

Second Edition

COMPUTER SECURITY AND PENETRATION TESTING

Alfred Basta, Nadine Basta, and Mary Brown



PREPARING TOMORROW'S
INFORMATION
SECURITY
PROFESSIONALS

Copyrighted material



Computer Security and Penetration Testing

Second Edition

Alfred Basta
Nadine Basta
Mary Brown



Australia • Brazil • Mexico • Singapore • United Kingdom • United States

**Computer Security and Penetration Testing,
Second Edition**

Alfred Basta, Nadine Basta, and Mary Brown

Vice President, Careers & Computing: Dave Garza

Acquisitions Editor: Nick Lombardi

Director, Development—Careers and Computing:
Marah Bellegarde

Product Development Manager: Leigh Hefferon

Senior Product Manager: Natalie Pashoukos

Developmental Editor: Kent Williams

Technical Editor: Robert Zemelka

Editorial Assistant: Torey Schantz

Vice President, Marketing: Jennifer Ann Baker

Marketing Director: Deborah Yarnell

Production Director: Wendy A. Troeger

Production Manager: Andrew Crouth

Content Project Manager: Brooke Baker

Art Director: GEX

Media Editor: William Overocker

Cover Photo: ©iStockphoto.com/pheonix3d

© 2014, 2008 Cengage Learning

WCN: 02-200-208

ALL RIGHTS RESERVED. No part of this work covered by the copyright herein may be reproduced, transmitted, stored, or used in any form or by any means graphic, electronic, or mechanical, including but not limited to photocopying, recording, scanning, digitizing, taping, web distribution, information networks, or information storage and retrieval systems, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the publisher.

For product information and technology assistance, contact us at
Cengage Learning Customer & Sales Support, 1-800-354-9706

For permission to use material from this text or product,
submit all requests online at **www.cengage.com/permissions**

Further permissions questions can be emailed to
permissionrequest@cengage.com

Library of Congress Control Number: 2013939807

ISBN-13: 978-0-8400-2093-2

ISBN-10: 0-8400-2093-7

Cengage Learning200 First Stamford Place, 4th Floor
Stamford, CT 06902
USA

Cengage Learning is a leading provider of customized learning solutions with office locations around the globe, including Singapore, the United Kingdom, Australia, Mexico, Brazil, and Japan. Locate your local office at **www.cengage.com/global**.

Cengage Learning products are represented in Canada by
Nelson Education, Ltd.

To learn more about Cengage Learning Solutions, visit **www.cengage.com**.

Purchase any of our products at your local college store or at our preferred
online store **www.cengagebrain.com**.

Printed in the United States of America
1 2 3 4 5 6 7 17 16 15 14 13

Brief Contents

INTRODUCTION	xv
CHAPTER 1	
Ethics of Hacking and Cracking	1
CHAPTER 2	
Reconnaissance	17
CHAPTER 3	
Scanning Tools	45
CHAPTER 4	
Sniffers	67
CHAPTER 5	
TCP/IP Vulnerabilities	95
CHAPTER 6	
Encryption and Password Cracking	115
CHAPTER 7	
Spoofing	137
CHAPTER 8	
Session Hijacking	157
CHAPTER 9	
Hacking Network Devices	175
CHAPTER 10	
Trojan Horses	195
CHAPTER 11	
Denial-of-Service Attacks	211
CHAPTER 12	
Buffer Overflows	231
CHAPTER 13	
Programming Exploits	249
CHAPTER 14	
Mail Vulnerabilities	265
CHAPTER 15	
Web Application Vulnerabilities	289
CHAPTER 16	
Windows Vulnerabilities	311
CHAPTER 17	
UNIX/Linux Vulnerabilities	321
CHAPTER 18	
Incident Handling	335
GLOSSARY	359
INDEX	367

