. The problem is that attackers can potentially obtain these configuration files using a number of means, such as Usenet postings, help forums, or even a TFTP server. Others of you who say that "it's only router passwords" might be right, but let's hope that the administrator doesn't reuse passwords (as many people do). As you can see, you can gain additional information about an organization and its technical strengths just by uncovering a few Usenet posts. With possession of the password, the attacker can then use any number of tools to quickly decode the obscured password. Well-known tools that can decode Cisco 7 passwords include Cain and Abel and the Cisco Password decoder. A quick search of the Web returns dozens of hits on such a query. This brings us to the inevitable question of how to fix this problem. Actually, it is not that hard to do. First, you should not post router or firewall configurations, and the enable password command should no longer be used. Use the **enable secret** command instead; it uses the MD5 algorithm, which is much more secure.

Registrar Query

Not long ago, searching for domain name information was much easier. There were only a few places to obtain domain names, and the activities of spammers

and hackers had yet to cause the Internet Assigned Numbers Authority (IANA) to restrict the release of this information. Today, the Internet Corporation for Assigned Names and Numbers (ICANN) is the primary body charged with management of IP address space allocation, protocol parameter assignment, and domain name system management. Its role is that of overall management, as domain name registration is handled by a number of competing firms that offer various value-added services. These include firms such as Network Solutions (https://networksolutions.com), Register.com (https://www.register.com), GoDaddy (https://godaddy.com), and Tucows (http://www.tucows.com). There is also a series of Regional Internet Registries (RIRs) that manage, distribute, and register public IP addresses within their respective regions. There are five RIRs. These are shown in Table 3-3.

Table 3-3 RIRs and Their Area of Control

RIR	Region of Control
ARIN	North and South America and sub-Saharan Africa
APNIC	Asia and Pacific
RIPE	Europe, Middle East, and parts of Africa
LACNIC	Latin America and the Caribbean
AfriNIC	Planned RIR to support Africa

TIP Know the RIR for each region of the world, because this could be something you are tested on.

The primary tool to navigate these databases is Whois. Whois is a utility that interrogates the Internet domain name administration system and returns the domain ownership, address, location, phone number, and other details about a specified domain name. Whois is the primary tool used to query Domain Name System (DNS). If you're performing this information gathering from a Linux computer, the good news is Whois is built in. From the Linux prompt, users can type **whois domainname.com** or **whois?** to get a list of various options. Windows users are not as fortunate because Windows does not have a built-in Whois client. Windows users have to use a third-party tool or website to obtain Whois information.

One tool that a Windows user can use to perform Whois lookups is SmartWhois. It can be downloaded from http://www.tamos.com/products/smartwhois/. SmartWhois is a useful network information utility that allows you to look up all the available information about an IP address, hostname, or domain, including country, state or province, city, name of the network provider, administrator, and technical

support contact information. You can also use a variety of other tools to obtain Whois information, including the following:

- **BetterWhois:** http://www.betterwhois.com
- **All NETTOOLS:** www.all-nettools.com
- **DNSstuff:** www.dnsstuff.com
- **Whois Proxy:** http://geektools.com/whois.php
- **Whois Lookup:** http://www.pentest-tools.com
- **3d Traceroute:** http://www.d3tr.de/
- **Path Analyzer Pro:** https://www.pathanalyzer.com/
- **LoriotPro:** http://www.loriotpro.com/

Regardless of the tool, the goal is to obtain registrar information. As an example, the following listing shows the results after www.domaintools.com/ is queried for information about www.pearson.com:

```
Registrant:
      Pearson PLC
      Clive Carmock
      80 Strand London
      London, UK WC2R 0RL
      GB
      Email:

   Registrar Name....: CORPORATE DOMAINS, INC.
   Registrar Whois...: whois.corporatedomains.com
   Registrar Homepage: www.cscprotectsbrands.com

   Domain Name: pearson.com

      Created on..............: Mon, Nov 25, 1996
      Expires on..............: Thu, Nov 23, 2023
      Record last updated on..: Thu, Feb 02, 2017

   Administrative Contact :
      Pearson PLC
      Clive Carmock
      80 Strand London
```

```
    ., . WC2R 0RL
    GB
    Phone: 044-2070-105580
    Email:

Technical Contact:
    Pearson PLC
    Clive Carmock
    80 Strand London
    ., . WC2R 0RL
    GB
    Phone: 044-2070-105580
    Email:

DNS Servers:
usrxdns1.pearsontc.com
oldtxdns2.pearsontc.com
ns.pearson.com
ns2.pearson.com
```

This information provides a contact, address, phone number, and DNS servers. A hacker skilled in the art of social engineering might use this information to call the organization and pretend to be a valid contact.

TIP A domain proxy is one way that organizations can protect their identity while still complying with laws that require domain ownership to be public information. Domain proxies work by applying anonymous contact information as well an anonymous email address. This information is displayed when someone performs a domain Whois. The proxy then forwards any emails or contact information that might come to those addresses on to you.

DNS Enumeration

If all the previous information has been acquired, the DNS might be targeted for zone transfers. A zone transfer is the mechanism used by DNS servers to update each other by transferring the contents of their database. DNS is structured as a hierarchy so that when you request DNS information, your request is passed up the hierarchy until a DNS server is found that can resolve the domain name request. You can get a better idea of how DNS is structured by examining Figure 3-6, which shows a total of 13 DNS root servers.

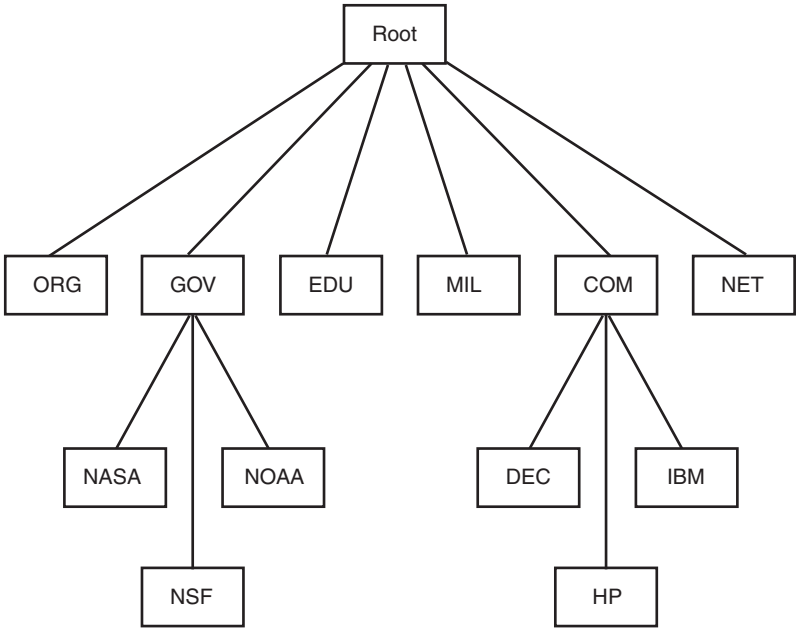

FIGURE 3-6 DNS Structure

What's left at this step is to try to gather additional information from the organization's DNS servers. The primary tool to query DNS servers is Nslookup. Nslookup provides machine name and address information. Both Linux and Windows have Nslookup clients. Nslookup is used by typing **nslookup** from the command line followed by an IP address or a machine name. Doing so causes Nslookup to return the name, all known IP addresses, and all known CNAMEs for the identified machine. Nslookup queries DNS servers for machine name and address information. Using Nslookup is rather straightforward. Let's look at an example in which Nslookup is used to find out the IP addresses of Google's web servers. If you enter **nslookup www.google.com**, the following response is obtained:

```
C:\ >nslookup www.google.com
Server:dnsr1.sbcglobal.net
Address:68.94.156.1
Non-authoritative answer:
Name:www.google.com
Addresses:64.233.187.99, 64.233.187.104
Aliases:www.google.com
```

The first two lines of output say which DNS servers are being queried. In this case, it's dnsr1.sbcglobal.net in Texas. The nonauthoritative answer lists two IP addresses for the Google web servers. Responses from nonauthoritative servers do not contain copies of any domains. They have a cache file that is constructed from all the

DNS lookups it has performed in the past for which it has gotten an authoritative response.

Nslookup can also be used in an interactive mode by just typing **nslookup** at the command prompt in Windows or the Bash shell in Linux. In interactive mode, the user will be given a prompt of **>;** at which point the user can enter a variety of options, including attempts to perform a zone transfer. Table 3-4 shows some common DNS resource record names and types.

Table 3-4 IPv4 DNS Records and Types

Record Name	Record Type	Purpose
Host	A	Maps a domain name to an IPv4 address
Host	AAAA	Maps a domain name to an IPv6 address
Pointer	PTR	Maps an IP address to a domain name
Name Server	NS	Specifies the servers that provide DNS services
Start of Authority	SOA	Configures settings for zone transfers and record caching
Service Locator	SRV	Used to locate services in the network
Mail	MX	Used to identify SMTP servers

TIP Know the various record names and types for DNS.

TIP The SOA contains the timeout value, which can be used by a hacker to tell how long any DNS poisoning would last. The Time To Live (TTL) value is the last value within the SOA.

DNS normally moves information from one DNS server to another through the DNS zone transfer process. If a domain contains more than one name server, only one of these servers will be the primary. Any other servers in the domain will be secondary servers. Zone transfers are much like the DHCP process in that each is a four-step process. DNS zone transfers function as follows:

1. The secondary name server starts the process by requesting the SOA record from the primary name server.
2. The primary then checks the list of authorized servers, and if the secondary server's name is on that list, the SOA record is sent.
3. The secondary must then check the SOA record to see whether there is a match against the SOA it already maintains. If the SOA is a match, the process

stops here; however, if the SOA has a serial number that is higher, the secondary will need an update. The serial number indicates if changes were made since the last time the secondary server synchronized with the primary server. If an update is required, the secondary name server will send an All Zone Transfer (AXFR) request to the primary server.

4. Upon receipt of the AXFR, the primary server sends the entire zone file to the secondary name server.

NOTE In September 2012, Bash, which is widely used in Linux/UNIX systems, was discovered to be vulnerable to arbitrary command execution. This family of vulnerabilities would come to be known as Shellshock and was exploited millions of times in the days following disclosure of the vulnerabilities.

A zone transfer is unlike a normal lookup in that the user is attempting to retrieve a copy of the entire zone file for a domain from a DNS server. This can provide a hacker or pen tester with a wealth of information. This is not something that the target organization should be allowing. Unlike lookups that primarily occur on UDP 53, unless the response is greater than 512 bytes, zone transfers use TCP 53. To attempt a zone transfer, you must be connected to a DNS server that is the authoritative server for that zone. An example is shown here for your convenience:

```
Registrant:
       Technology Centre
       Domain Administrator
       200 Old Tappan Rd.
       Old Tappan, NJ 07675 USA
       Email: billing@superlibrary.com
 Phone: 001-201-7846187
   Registrar Name....: REGISTER.COM, INC.
   Registrar Whois...: whois.register.com
   Registrar Homepage: www.register.com
DNS Servers:
   usrxdns1.pearsontc.com
   oldtxdns2.pearsontc.com
```

Review the last two entries. Both usrxdns1.pearsontc.com and oldtxdns2.pearsontc.com are the DNS authoritative servers listed. These are the addresses that an attacker will target to attempt a zone transfer. The steps to try to force a zone transfer are shown here:

1. **nslookup:** Enter **nslookup** from the command line.
2. **server <*ipaddress*>:** Enter the IP address of the authoritative server for that zone.

3. **set type = any:** Tells Nslookup to query for any record.
4. **ls -d <*domain.com*>:** Domain.com is the name of the targeted domain of the final step that performs the zone transfer.

One of two things will happen at this point. You will receive an error message indicating that the transfer was unsuccessful, or you will be returned a wealth of information, as shown in the following:

```
C:\Windows\system32>nslookup
Default Server:dnsr1.sbcglobal.net
Address:128.112.3.12
server 172.6.1.114
set type=any
ls -d example.com
example.com. SOA    hostmaster.sbc.net (950849 21600 3600 1728000
  3600)
example.com. NS         auth100.ns.sbc.net
example.com. NS         auth110.ns.sbc.net
example.com.  A      10.14.229.23
example.com. MX       10   dallassmtpr1.example.com
example.com. MX       20   dallassmtpr2.example.com
example.com. MX       30   lasmtpr1.example.com
lasmtpr1      A      192.172.243.240
dallassmtpr1  A      192.172.163.9
dallaslink2   A      192.172.161.4
spamassassin  A      192.172.170.49
dallassmtpr2  A      192.172.163.7
dallasextra   A      192.172.170.17
dallasgate    A      192.172.163.22
lalink        A      172.16.208.249
dallassmtp1   A      192.172.170.49
nygate        A      192.172.3.250
www           A      10.49.229.203
dallassmtp   MX       10   dallassmtpr1.example.com
dallassmtp   MX       20   dallassmtpr2.example.com
dallassmtp   MX       30   lasmtpr1.example.com
```

Dig is another tool that you can use to provide this type of information. It's built in to most all Linux distributions and can be run from Bash or run from the command prompt when installed into Windows. Dig is a powerful tool that can be used to

investigate the DNS system. There is also a range of tools that can be used to interrogate DNS servers, including the following:

- **WhereISIP:** http://www.whereisip.net/
- **DNSMap:** http://code.google.com/archive/p/dnsmap/

Internal DNS information should not be made available to just anyone. Hackers can use this to find out what other servers are running on the network, and it can help them map the network and formulate what types of attacks to launch. Notice the first line in the previous printout that has example.com listed. Observe the final value of 3600 on that line. That is the TTL value discussed previously and would inform a hacker as to how long DNS poisoning would last. 3,600 seconds is 60 minutes. Zone transfers are intended for use by secondary DNS servers to synchronize with their primary DNS server. You should make sure that only specific IP addresses are allowed to request zone transfers. Most operating systems restrict this by default. All DNS servers should be tested. It is often the case that the primary has tight security but the secondaries may allow zone transfers if misconfigured.

TIP The CEH exam expects you to understand the Nslookup and Dig functions. Be sure that you know how to get into interactive mode with Nslookup and how to extract specific information. You may be asked to verify a specific Nslookup command.

Determining the Network Range

Now that the pen test team has been able to locate names, phone numbers, addresses, some server names, and IP addresses, it's important to find out what IP addresses are available for scanning and further enumeration. If you take the IP address of a web server discovered earlier and enter it into the Whois lookup at https://www.arin.net, you can determine the network's range. For example, 192.17.170.17 was entered into the ARIN Whois, and the following information was received:

```
OrgName:                    target network
OrgID:                      Target-2
Address:                    1313 Mockingbird Road
City:                       Anytown
StateProv:                  Tx
PostalCode:                 72341
Country:                    US
ReferralServer:             rwhois://rwhois.exodus.net:4321/
NetRange:                   192.17.12.0 - 192.17.12.255
```

```
CIDR:                    192.17.0.0/24
NetName:                 SAVVIS
NetHandle                NET-192-17-12-0-1
Parent:                  NET-192-0-0-0-0
```

This means that the target network has 254 total addresses. The attacker can now focus his efforts on the range from 192.17.12.1 to 192.17.12.254/24. If these results don't prove satisfactory, the attacker can use traceroute for additional mapping.

Subnetting's Role in Mapping Networks

Some of the items you may see on the exam but are not included in any of the official courseware include subnetting. Subnetting also allows the creation of many logical networks that exist within a single Class A, B, or C network. Subnetting is important in that it helps pen testers identify what systems are part of which specific network.

To subnet a network, you must extend the natural mask with some of the bits from the host ID portion of the address. For example, if you had a Class C network of 192.168.5.0, which has a natural mask of 255.255.255.0, you can create subnets in this manner:

```
192.168.5.0 -11001100.10101000.00000101.00000000
255.255.255.224 - 11111111.11111111.11111111.11100000
-------------------------------------------------|subnet|----
```

By extending the mask from 255.255.255.0 to 255.255.255.224, you have taken 3 bits from the original host portion of the address and used them to make subnets. By borrowing 3 bits, it is possible to create eight subnets. The remaining 5 bits can provide for up to 32 host addresses, 30 of which can actually be assigned to a device because host addresses with all zeros and all ones are not assigned to specific devices. Here is a breakdown of the subnets and their address ranges:

Subnet	Host Range
192.168.5.0 255.255.255.224	host address range 1 to 30
192.168.5.32 255.255.255.224	host address range 33 to 62
192.168.5.64 255.255.255.224	host address range 65 to 94
192.168.5.96 255.255.255.224	host address range 97 to 126
192.168.5.128 255.255.255.224	host address range 129 to 158
192.168.5.160 255.255.255.224	host address range 161 to 190
192.168.5.192 255.255.255.224	host address range 193 to 222
192.168.5.224 255.255.255.224	host address range 225 to 254

The more host bits you use for a subnet mask, the more subnets you have available. However, the more subnets that are available, the fewer host addresses that are available per subnet.

Traceroute

It's advisable to check out more than one version of traceroute if you don't get the required results. Some techniques can also be used to try to slip traceroute past a firewall or filtering device. When UDP and ICMP are not allowed on the remote gateway, you can use TCPtraceroute. Another unique technique was developed by Michael Schiffman, who created a patch called traceroute.diff that allows you to specify the port that traceroute will use. With this handy tool, you could easily direct traceroute to use UDP port 53. Because that port is used for DNS queries, there's a good chance that it could be used to slip past the firewall. If you're looking for a graphical user interface (GUI) program to perform traceroute with, several are available, as described here:

- **LoriotPro:** LoriotPro (see Figure 3-7) is a professional and scalable SNMP manager and network monitoring solution that enables availability and performance control of your networks, systems, and smart infrastructures. The graphical display shows you the route between you and the remote site, including all intermediate nodes and their registrant information.

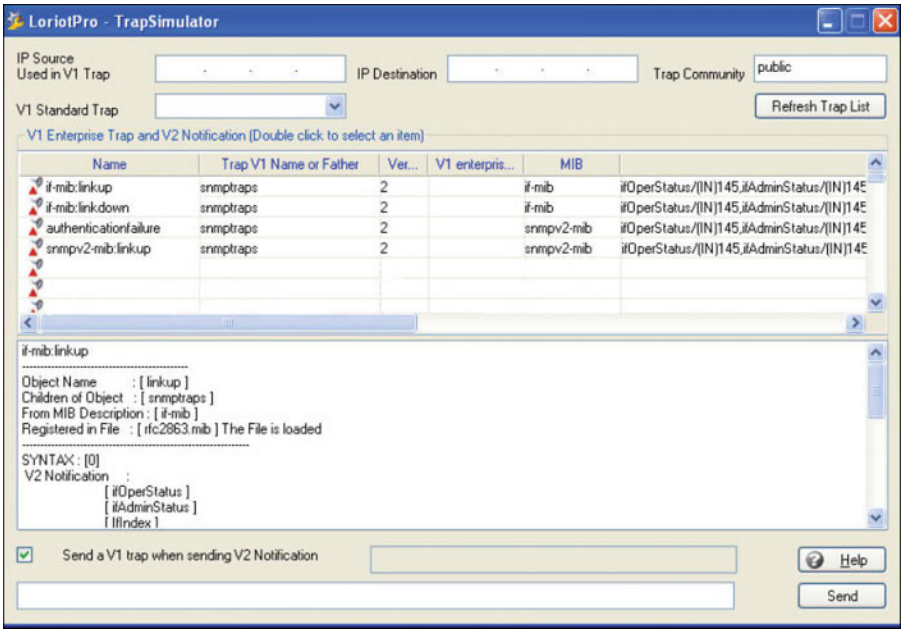

FIGURE 3-7 LoriotPro

- **Trout:** Trout is another visual traceroute and Whois program. What's great about this program is its speed. Unlike traditional traceroute programs, Trout performs parallel pinging. By sending packets with more than one TTL at a time, it can quickly determine the path to a targeted device.
- **VisualRoute:** VisualRoute is another graphical traceroute for Windows. VisualRoute not only shows a graphical world map that displays the path packets are taking, but also lists information for each hop, including IP address, node name, and geographic location. This tool is commercial and must be purchased.