Table of Contents

INTRODUCTION	xv
CHAPTER 1	
Ethics of Hacking and Cracking	1
The Impact of Unethical Hacking	2
Hacker Communities	3
Hat Categories	3
Hacker Profiling	3
Hacker Motivations	5
Ethical Hacking	6
Evolution of Hacking	7
Vendor-Neutral Security Certifications	8
Vendor-Specific Security Certificates	10
What Needs to Be Secured	10
Chapter Summary	12
Key Terms	13
Review Questions	13
Hands-On Project	15
References	15
CHAPTER 2	
Reconnaissance	17
Introduction to Reconnaissance	18
Legal Reconnaissance	19
Questionable Reconnaissance	19
Illegal Reconnaissance	20
Impact of Context on Reconnaissance	20
Social Engineering	20
Social Engineering Techniques	21
Physical Intrusion	23
Communication Media	24
Countering Social Engineering	27
Dumpster Diving	27
Importance of Proper Discarding of Refuse	27
Prevention of Dumpster Diving	28
Internet Footprinting	28
Social Networking	29
Web Searching	29
Network Enumeration	31
Domain Name System–Based Reconnaissance	33
Network-Based Reconnaissance	36
Chapter Summary	39
Key Terms	40
Review Questions	41
Hands-On Projects	42
Reference	43

CHAPTER 3

Scanning Tools 45

- Introduction 46
- Evolution of Scanners 46
- How Scanners Work 48
- Types of Scanning 48
 - TCP Connect Scanning 48
 - Half-Open Scanning 49
 - UDP Scanning 49
 - IP Protocol Scanning 49
 - Ping Scanning 49
 - Stealth Scanning 49
- Review of Scanner Technology 50
 - Discovery 51
 - Reconnaissance 53
 - Vulnerability Identification 56
 - Exploitation 61
- Chapter Summary 64
- Key Terms 64
- Review Questions 65
- Hands-On Projects 66

CHAPTER 4

Sniffers 67

- Sniffer Types 68
 - Bundled Sniffers 68
 - Commercial Sniffers 69
 - Free Sniffers 69
- Sniffer Operation 69
 - Sniffer Components 70
 - Placement of a Sniffer 72
 - MAC Addresses 74
 - Data Transfer over a Network 75
 - Role of a Sniffer on a Network 77
- Sniffer Programs 78
 - Wireshark (Ethereal) 78
 - tcpdump/WinDump 80
 - Snort 81
 - Network Monitor 82
 - Cain and Abel 83
 - Kismet 83
 - Fluke Networks Protocol Analyzers 84
- Detecting a Sniffer 84
 - DNS Test 85
 - Network Latency Tests 85
 - Ping Test 85
 - Source-Route Method 85
 - Decoy Method 86
 - Commands 86
 - Time Domain Reflectometer (TDR) Method 87

Protecting Against a Sniffer	87
Secure Sockets Layer (SSL)	88
Pretty Good Privacy (PGP) and Secure/Multipurpose Internet Mail Extensions (S/MIME)	88
Secure Shell (SSH)	89
More Protection	89
Chapter Summary	89
Key Terms	90
Review Questions	91
Hands-On Projects	92
CHAPTER 5	
TCP/IP Vulnerabilities	95
Introduction to TCP/IP Vulnerabilities	96
Data Encapsulation	97
IP (Internet Protocol)	97
TCP	98
Connection Setup and Release	101
TCP/IP Timers	103
Vulnerabilities in TCP/IP	103
IP Spoofing	103
Source Routing	104
Connection Hijacking	104
ICMP Attacks	104
TCP SYN Attacks	105
RIP Attacks	105
Securing TCP/IP	105
IP Security Architecture (IPSec)	106
Chapter Summary	107
Key Terms	108
Review Questions	109
Hands-On Projects	110
CHAPTER 6	
Encryption and Password Cracking	115
Introduction to Encryption and Password Cracking	116
Cryptography	116
Symmetric and Asymmetric Key Encryption	118
Symmetric Key Encryption	118
Asymmetric Key Algorithms	120
Cryptanalysis	120
Descriptions of Popular Ciphers	121
Symmetric Key Ciphers	121
Asymmetric Key Ciphers	122
Cryptographic Hash Functions	123
Attacks on Passwords	123
Dictionary Attacks	124
Hybridization	124
Brute-Force Attacks	125
Observation	126
Keyloggers	126

Social Engineering 126
Sniffing Methods 126
Password File Stealing 127
Password Crackers 127
 Aircrack 127
 Cain & Abel 127
 John the Ripper 127
 THC Hydra 129
 LOphtCrack and Lc6 129
Chapter Summary 129
Key Terms 130
Review Questions 131
Hands-On Projects 132
References 136

CHAPTER 7

Spoofing 137
 The Process of an IP Spoofing Attack 139
 Costs of Spoofing 145
 Kinds of Tangible Loss 145
 Types of Spoofing 146
 Blind Spoofing 146
 Active Spoofing 147
 IP Spoofing 147
 ARP Spoofing 147
 Web Spoofing 147
 DNS Spoofing 148
 Spoofing Tools 149
 Mausezahn 149
 Ettercap 149
 Arpspoof 152
 Prevention and Mitigation 152
 Chapter Summary 153
 Key Terms 154
 Review Questions 154
 Hands-On Projects 156

CHAPTER 8

Session Hijacking 157
 TCP Session Hijacking 158
 Session Hijacking – Hacker’s Point of View 158
 TCP Session Hijacking with Packet Blocking 161
 Methods 162
 Session Hijacking Tools 169
 Hunt 169
 UDP Hijacking 169
 Prevention and Mitigation 169
 Encryption 169
 Storm Watching 170

.NET Framework	253
Vulnerabilities in the .NET Framework	254
Countering .NET Framework Vulnerabilities	254
HTML5	254
Vulnerabilities in HTML5	255
Countering HTML5 Vulnerabilities	256
Java and JavaScript	256
Java	256
JavaScript	257
Security Vulnerabilities in Java	258
Vulnerabilities in JavaScript	258
Countering Java and JavaScript Vulnerabilities	259
Chapter Summary	259
Key Terms	261
Review Questions	261
Hands-On Projects	262
References	263
CHAPTER 14	
Mail Vulnerabilities	265
Major Mail Protocols	266
Simple Mail Transfer Protocol (SMTP)	266
Post Office Protocol (POP)	270
Internet Message Access Protocol (IMAP)	270
Server Application Vulnerabilities	271
Microsoft Exchange Server	272
IBM Lotus Domino Notes	272
E-mail Attacks	272
List-Linking	272
E-mail Bombing	274
E-mail Spamming	274
E-mail Sniffing and Spoofing	275
E-mail Attachments	275
419s, Scams, and Phishing	276
Browser-Based Vulnerabilities	276
Microsoft Outlook 2010	277
Mozilla Thunderbird 15	277
Opera Mail	277
Protection	277
Personal E-mail Security Countermeasures	278
Corporate E-mail Security Countermeasures	279
Chapter Summary	281
Key Terms	281
Review Questions	282
Hands-On Projects	283
CHAPTER 15	
Web Application Vulnerabilities	289
Why the Web Is Vulnerable	291
Weak Passwords	292

- Unsecure Software Configuration 293
- Ease of Information Distribution 293
- Availability of Hacking Tools 293
- Increasing Opportunities for Internet-Related Criminal Activity 294
- Web Server Vulnerabilities 294**
 - Unsecure Networks 295
 - Unsecure Hardware 295
 - Threats from Insiders 295
 - Weaknesses in Site Administration Tools 295
 - Weaknesses in Application or Protocol Design 296
 - Weaknesses in Operating System Software 296
 - Coding Vulnerabilities 298
 - Implementation Vulnerabilities 299
- Protection against Web Application Vulnerabilities 300**
 - Securing the Operating System and the Web Server 300
 - Monitoring the Server for Suspicious Activity 300
 - Controlling Access to Confidential Documents 300
 - Protecting the Web Server on a LAN 301
 - Checking for Security Issues 301
- Web-Browser Vulnerabilities 301**
 - Cache File 301
 - History File 302
 - Bookmarks 303
 - Cookies 303
- Location of Web Files Cache 304**
 - Browser Information 305
 - Session ID Exploits 305
- Web-Browser Protection 306**
- Chapter Summary 307**
- Key Terms 308**
- Review Questions 308**
- Hands-On Projects 309**