TIP Traceroute and ping are useful tools for identifying active systems, mapping their location, and learning more about their location. Just keep in mind that these tools are limited by what they can see; if these services are blocked by a firewall, you may get no useful data returned.

Identifying Active Machines

Attackers will want to know whether machines are alive before they attempt to attack. One of the most basic methods of identifying active machines is to perform a ping sweep. Just because ping can be blocked does not mean it is. Although ping has been restricted by many organizations, you should still check to see if it is available. Ping uses ICMP and works by sending an echo request to a system and waiting for the target to send an echo reply back. If the target device is unreachable, a request timeout is returned. Ping is a useful tool to identify active machines and to measure the speed at which packets are moved from one host to another or to get details like the TTL. Figure 3-8 shows a ping capture from a Windows computer. If you take a moment to examine the ASCII decode in the bottom-left corner, you will notice that the data in the ping packet is composed of the alphabet, which is unlike a Linux ping, which would contain numeric values. That's because the RFC that governs ping doesn't specify what's carried in the packet as payload. Vendors fill in this padding as they see fit. Unfortunately, this can also serve hackers as a covert channel. Hackers can use a variety of programs to place their own information in place of the normal padding. Tools like Loki and icmpsend are designed for just this purpose. Then what appear to be normal pings are actually a series of messages entering and leaving the network.

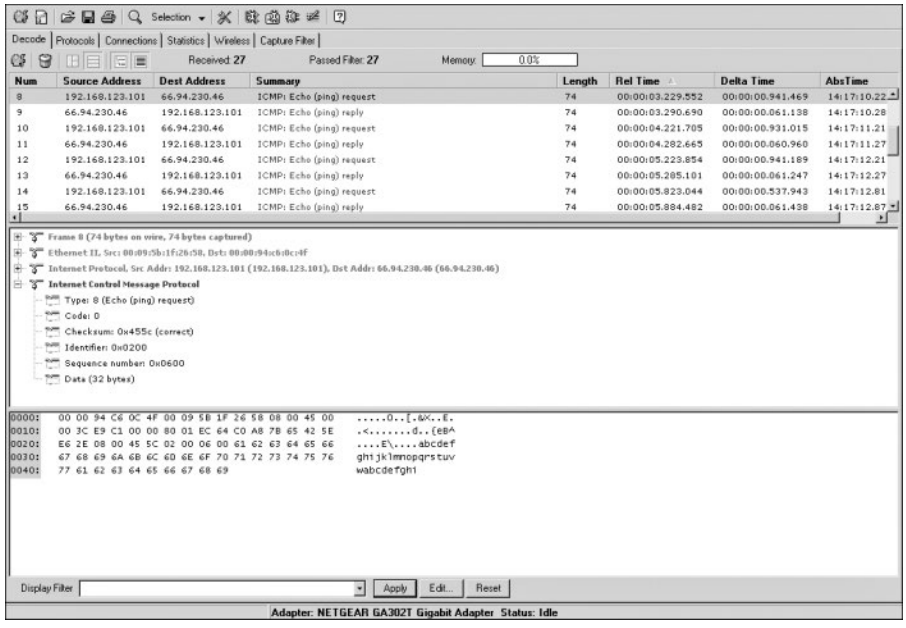

FIGURE 3-8 Ping Capture

Ping does have a couple of drawbacks: First, only one system at a time is pinged, and second, not all networks allow ping. To ping a large number of hosts, a ping sweep is usually performed. Programs that perform ping sweeps usually sweep through a range of devices to determine which ones are active. Programs that will perform ping sweeps include the following:

- **Angry IP Scanner:** http://angryip.org/
- **Hping:** http://www.hping.org/
- **WS_Ping ProPack:** https://ws-ping-propack.en.softonic.com/
- **SuperScan:** http://www.mcafee.com/us/downloads/free-tools/superscan.aspx
- **Nmap:** https://nmap.org/

TIP Know the positives and negatives of ping before taking the CEH exam.

Finding Open Ports and Access Points

Port scanning is the process of connecting to TCP and UDP ports for the purpose of finding what services and applications are running on the target device. After

discovering running applications, open ports, and services, the hacker can then determine the best way to attack the system.

As discussed in Chapter 2, "The Technical Foundations of Hacking," there are a total of 65,535 TCP and UDP ports. These port numbers are used to identify a specific process that a message is coming from or going to. Table 3-5 lists some common port numbers.

Table 3-5 Common Ports and Protocols

Port	Protocol	Service/Transport
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

TIP The exam may ask you about common or not so common ports, such as 514 (syslog) or even 179 (Internet Printing Protocol). If you see these on the test questions, the best approach is to first eliminate known ports and reduce down to the best answer.

As you have probably noticed, some of these applications run on TCP, others on UDP. Although it is certainly possible to scan for all 65,535 TCP and 65,535 UDP ports, many hackers will not. They will concentrate on the first 1,024 ports. These well-known ports are where we find most of the commonly used applications. You can find a list of well-known ports at http://www.iana.org/assignments/port-numbers. This is not to say that high-order ports should be totally ignored, because hackers might break into a system and open a high-order port, such as 31337, to use as a backdoor. So, is one protocol easier to scan for than the other? The answer to that question is yes. TCP offers more opportunity for the hacker to manipulate than UDP. Let's take a look at why.

TCP offers robust communication and is considered a connection protocol. TCP establishes a connection by using what is called a three-way handshake. Those three steps proceed as follows:

1. The client sends the server a TCP packet with the sequence number flag (SYN flag) set and an initial sequence number (ISN).
2. The server replies by sending a packet with the SYN/ACK flag set to the client. The synchronize sequence number flag informs the client that it would like to communicate with it, and the acknowledgment flag informs the client that it received its initial packet. The acknowledgment number will be one digit higher than the client's ISN. The server generates an ISN, as well, to keep track of every byte sent to the client.
3. When the client receives the server's packet, it creates an ACK packet to acknowledge that the data has been received from the server. At this point, communication can begin.

The TCP header contains a 1-byte field for the flags. Table 3-6 describes the six most common flags.

Key Topic

Table 3-6 TCP Flag Types

Flag	Description
SYN	Synchronize and initial sequence number (ISN)
ACK	Acknowledgment of packets received
FIN	Final data flag used during the four-step shutdown of a session
RST	Reset bit used to close an abnormal connection
PSH	Push data bit used to signal that data in the packet should be pushed to the beginning of the queue; usually indicates an urgent message
URG	Urgent data bit used to signify that urgent control characters are present in this packet that should have priority

TIP One easy way to remember the six most commonly used flags is as follows: **U**nruly **A**ttackers **P**ester **R**eal **S**ecurity **F**olks.

At the conclusion of communication, TCP terminates the session by using a four-step shutdown:

1. The client sends the server a packet with the FIN/ACK flags set.
2. The server sends a packet ACK flag set to acknowledge the client's packet.

3. The server then generates another packet with the FIN/ACK flags set to inform the client that it also is ready to conclude the session.
4. The client sends the server a packet with the ACK flag set to conclude the session.

TIP TCP flags are considered testable topics. You should understand their use and purpose.

The TCP system of communication makes for robust communication but also allows a hacker many ways to craft packets in an attempt to coax a server to respond or to try and avoid detection of an intrusion detection system (IDS). Many of these methods are built in to Nmap and other port-scanning tools. Before we take a look at those tools, though, some of the more popular port-scanning techniques are listed here:

- **TCP Full Connect scan:** This type of scan is the most reliable, although it is also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK, and closed ports respond with an RST/ACK.
- **TCP SYN scan:** This type of scan is known as *half open* because a full TCP three-way connection is not established. This type of scan was originally developed to be stealthy and evade IDSs, although most now detect it. Open ports reply with a SYN/ACK, and closed ports respond with an RST/ACK.
- **TCP FIN scan:** Forget trying to set up a connection; this technique jumps straight to the shutdown. This type of scan sends a FIN packet to the target port. An open port should return no response. Closed ports should send back an RST/ACK. This technique is usually effective only on UNIX devices or those compliant to RFC 793.
- **TCP NULL scan:** Sure, there should be some type of flag in the packet, but a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, open ports send no reply, whereas closed ports will return an RST.
- **TCP ACK scan:** This scan attempts to determine access control list (ACL) rule sets or identify if a firewall or simply stateless inspection is being used. A stateful firewall should return no response. If an ICMP destination is unreachable, and a communication administratively prohibited message is returned, the port is considered to be filtered. If an RST is returned, no firewall is present.

- **TCP XMAS scan:** Sorry, there are no Christmas presents here, just a port scan that has toggled on the FIN, URG, and PSH flags. Open ports should provide no response. Closed ports should return an RST. Systems must be designed per RFC 793 for this scan to work, as is common for Linux. It does not work against Windows computers.

TIP You should know common scan types, such as full and stealth, to successfully pass the exam. It's suggested that you download the Nmap tool and play with it to fully understand the options. The exam may test you over any type of Nmap scan.

Certain operating systems have taken some liberties when applying the TCP/IP RFCs and do things their own way. Because of this, not all scan types work against all systems. Results will vary, but Full Connect scans and SYN scans should work against all systems.