CHAPTER 16

- Windows Vulnerabilities 311**
 - Windows Operating Systems 312**
 - Windows XP 312
 - Windows Vista 312
 - Windows Server 2008 313
 - Windows 7 313
 - Windows 8 313
 - Vulnerabilities in Windows Server 2008/XP/Vista/7/8 313**
 - Passwords 314
 - Default Accounts 315
 - File Sharing 315
 - Windows Registry 315
 - Trust Relationship 316
 - Windows Server 2008 Viewer Buffer Overflow 316
 - Vulnerabilities to Obtain or Elevate Privileges 317
 - RPC Service Failure 317
 - SMTP MX Record Vulnerability 318
 - Code Execution Vulnerabilities 318

Chapter Summary	318
Key Terms.	319
Review Questions.	319
Hands-On Project.	320
References	320
CHAPTER 17	
UNIX/Linux Vulnerabilities	321
Introduction.	322
UNIX-Based Operating Systems.	322
Linux Operating Systems	322
Vulnerabilities from Default Installation	323
Basic Exploits	324
Login Passwords	324
Bad System Administration Practices	324
Utility Vulnerabilities	327
Trivial File Transfer Protocol (TFTP) Vulnerability	327
Kernel Vulnerability	328
Printing Vulnerability	328
Vulnerability in mem_write Function	328
Integer Overflow Vulnerability	328
Buffer Overflow Vulnerability	328
UseLogin Vulnerability of OpenSSH	328
wu-ftpd Exploits	329
BIND Exploit.	329
Chapter Summary	329
Key Terms.	330
Review Questions.	331
Hands-On Projects	332
CHAPTER 18	
Incident Handling	335
Introduction.	336
Need for Incident Handling.	337
Types of Incidents	337
Approach to Incident Detection.	340
Detection Tools	340
Phases of Incident Handling	340
Preparation for Incident Handling	342
Classification of Incidents	343
Establishing the Impact of an Incident	344
Establishing the Likelihood of an Incident	344
Evaluation	345
Reporting and Communicating Incidents	346
Reporting the Incident	346
Communicating the Incident	347
Eliminating the Bug	347
Correcting the Root Problem.	347
Identifying and Implementing the Steps to Fix the Problem	348
Denial-of-Service Attacks	349

Recovering from Incidents	349
Reinstallation	349
Re-authentication	350
Scanning	350
Resuming work	350
Postmortem	350
Identifying the Root Cause of the Problem	350
Identifying Short-Term and Long-Term Changes	351
Identifying Actions for Any Unpredictable Incident	351
Implementing the Learning	351
Tracking Hackers	352
Generic to Specific	352
Specific to Generic to Specific	352
Emergency Steps	353
Chapter Summary	354
Key Terms	355
Review Questions	355
Hands-On Projects	356
GLOSSARY	359
INDEX	367



Introduction

This text was written to provide a large number of options for further study for interested individuals or enrolled students who desire an accurate and interesting introduction to the fascinating realm of network security.

This work is designed to give students, professionals, and hobbyists accurate and well-researched examples of current security topics. The field of information security changes quickly, and this text is formulated to provide a solid foundation to enable the reader to understand and differentiate between hype and fact. Readers will acquire a firm grasp of the concepts and history of network development and network security as they have evolved. This platform is anchored to real-world examples and techniques to glean the most useful information from the Internet. It is intended to burst the mystique, shine a light into how and why people attack computers and networks, and prepare the reader with the right techniques to begin winning the network security game.

This text is primarily intended for students in the second or third year of programs in:

- Information technology
- Network security
- Network engineering
- Computer science

ExamView®

This book is accompanied by ExamView®, a powerful testing software package that allows instructors to create and administer printed, computer (LAN-based), and Internet exams. ExamView® includes hundreds of questions that correspond to the topics covered in this text, enabling students to generate detailed study guides that include page references for further review. The computer-based and Internet testing components allow students to take exams at their computers and also save the instructor time by grading each exam automatically.

PowerPoint® Presentations

This book comes with Microsoft® PowerPoint® slides for each chapter. These are included as a teaching aid for classroom presentation, to make available to students on the network for chapter review, or to be printed for classroom distribution. Instructors, please feel free to add your own slides for additional topics you introduce to the class.