These are not the only types of possible scans; there are other scan types. Some scanning techniques can be used to obscure attackers and help hide their identity. One such technique is the idle or zombie scan. Before we go through an example of idle scanning, let's look at some basics on how TCP/IP connections operate. IP makes use of an identification number known as an IPID. This counter helps in the reassembly of fragmented traffic. TCP offers reliable service; it must perform a handshake before communication can begin. The initializing party of the handshake sends a SYN packet to which the receiving party returns a SYN/ACK packet if the port is open. For closed ports, the receiving party returns an RST. The RST acts as a notice that something is wrong, and further attempts to communicate should be discontinued. RSTs are not replied to; if they were replied to, we might have a situation in which two systems flood each other with a stream of RSTs. This means that unsolicited RSTs are ignored. By combining these characteristics with IPID behavior, a successful idle scan is possible.

An open port idle scan works as follows: An attacker sends an IDIP probe to the idle host to solicit a response. Suppose, for example, that the response produces an IPID of 12345. Next, the attacker sends a spoofed packet to the victim. This SYN packet is sent to the victim but is addressed from the idle host. An open port on the victim's system will then generate a SYN ACK. Because the idle host was not the source of the initial SYN packet and did not at any time want to initiate communication, it responds by sending an RST to terminate communications. This increments the IPID by one to 12346. Finally, the attacker again queries the idle host and is issued an IPID response of 12347. Because the IPID count has now been incremented by

two from the initial number of 12345, the attacker can deduce that the scanned port on the victim's system is open. Figure 3-9 provides an example of this situation.

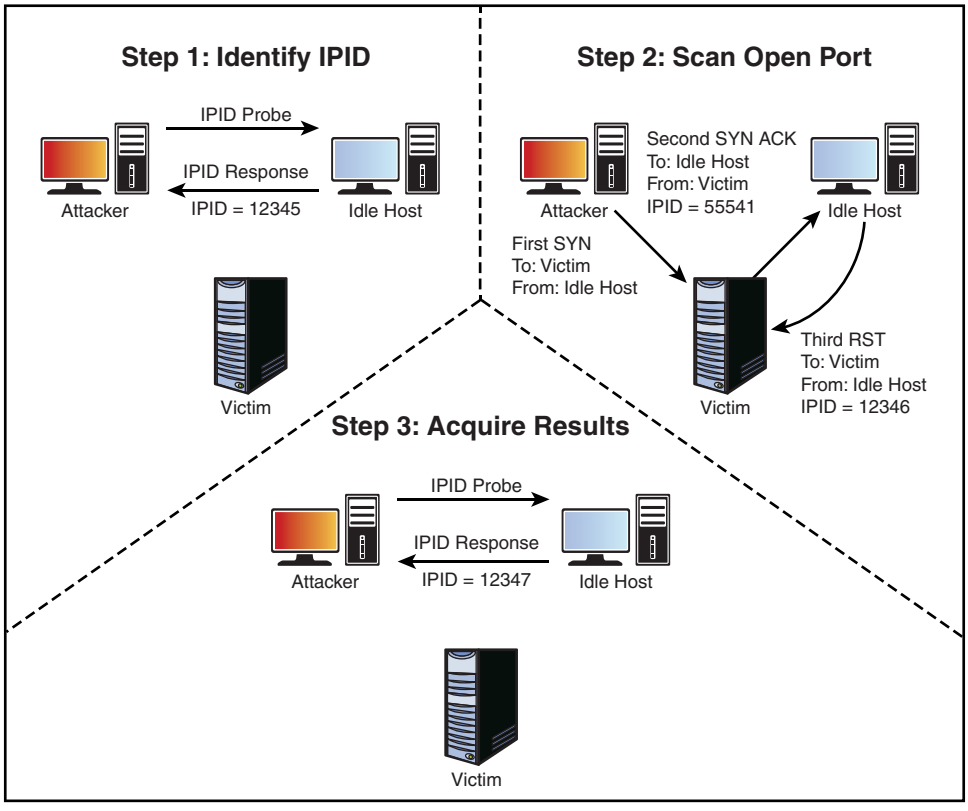

FIGURE 3-9 IPID Open Port

But what if the target system has its port closed? In that situation, the scan starts the same way as previously described. An attacker makes an initial query to determine the idle host's IPID value. Note that the value returned was 12345. In Step 2, the attacker sends a SYN packet addressed to the victim but spoofs it to appear that it originated from the idle host. Because the victim's port is closed, it responds to this query by issuing an RST. Because RSTs don't generate additional RSTs, the communication between the idle host and the victim ends here. Finally, the attacker again probes the idle host and examines the response. Because the victim's port was closed, we can see that the returned IPID was 12346. It was only incremented by one because no communication had taken place since the last IPID probe that determined the initial value. Figure 3-10 provides an example of this situation.

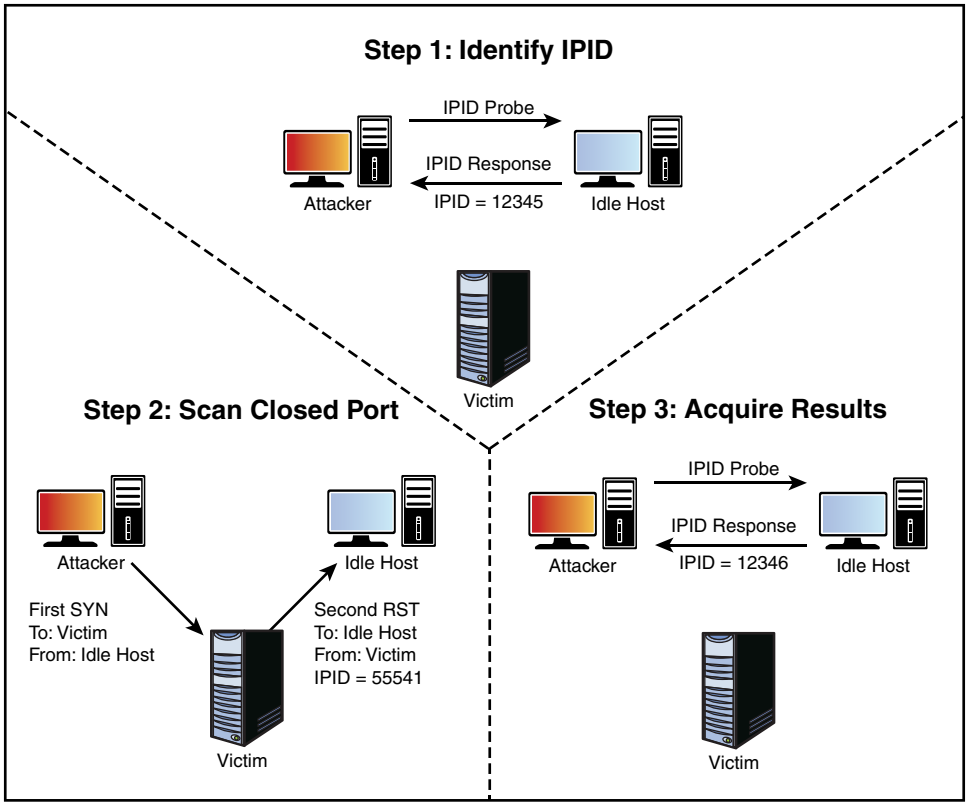

FIGURE 3-10 IPID Port Closed

Although not perfect, this scanning technique enables attackers to obscure their true address. However, limitations apply to the capability of an idle scan. First, the system designated to play the role of the idle host must truly be idle. A chatty system is of little use because the IPID will increment too much to be useful. There is also the fact that not all operating systems use an incrementing IPID. For example, some versions of Linux set the IPID to zero or generate a random IPID value. Again, these systems are of little use in such an attack. Finally, these results must be measured; by this, I mean that several passes need to be performed to validate the results and be somewhat sure that the attacker's conclusions are valid. Although the concept of idle scanning is interesting, there are a few other scan types worth briefly noting:

- **ACK scan:** Sends an ACK probe with random sequence numbers. ICMP type 3 code 13 responses may mean that stateless firewalls are being used, and an RST can mean that the port is not filtered.
- **FTP Bounce scan:** Uses an FTP server to bounce packets off of and make the scan harder to trace.

- **RPC scan:** Attempts to determine whether open ports are RPC ports.
- **Window scan:** Similar to an ACK scan but can sometimes determine open ports. It does so by examining the TCP window size of returned RST packets. On some systems, open ports return a positive window size and closed ones return a zero window size.

Now let's look at UDP scans. UDP is unlike TCP. TCP is built on robust connections, but UDP is based on speed. With TCP, the hacker can manipulate flags in an attempt to generate a TCP response or an error message from ICMP. UDP does not have flags, nor does UDP issue responses. It's a fire and forget protocol! The most you can hope for is a response from ICMP.

If the port is closed, ICMP attempts to send an ICMP type 3 code 3 port unreachable message to the source of the UDP scan. But, if the network is blocking ICMP, no error message is returned. Therefore, the response to the scans might simply be no response. If you are planning on doing UDP scans, plan for unreliable results.

Next, some of the programs that can be used for port scanning are discussed.

Is Port Scanning Legal?

In 2000, two contractors ended up in a U.S. district court because of a dispute over the legality of port scanning. The plaintiff believed that port scanning is a crime, whereas the defendant believed that only by port scanning was he able to determine which ports were open and closed on the span of network he was responsible for. The U.S. district court judge ruled that port scanning was not illegal because it does not cause damage. So, although port scanning is not a crime, you should still seek to obtain permission before scanning a network. Also, home users should review their service provider's terms and conditions before port scanning. Most cable companies prohibit port scanning and maintain the right to disconnect customers who perform such acts, even when they are performing such activities with permission. Time Warner's policy states the following: "Please be aware that Time Warner Road Runner has received indications of port scanning from a machine connected to the cable modem on your Road Runner Internet connection. This violates the Road Runner AUP (Acceptable Use Policy). Please be aware that further violations of the Acceptable Usage Policy may result in the suspension or termination of your Time Warner Road Runner account." See https://latesthackingnews.com/2017/09/30/port-scanning-legal/.

Key Topic

Nmap

Nmap was developed by a hacker named Fyodor Yarochkin. This popular application is available for Windows and Linux as a GUI and command-line program. It is probably the most widely used port scanner ever developed. It can do many types of scans and OS identification. It also enables you to control the speed of the scan from slow to insane. Its popularity can be seen by the fact that it's incorporated into other products and was even used in the movie *The Matrix*. Nmap with the help option is shown here so that you can review some of its many switches:

```
C:\ nmap-7.70>nmap -h
Nmap 7.70 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
  -sL list scan that simply does a reverse DNS lookup without actually
    scanning
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sV Version scan probes open ports determining service and app
    names/versions
 -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -P0 Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -6 scans via IPv6 rather than IPv4
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing
    policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes
    resolve]
  -oN/-oX/-oG <logfile > Output normal/XML/grepable scan logs to
    <logfile>
  -iL <inputfile > Get targets from file; Use '-' for stdin
  -sC Scripting engine
* -S <your_IP >/-e <devicename > Specify source address or network
    interface
```

```
  --interactive Go into interactive mode (then press h for help)
  --win_help Windows-specific features
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
```

TIP To better understand Nmap and fully prepare for the CEH exam, it's advisable to download and review Nmap's documentation. You can find it at https://nmap.org/book/man.html.

NOTE One example of an Nmap switch you should know is decoy. The decoy switch is used to evade an IDS or firewall. The idea is to make it appear to the target that the decoys are the source of the scan, which obscures the real source of the attacker. Decoy can be used two ways. The first is with the RND option so that nmap generates a random set of source IP addresses. The second is that the attacker can specify a specific list of spoofed source addresses.

As shown in the output of the help menu in the previous listing, Nmap can run many types of scans. Nmap is considered a required tool for all ethical hackers.

The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to create and use simple scripts to automate a wide variety of networking tasks. Nmap's output provides the open port's well-known service name, number, and protocol. Ports can either be open, closed, or filtered. If a port is open, it means that the target device will accept connections on that port. A closed port is not listening for connections, and a filtered port means that a firewall, filter, or other network device is guarding the port and preventing Nmap from fully probing it or determining its status. If a port is reported as unfiltered, it means that the port is closed, and no firewall or router appears to be interfering with Nmap's attempts to determine its status.

To run Nmap from the command line, type **nmap**, followed by the switch, and then enter a single IP address or a range. For the example shown here, the **-sT** option was used, which performs a TCP full three-step connection:

```
C:\ nmap-7.70>nmap -sT 192.168.1.108
Starting nmap 7.70 (https://nmap.org/) at 2015-10-05 23:42 Central
Daylight Time
Interesting ports on Server (192.168.1.108):
```

```
(The 1653 ports scanned but not shown below are in state:
filtered)
PORTSTATE SERVICE
80/tcpopenhttp
445/tcp opensmb
515/tcp openprinter
548/tcp openafpovertcp
Nmap run completed -- 1 IP address (1 host up) scanned in
420.475 seconds
```

Several interesting ports were found on this computer, including 80 and 139. A UDP scan performed with the **-sU** switch returned the following results:

```
C:\ nmap-7.70>nmap -sU 192.168.1.108
Starting nmap 7.70 (https://nmap.org/ ) at 2015-10-0523:47
Central
Daylight Time
Interesting ports on Server (192.168.1.108):
(The 1653 ports scanned but not shown below are in state:
filtered)
PORTSTATE SERVICE
69/udpopentftp
Nmap run completed -- 1 IP address (1 host up) scanned in
843.713 seconds
```

Now let's scan a second system so we can see the difference between a Windows computer and a Linux computer. One big clue is the potential for open ports such as 37, 79, 111, and 6000. Those represent programs such as Time, Finger, SunRpc, and X11.

```
[root@mg /root]# nmap -O 192.168.13.10
Starting nmap V. 7.70 (https://nmap.org// )
Interesting ports on unix1 (192.168.13.10):
(The 1529 ports scanned but not shown below are in state: closed)
Port        State        Service
21/tcp      open         ftp
23/tcp      open         telnet
25/tcp      open         smtp
37/tcp      open         time
79/tcp      open         finger
111/tcp     open         sunrpc
139/tcp     filtered     netbios-ssn
513/tcp     open         login
1103/tcp    open         xaudio
2049/tcp    open         nfs
```

```
4045/tcp   open         lockd
6000/tcp   open         X11
7100/tcp   open         font-service
32771/tcp  open         sometimes-rpc5
32772/tcp  open         sometimes-rpc7
32773/tcp  open         sometimes-rpc9
32774/tcp  open         sometimes-rpc11
32775/tcp  open         sometimes-rpc13
32776/tcp  open         sometimes-rpc15
32777/tcp  open         sometimes-rpc17

Remote operating system guess: Solaris 2.6 - 2.7
Uptime 319.638 days (since Wed Aug 09 19:38:19 2017)
Nmap run completed -- 1 IP address (1 host up) scanned in
7 seconds
```

Notice that the ports shown from this scan are much different from what was seen from Windows scans earlier in the chapter. Ports such as 37, 79, 111, and 32771 are shown as open. Also note that Nmap has identified the OS as Solaris. If you can, you also want to identify which applications are installed. Commands to find common ones include the following:

```
ls -alh /usr/bin/
ls -alh /sbin/
ls -alh /var/cache/apt/archivesO
dpkg -l
rpm -qa
```

TIP Regardless of the OS, scanning an IPv6 network is much harder than scanning IPv4 network ranges in that the search space is so much larger. The amount of IP addresses that must be scanned in IPv6 make it difficult to gather valid addresses. Other techniques are typically used to gather valid addresses. IPv6 addresses must be harvested in some way, such as by network traffic, recorded logs, or address received from.

Zenmap is the official Nmap Security Scanner GUI. Most of the options in Zenmap correspond directly to the command-line version. Some people call Zenmap the Nmap tutor because it displays the command-line syntax at the bottom of the GUI interface, as shown in Figure 3-11.

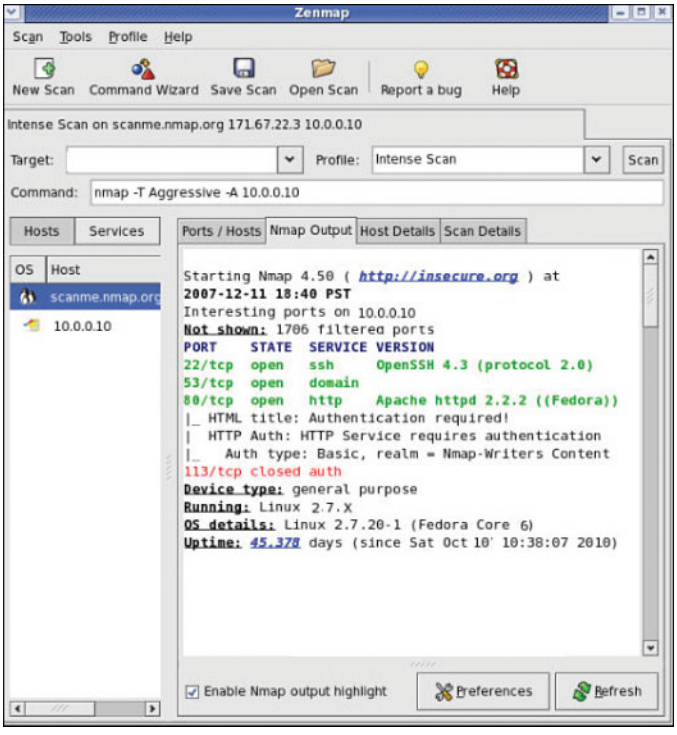

FIGURE 3-11 Zenmap

SuperScan

SuperScan is written to run on Windows machines. It's a versatile TCP/UDP port scanner, pinger, and hostname revolver. It can perform ping scans and port scans using a range of IP addresses, or it can scan a single host. It also has the capability to resolve or reverse-lookup IP addresses. It builds an easy-to-use HTML report that contains a complete breakdown of the hosts that were scanned. This includes information on each port and details about any banners that were found. It's free; therefore, it is another tool that all ethical hackers should have.

THC-Amap

THC-Amap is another example of a tool that is used for scanning and banner grabbing. One problem that traditional scanning programs have is that not all services are ready and eager to give up the appropriate banner. For example, some services, such as Secure Sockets Layer (SSL), expect a handshake. Amap handles this by storing a collection of responses that it can fire off at the port to interactively elicit it to respond. Amap was the first to perform this functionality, but it has been replaced with Nmap. One technique is to use this program by taking the greppable format of Nmap as an

input to scan for those open services. Defeating or blocking Amap is not easy, although one technique would be to use a *port-knocking* technique. Port knocking is similar to a secret handshake or combination. Only after inputting a set order of port connections can a connection be made. For example, you may have to first connect on 80, 22, and 123 before connecting to 443. Otherwise, the port will show as closed.

Hping

Hping is another very useful ethical hacking tool that can perform both ping sweeps and port scans. Hping works on Windows and Linux computers and can function as a packet builder. You can find the Hping tool at http://www.hping.org or download the Linux Backtrack distribution, which also contains Hping. Hping2 and 3 can be used for firewall testing, identifying honeypots, and port scanning. Here are some other Hping3 syntax examples of note:

- **Ping sweep: hping3 -1** *IP_Address*
- **UDP scan: hping3 -2** *IP_Address*
- **SYN scan: hping3 -8** *IP_Address*
- **ACK scan: hping3 -A** *IP_Address*
- **IPID collection:** *IP_Address* **-Q -p 139 -s**
- **XMAS scan: hping3 -F -P -U** *IP_Address*

TIP Hping is a powerful tool that you can use to bypass filtering devices by injecting crafted or otherwise modified IP packets or to port scan and perform just about any type of scan that Nmap can. Hping syntax could come up on the exam.

Port Knocking

Port knocking is a method of establishing a connection to a host that does not initially indicate that it has any open ports. Port knocking works by having the remote device send a series of connection attempts to a specific series of ports. It is somewhat analogous to a secret handshake. After the proper sequence of port knocking has been detected, the required port is opened, and a connection is established. The advantage of using a port-knocking technique is that hackers cannot easily identify open ports. The disadvantages include the fact that the technique does not harden the underlying application. Also, it isn't useful for publicly accessible services. Finally, anyone who has the ability to sniff the network traffic will be in possession of the appropriate knock sequence. A good site to check out to learn more about this defensive technique is http://www.portknocking.org.

War Driving

War driving is named after war dialing because it is the process of looking for open access points. Many pen tests contain some type of war driving activity. The goal is to identify open or rogue access points. Even if the organization has secured its wireless access points, there is always the possibility that employees have installed their own access points without the company's permission. Unsecured wireless access points can be a danger to organizations because, much like modems, they offer the hacker a way into the network that might bypass the firewall. A whole host of security tools released for Windows and Linux is available to use for war driving and wireless cracking activities.

Key Topic

OS Fingerprinting

At this point in the information-gathering process, the hacker has made some real headway. IP addresses, active systems, and open ports have been identified. Although the hacker might not yet know the type of systems he is dealing with, he is getting close. Fingerprinting is the primary way to identify a specific system. Fingerprinting works because each vendor implements the TCP/IP stack in different ways. For example, it's much the same as when you text a specific friend who typically says something like, "Hey, what's up?" while another friend simply says, "Hi." There are two ways in which the hacker can attempt to identify the targeted devices. The hacker's first choice is passive fingerprinting. The hacker's second choice is to perform active fingerprinting, which basically sends malformed packets to the target in hope of eliciting a response that will identify it. Although active fingerprinting is more accurate, it is not as stealthy as passive fingerprinting.

Passive fingerprinting is really sniffing, because the hacker is sniffing packets as they come by. These packets are examined for certain characteristics that can be pointed out to determine the OS. The following are four commonly examined items that are used to fingerprint the OS:

- **IP TTL value:** Different operating systems set the TTL to unique values on outbound packets.
- **TCP window size:** OS vendors use different values for the initial window size.
- **IP DF option:** Not all OS vendors handle fragmentation in the same way. 1500 bytes is a common size with Ethernet.
- **IP Type of Service (TOS) option:** TOS is a 3-bit field that controls the priority of specific packets. Again, not all vendors implement this option in the same way.

These are just four of many possibilities that can be used to passively fingerprint an OS. Other items that can be examined include IP identification number (IPID), IP options, TCP options, and even ICMP. Ofir Arkin has written an excellent paper on

this, titled "ICMP Usage in Scanning." An example of a passive fingerprinting tool is the Linux-based tool P0f. P0f attempts to passively fingerprint the source of all incoming connections after the tool is up and running. Because it's a truly passive tool, it does so without introducing additional traffic on the network. P0fv2 is available at http://lcamtuf.coredump.cx/p0f.tgz.

NOTE One of the most common methods used to determine the OS is to examine the TTL. For example, the default TTL of a Linux system is 64, the default TTL of Windows is 128, and the default TTL of routers is typically 254.

Active fingerprinting is more powerful than passive fingerprint scanning because the hacker doesn't have to wait for random packets, but as with every advantage, there is usually a disadvantage. This disadvantage is that active fingerprinting is not as stealthy as passive fingerprinting. The hacker actually injects the packets into the network. Active fingerprinting has a much higher potential for being discovered or noticed. Like passive OS fingerprinting, active fingerprinting examines the subtle differences that exist between different vendor implementations of the TCP/IP stack. Therefore, if hackers probe for these differences, the version of the OS can most likely be determined. One of the individuals who has been a pioneer in this field of research is Fyodor. He has an excellent chapter on remote OS fingerprinting at https://nmap.org/book/osdetect.html. Listed here are some of the basic methods used in active fingerprinting:

- **The FIN probe:** A FIN packet is sent to an open port, and the response is recorded. Although RFC 793 states that the required behavior is not to respond, many operating systems such as Windows will respond with an RST.
- **Bogus flag probe:** As you might remember from Table 3-6, the flag field is only 1 byte in the TCP header. A bogus flag probe sets one of the used flags along with the SYN flag in an initial packet. Linux will respond by setting the same flag in the subsequent packet.
- **Initial sequence number (ISN) sampling:** This fingerprinting technique works by looking for patterns in the ISN. Although some systems use truly random numbers, others, such as Windows, increment the number by a small fixed amount.
- **IPID sampling:** Many systems increment a systemwide IPID value for each packet they send. Others, such as older versions of Windows, do not put the IPID in network byte order, so they increment the number by 256 for each packet.
- **TCP initial window:** This fingerprint technique works by tracking the window size in packets returned from the target device. Many operating systems use exact sizes that can be matched against a database to uniquely identify the OS.
- **ACK value:** Again, vendors differ in the ways they have implemented the TCP/IP stack. Some operating systems send back the previous value +1, whereas others send back more random values.

- **Type of service:** This fingerprinting type tweaks ICMP port unreachable messages and examines the value in the TOS field. Whereas some use 0, others return different values.
- **TCP options:** Here again, different vendors support TCP options in different ways. By sending packets with different options set, the responses will start to reveal the server's fingerprint.
- **Fragmentation handling:** This fingerprinting technique takes advantage of the fact that different OS vendors handle fragmented packets differently. RFC 1191 specifies that the maximum transmission unit (MTU) is normally set between 68 and 65535 bytes. This technique was originally discovered by Thomas Ptacek and Tim Newsham.

Active Fingerprinting Tools

One of the first tools to be widely used for active fingerprinting back in the late 1990s was Queso. Although no longer updated, it helped move this genre of tools forward. Nmap is the tool of choice for active fingerprinting and is one of the most feature-rich free fingerprint tools in existence today. Nmap's database can fingerprint literally hundreds of different operating systems. Fingerprinting with Nmap is initiated by running the tool with the **-O** option. When started with this command switch, Nmap probes port 80 and then ports in the 20 to 23 range. Nmap needs one open and one closed port to make an accurate determination of what OS a particular system is running.

Here is an example:

```
C:\ nmap-7.70>nmap -O 192.168.123.108
Starting nmap 6.25 (https://nmap.org/) at 2005-10-0715:47
Central
Daylight Time
Interesting ports on 192.168.1.108:
(The 1653 ports scanned but not shown below are in state:
closed)
PORTSTATE SERVICE
80/tcpopenhttp
139/tcp opennetbios-ssn
515/tcp openprinter
548/tcp openafpovertcp
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 0.282 days (since Fri Oct 07 09:01:33 2018)
Nmap run completed -- 1 IP address (1 host up) scanned in 4.927
seconds
```

You might also want to try Nmap with the **-v** or **-vv** switch. There are devices such as F5 Load Balancer that will not identify themselves using a normal **-O** scan but will reveal their ID with the **-vv** switch. Just remember that with Nmap or any other active fingerprinting tool, you are injecting packets into the network. This type of activity can be tracked and monitored by an IDS. Active fingerprinting tools, such as Nmap, can be countered by tweaking the OS's stack. Anything that tampers with this information can affect the prediction of the target's OS version.

Nmap's dominance of active fingerprinting is being challenged by a new breed of tools. One such tool is Xprobe2, a Linux-based active OS fingerprinting tool with a different approach to OS fingerprinting. Xprobe is unique in that it uses a mixture of TCP, UDP, and ICMP to slip past firewalls and avoid IDS systems. Xprobe2 relies on fuzzy signature matching. In layman's terms, this means that targets are run through a variety of tests. These results are totaled, and the user is presented with a score that tells the probability of the targeted machine's OS—for example, 75% Windows 10 and 1% Windows Vista.

Because some of you might actually prefer GUI tools, the final fingerprinting tool for discussion is Winfingerprint. This Windows-based tool can harvest a ton of information about Windows servers. It allows scans on a single host or the entire network neighborhood. You can also input a list of IP addresses or specify a custom IP range to be scanned. After a target is found, Winfingerprint can obtain NetBIOS shares, disk information, services, users, groups, detection of the service pack, and even hotfixes. Figure 3-12 shows a screenshot of Winfingerprint.

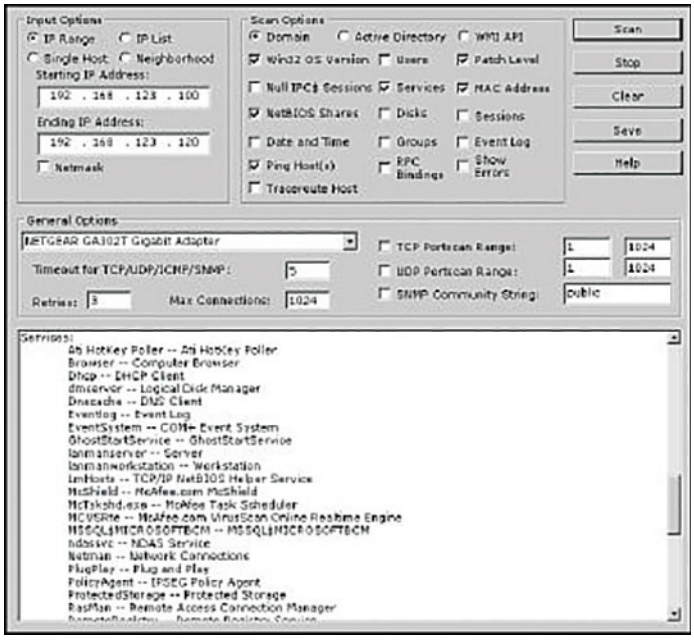

FIGURE 3-12 Winfingerprint

Fingerprinting Services

If there is any doubt left as to what a particular system is running, this next step of information gathering should serve to answer those questions. Knowing what services are running on specific ports allows the hacker to formulate and launch application-specific attacks. Knowing the common default ports and services and using tools such as Telnet and Netcat is one way to ensure success at this pre-attack stage.

Default Ports and Services

A certain amount of default information and behavior can be gleaned from any system. For example, if a hacker discovers a Windows 2012 server with port 80 open, he can assume that the system is running IIS 8.0, just as a Linux system with port 25 open is likely to be running Sendmail. Although it's possible that the Windows 2012 machine might be running another version or type of web server, that most likely is not a common occurrence.

Keep in mind that at this point, the attacker is making assumptions. Just because a particular port is active or a known banner is returned, you cannot be certain that information is correct. Ports and banners can be changed, and assumptions by themselves can be dangerous. Additional work will need to be done to verify what services are truly being served up by any open ports.

Finding Open Services

The scanning performed earlier in the chapter might have uncovered other ports that were open. Most scanning programs, such as Nmap and SuperScan, report what common services are associated with those open ports. This easiest way to determine what services are associated with the open ports that were discovered is by banner grabbing.

Banner grabbing takes nothing more than the Telnet and FTP client built in to the Windows and Linux platforms. Banner grabbing provides important information about what type and version of software is running. Many servers can be exploited with just a few simple steps if the web server is not properly patched. Telnet is an easy way to do this banner grabbing for FTP, SMTP, HTTP, and others. The command issued to banner grab with Telnet would contain the following syntax: **telnet *IP_Address* port**. An example of this is shown here. This banner-grabbing attempt was targeted against a web server:

```
C:\ >telnet 192.168.1.102 80
HTTP/1.1 400 Bad Request
Server: Microsoft-IIS/7.5
Date: Fri, 07 Oct 2012 22:22:04 GMT
```

```
Content-Type: text/html
Content-Length: 87
<html><head><title>Error</title></head><body>The parameter is
incorrect. </body>
</html>
Connection to host lost.
```

After the command was entered, **telnet 192.168.1.102 80**, the Return key was pressed a couple of times to generate a response. As noted in the Telnet response, this banner indicates that the web server is IIS 7.5.

The Microsoft IIS web server's default behavior is to return a banner after two carriage returns. This can be used to pinpoint the existence of an IIS server.

Telnet isn't your only option for grabbing banners; HTTPrint is another choice. It is available for both Windows and Linux distributions. It is not a typical banner-grabbing application, in that it can probe services to determine the version of services running. Its main fingerprinting technique has to do with the semantic differences in how web servers/applications respond to various types of probes. Here is an example of a scan:

```
./httprint -h 192.168.1.175 -s signatures.txt
httprint - web server fingerprinting tool
Finger Printing on http://192.168.1.175:80/
Finger Printing Completed on http://192.168.1.175:80/
-------------------------------------------------
Host: 192.168.1.175
Derived Signature:
Apache/2.2.0 (Fedora RedHat)
9E431BC86ED3C295811C9DC5811C9DC5050C5D32505FCFE84276E4BB811C9DC5
0D7645B5811C9DC5811C9DC5CD37187C11DDC7D7811C9DC5811C9DC58A91CF57FCCC5
35B6ED3C295FCCC535B811C9DC5E2CE6927050C5D336ED3C2959E431BC86ED3C295
E2CE69262A200B4C6ED3C2956ED3C2956ED3C2956ED3C295E2CE6923E2CE69236ED
3C295811C9DC5E2CE6927E2CE6923
Banner Reported: Apache/2.2.0 (Fedora RedHat)
Banner Deduced: Apache/2.0.x
Score: 140
Confidence: 84.31------------------------
```

Netcat can also be used for banner grabbing. Netcat is shown here to introduce you to its versatility. Netcat is called the "Swiss-army knife of hacking tools" because of its many uses. To banner grab with Netcat, you issue the following command from the command line:

```
nc -v -n IP_Address Port
```

This command gives you the banner of the port you asked to check. Netcat is available for Windows and Linux. If you haven't downloaded Netcat, don't feel totally left behind; FTP is another choice for banner grabbing. Just FTP to the target server and review the returned banner.

Most all port scanners, including those discussed in this chapter, also perform banner grabbing. However, there are lots of tools for the security professional to use to analyze open ports and banners. Some of the more notable ones you may want to review include the following:

- **ID Serve:** https://www.grc.com/id/idserve.htm
- **NetworkMiner:** http://www.netresec.com/?page=NetworkMiner
- **Satori:** http://chatteronthewire.org/
- **Netcraft:** http://toolbar.netcraft.com/site_report

Although changing banner information is not an adequate defense by itself, it might help to slow a hacker. In the Linux environment, you can change the ServerSignature line in the httpd.conf file to ServerSignature off. In the Windows environment, you can install the UrlScan security tool. UrlScan contains the RemoveServerHeader feature, which removes or alters the identity of the server from the "Server" response header in response to the client's request.

Key Topic

Mapping the Network Attack Surface

The hacker would have now gained enough information to map the network. Mapping the network provides the hacker with a blueprint of the organization. There are manual and automated ways to compile this information. Manual and automated tools are discussed in the following sections.

Manual Mapping

If you have been documenting findings, the matrix you began at the start of this chapter should be overflowing with information. This matrix should now contain domain name information, IP addresses, DNS servers, employee info, company location, phone numbers, yearly earnings, recently acquired organizations, email addresses, the publicly available IP address range, open ports, wireless access points, modem lines, and banner details.

Automated Mapping

If you prefer a more automated method of mapping the network, a variety of tools are available. Visual traceroute programs, such as SolarWinds's Network Topology

Mapper (http://www.solarwinds.com/network-topology-mapper), can help you map out the placement of these servers. You can even use Nmap scripts to trace a route and map the geolocation of a target. As an example, **nmap --traceroute --script traceroute-geolocation.nse -p 80 example.com** would perform a traceroute and provide geolocation data for each hop along the way. Geolocation allows you to identify information such as country, region, ISP, and the like. Examples of geolocation tools include IP Location Finder (https://tools.keycdn.com) and GeoIP Lookup Tool (https://www.ultratools.com).

Automatic mapping can be faster but might generate errors or sometimes provide erroneous results. Table 3-7 reviews some of the primary steps we have discussed.

NLog is one option to help keep track of your scanning and mapping information. NLog enables you to automate and track the results of your Nmap scans. It allows you to keep all your Nmap scan logs in a database, making it possible to easily search for specific entries. It's browser based, so you can easily view the scan logs in a highly customizable format. You can add your own extension scripts for different services, so all hosts running a certain service will have a hyperlink to the extension script. NLog is available at http://nlog-project.org/.

CartoReso is another network mapping option. If run from the Internet, the tool will be limited to devices that it can contact. These will most likely be devices within the demilitarized zone (DMZ). Run internally, it will diagram a large portion of the network. In the hands of a hacker, it's a powerful tool, because it uses routines taken from a variety of other tools that permit it to perform OS detection port scans for service detection and network mapping using common traceroute techniques. You can download it from https://sourceforge.net/projects/cartoreso/.

A final item worth discussing is that attacker the will typically attempt to hide her activity while actively probing a victim's network. This can be attempted via anonymizers and proxies. The concept is to try to obscure the true source address. Examples of tools that are available for this activity include the following:

- Proxy Switcher
- Proxy Workbench
- CyberGhost
- Tor

TIP Kali Linux, at https://www.kali.org/, contains many of the tools discussed in this chapter and is used for penetration testing.

Table 3-7 The Seven Steps of the Pre-Attack Phase

Step	Title	Active/Passive	Common Tools
One	Information gathering	Passive	www.domaintools.com, ARIN, IANA, Whois, Nslookup
Two	Determining network range	Passive	RIPE, APNIC, LACNIC, ARIN
Three	Identifying active machines	Active	Ping, traceroute, SuperScan, Angry IP Scanner
Four	Finding open ports and access points	Active	Nmap, Hping, Angry IP Scanner, SuperScan
Five	OS fingerprinting	Active/passive	Nmap, Winfingerprint, P0f, Xprobe2
Six	Fingerprinting services	Active	Nmap, Telnet, FTP, Netcat
Seven	Mapping the network attack surface	Active	CartoReso, traceroute, Network Topology Mapper

Summary

In this chapter, you learned the seven steps that compose the pre-attack phase: information gathering, determining the network range, identifying active machines, finding open ports and access points, OS fingerprinting, fingerprinting services, and mapping the network attack surface.

This chapter is an important step for the ethical hacker because at this point you are gathering information to launch an attack and determine the best path forward. The more information that is gathered here, the better the chance of success. You might find enough information at this point to be able to launch an attack. If not, the information gathered will serve as a foundation for subsequent steps of the attack. An important part of ethical hacking is documentation. That's why several ways to collect and document your findings are shown. There is no such thing as too much information. You may want to use a proxy or anonymizer to obscure the probes. These notes will prove useful when you prepare your report. Finally, make sure that the organization has given you written permission before beginning any work, even the reconnaissance.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have several choices for exam preparation: the exercises here, Chapter 12, "Final Preparation," and the exam simulation questions in the Pearson Test Prep Software Online.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 3-8 lists a reference of these key topics and the page numbers on which each is found.

Table 3-8 Key Topics for Chapter 3

Key Topic

Key Topic Element	Description	Page Number
List	Describes the seven-step information-gathering process	90
Table 3-6	Understand and define TCP flags	118
Section	Describes NMAP switches	124
Section	Describes how passive and active OS fingerprinting works	130
Section	Explains how to find open services: banner grabbing	134
Section	Explains tools used to map the attack surface	136

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

active fingerprinting, CNAMEs, covert channel, demilitarized zone (DMZ), denial of service (DoS), echo reply, echo request, EDGAR database, initial sequence number (ISN), Internet Assigned Numbers Authority (IANA), intrusion detection system (IDS), Nslookup, open source, passive fingerprinting, ping sweep, port knocking, script kiddie, Simple Network Management Protocol (SNMP), social engineering, synchronize sequence number, Time To Live (TTL), traceroute, war driving, Whois, written authorization, zone transfer

Exercises

3.1 Performing Passive Reconnaissance

The best way to learn passive information gathering is to use the tools. In this exercise, you perform reconnaissance on several organizations. Acquire only the information requested.

Estimated Time: 20 minutes.

Step 1. Review Table 3-9 to determine the target of your passive information gathering.

Table 3-9 Passive Information Gathering

Domain Name	IP Address	Location	Contact Person	Address and Phone Number
Redriff.com				
Examcram.com				
	72.3.246.59			
Rutgers.edu				

Step 2. Start by resolving the IP address. This can be done by pinging the site.

Step 3. Next, use a tool such as https://www.whois.net or any of the other tools mentioned throughout the chapter. Some of these include

- http://www.betterwhois.com
- www.allwhois.com
- http://geektools.com
- www.centralops.net
- www.dnsstuff.com

Step 4. To verify the location of the organization, perform a traceroute or a ping with the **-r** option.

Step 5. Use the ARIN, RIPE, and IANA to fill in any information you have yet to acquire.

Step 6. Compare your results to those found in Appendix A. Results may vary.

3.2 Performing Active Reconnaissance

The best way to learn active information gathering is to use the tools. In this exercise, you perform reconnaissance on your own internal network. If you are not on a test network, make sure that you have permission before scanning it, or your action may be seen as the precursor of an attack.

Estimated Time: 15 minutes.

Step 1. Download the most current version of Nmap from https://nmap.org/download.html. For Windows systems, the most current version is 7.30.

Step 2. Open a command prompt and go to the directory in which you have installed Nmap.

Step 3. Run **nmap -h** from the command line to see the various options.

Step 4. You'll notice that Nmap has many options. Review and find the option for a full connect scan. Enter your result here:___

Step 5. Review and find the option for a stealth scan. Enter your result here: ___

Step 6. Review and find the option for a UDP scan. Enter your result here: ___

Step 7. Review and find the option for a fingerprint scan. Enter your result here: ___

Step 8. Perform a full connect scan on one of the local devices you have identified on your network. The syntax is **nmap -sT** *IP_Address*.

Step 9. Perform a stealth scan on one of the local devices you have identified on your network. The syntax is **nmap -sS** *IP_Address*.

Step 10. Perform a UDP scan on one of the local devices you have identified on your network. The syntax is **nmap -sU** *IP_Address*.

Step 11. Perform a fingerprint scan on one of the local devices you have identified on your network. The syntax is **nmap -O** *IP_Address*.

Step 12. Observe the results of each scan. Could Nmap successfully identify the system? Were the ports it identified correct?

Review Questions

1. Your client has asked you to run an Nmap scan against the servers it has located in its DMZ. The client would like you to identify the OS. Which of the following switches would be your best option?
   a. **nmap -P0**
   b. **nmap -sO**
   c. **nmap -sS**
   d. **nmap -O**

2. During an internal pen test, you have gained access to an internal switch. You have been able to SPAN a port and are now monitoring all traffic with Wireshark. While reviewing this traffic, you are able to identify the OS of the devices that are communicating. What best describes this activity?
   a. Vulnerability scanning
   b. Nmap port scanning
   c. Active OS fingerprinting
   d. Passive OS fingerprinting

3. ICMP is a valuable tool for troubleshooting and reconnaissance. What is the correct type for a ping request and a ping response?
   a. Ping request type 5, ping reply type 3
   b. Ping request type 8, ping reply type 0
   c. Ping request type 3, ping reply type 5
   d. Ping request type 0, ping reply type 8

4. Which of the following is a vulnerability in the Bash shell that was discovered in 2014 and thereafter exploited to launch a range of attacks against Linux and UNIX systems?
   a. Shellshock
   b. Heartbleed
   c. Bashshell
   d. Poodle

5. As part of a pen test, you have port scanned a Linux system. Listed here is the scan you performed: **nmap -sX -vv -P0 192.168.1.123 -p 80**. If the system had the specific listening port open, what would be returned?
   a. RST
   b. No response
   c. SYN ACK
   d. ACK

6. Which of the following Netcat commands could be used to perform a UDP scan of the lower 1024 ports?
   a. **Nc -sS -O target 1-1024**
   b. **Nc -hU** <*host(s)*>
   c. **Nc -sU -p 1-1024** <*host(s)*>
   d. **Nc -u -v -w2** <*host*> **1-1024**

7. You have been assigned a junior pen tester during a pen test. You performed the following scan:

```
nmap -sL www.example.com
Starting Nmap 6.25 ( http://nmap.org ) at 2016-10-12 18:
 46 Central Daylight Time
Host 93.184.216.34 not scanned
```

   Your partner asks you to explain the results. Which of the following best describes the correct answer?

   a. The system was offline.
   b. The technique only checks DNS and does not scan.
   c. The syntax is incorrect.
   d. ICMP is blocked, so no scan is performed.

8. Which of the following sets all TCP flags to zeros?

   a. **nmap -sn 192.168.1.1/24**
   b. **nmap -null 192.168.1.1/24**
   c. **nmap -sX 192.168.1.1/24**
   d. **nmap -sI 192.168.1.1/24**

9. You have captured some packets from a system you would like to passively fingerprint. You noticed that the IP header length is 20 bytes and there is a datagram length of 84 bytes. What do you believe the system to be?

   a. Windows XP
   b. Linux
   c. Windows 7
   d. Windows 8

10. During the network mapping phase of a pen test, you have discovered the following two IP addresses: 192.168.1.24 and 192.168.1.35. They both have a mask of 255.255.255.224. Which of the following is true?

    a. They are on the same network.
    b. They both have a default gateway of 192.168.1.63.
    c. They both have a default gateway of 192.168.1.254.
    d. They are on separate subnets.

11. What type of scan is harder to perform because of the lack of response from open services and because packets could be lost due to congestion or from firewall blocked ports?
    a. Stealth scanning
    b. ACK scanning
    c. UDP scanning
    d. FIN scan

12. You would like to perform a scan that runs a script against SSH and attempts to extract the SSH host key. Which of the following is the correct syntax?
    a. **nmap -sC -p21, 111, 139 -T3 www.knowthetrade.com**
    b. **nmap -sC -p22, 111, 139 -T4 www.knowthetrade.com**
    c. **nmap -sL -p21, 111, 139 -T3 www.knowthetrade.com**
    d. **nmap -sI -p22, 111, 139 -T4 www.knowthetrade.com**

13. You have just performed an ACK scan and have been monitoring a sniffer while the scan was performed. The sniffer captured the result of the scan as an ICMP type 3 code 13. What does this result mean?
    a. The firewall is only a router with an ACL.
    b. The port is open.
    c. Port knocking is used.
    d. The port is closed.

14. One of the members of your security assessment team is trying to find out more information about a client's website. The Brazilian-based site has a .com extension. She has decided to use some online Whois tools and look in one of the Regional Internet Registries. Which of the following represents the logical starting point?
    a. AfriNIC
    b. ARIN
    c. APNIC
    d. RIPE

15. You have captured the Wireshark scan results shown in Figure 3-13 and are attempting to determine what type of scan was performed against the targeted system. What is your answer?

    a. SYN

    b. IPID

    c. NULL

    d. XMAS

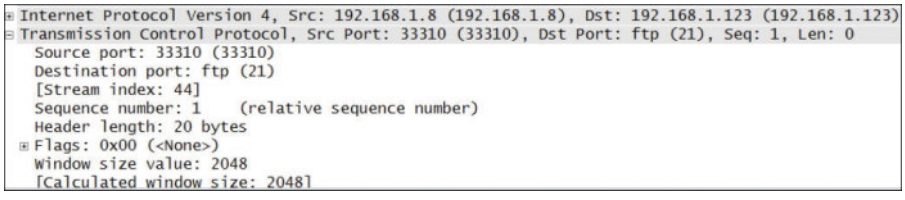

FIGURE 3-13 Wireshark Scan Capture

16. What is the purpose of the following Nmap scan?

```
Nmap -sn 192.168.123.1-254
```

    a. Ping only on the targets, no port scan

    b. A NULL TCP scan

    c. A TCP port scan

    d. Port scan all targets

17. You're starting a port scan of a new network. Which of the following can be used to scan all ports on the 192.168.123.1 network?

    a. **nmap -p 1,65536 192.168.123.1**

    b. **nmap -p- 192.168.123.1**

    c. **nmap 192.168.123.1 -ports "all"**

    d. **nmap -p 0-65536 192.168.123.1**

18. Which of following port-scanning techniques can be used to map out the firewall rules on a router?

    a. NULL scan

    b. ACK scan

    c. Inverse flag scan

    d. Firewalk

19. What are the two ICMP codes used when performing a ping?
    a. Type 0 and 8
    b. Type 0 and 3
    c. Type 3 and 5
    d. Type 5 and 11

20. You have successfully scanned a system and identified the following port 80 open. What is the next step you should perform?
    a. Attempt to go to the web page and examine the source code.
    b. Use FTP to connect to port 80.
    c. Telnet to the open port and grab the banner.
    d. Attempt to connect to port 443.

Suggested Reading and Resources

http://www.infosecwriters.com/text_resources/doc/Demystifying_Google_Hacks.doc: Demystifying Google hacks

http://www.domaintools.com/: Online Whois query website

https://nmap.org/book/man-port-scanning-techniques.html: Port-scanning techniques

https://www.exploit-db.com/google-hacking-database/: The Google Hackers Guide

https://www.greycampus.com/opencampus/ethical-hacking/scanning-methodology: The port scanning process

https://www.hackingloops.com/nmap-cheat-sheet-port-scanning-basics-ethical-hackers/: Nmap Cheat Sheet

http://www.forensicswiki.org/wiki/OS_fingerprinting: OS fingerprinting

http://www.utc.edu/center-information-security-assurance/pdfs/course-paper-5620-attacktcpip.pdf: TCP/IP from a security viewpoint

https://blog.sucuri.net/2014/09/quick-analysis-of-a-ddos-attack-using-ssdp.html: Simple Service Discovery Protocol (SSDP) usage in scanning

This page intentionally left blank

Index

B

C

D

E

F

G

H

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z