Figure Files

All of the figures are reproduced and can be used to customize the PowerPoint® slides or made available to students for review.

Read This Before You Begin

This book assumes that the student will have access to a networked PC running a current version of Linux. The computer should also have Internet access. In the Hands-On Projects at the end of Chapter 1, general instructions are given for setting up a PC to be used for this book. Note that the specific machine requirements listed are a suggestion, and that other configurations may work as well. In general, any current, standard Linux distribution should work.

Throughout the book, students will occasionally need to download software from the Internet and install it. Specific instructions are given where necessary. The text also references a “central Linux server” that the instructor may wish to set up to provide a central location from which students can access software or files. (For example, in Chapter 6, the instructor will need to provide students with a sample “passwd” file that students can use to practice using password-cracking software.) This central server is not required, and the instructor may choose to distribute files or software using other methods.

A few parts of the text—for example, Hands-On Project 10-3—are written assuming that the student has access to a Windows computer. If a Windows machine is not available, such sections can be read through without following along at the computer.

Finally, at times it will be necessary for students to access other lab computers. For example, in the project at the end of Chapter 8, the instructor should set up a TCP session between two computers, so that students can observe the session using a sniffer. At the instructor’s discretion, virtualization software such as VMware can be used if physical machines are not available.

About the Authors

Alfred Basta, PhD, is a professor of mathematics, cryptography, and information security as well as a professional speaker on Internet security, networking, and cryptography. He is a

member of many associations, including the Mathematical Association of America. Dr. Basta's other publications include *Mathematics for Information Technology*, *Linux Operations and Administration*, and *Database Security*.

Nadine Basta, MS, is a professor of computer science, information technology, and security. Her numerous certifications include MCSE, MSDBA, CCDP, NCSE, NCTE, and CCA. A security consultant and auditor, she combines strong “in the field” experience with her academic background. She is also coauthor of *Mathematics for Information Technology* and *Linux Operations and Administration*.

Mary Brown, CISSP, CISA, PhD, is a professor who leads the information assurance and security and health informatics specializations at Capella University. She manages the curricula for these programs and works with the NSA to maintain Capella as a Center of Excellence in IAS, which includes managing a Web site and blog. She is also a member of an advisory board for Advance IT, which promotes IT in Minnesota, as well as a member of numerous professional associations, including the Information Systems Security Association. Additional publications include *HIPAA Program Reference Handbook* and *Ethical Issues and Security Monitoring Trends in Global Healthcare: Technological Advancements*.

Acknowledgments

From Alfred Basta:

To my wife Nadine:

“It is the continuing symphony of your loving thoughts, caring actions, and continuous support that stands out as the song of my life.”

To our daughter Rebecca, our son Stavros:

“Fix your hearts upon God, and love Him with all your strength, for without this no one can be saved or be of any worth. Develop in yourselves an urge for a life of high and noble values. You are like little birds that will soon spread your wings and fly.”

To my mother:

“You are a never-ending melody of goodness and kindness. You are without equal in this world.”

And to the memory of my father:

“If one is weighed by the gifts one gives, your values given are beyond estimation.”

From Nadine Basta:

First, I would like to thank God for giving me the chance to complete this work. Every day I thank Him for my three precious gifts: Alfred, Becca, and Stavros.

To my beloved husband, Alfred: Thank you for your continuous love and support throughout our wonderful 17 years together.

To our children, Rebecca and Stavros: You are the true joy of our lives and our greatest blessing. We pray for you every day to live a life that honors and glorifies God. Fix your hearts upon Him, and love Him with all your strength.

Ethics of Hacking and Cracking

After reading this chapter and completing the exercises, you will be able to:

- Explain how unethical computer hacking is a crime
- Identify the various groups and classes of hackers and crackers
- Identify the various things that motivate hackers and crackers
- Explain differences in information security industry certifications
- Describe the origin and evolution of computer hacking
- Recognize the important issues related to ethical hacking

Hacking and cracking are of great interest to many students of information security as well as to hobbyists and others. This chapter introduces you to hacking and helps you understand the characteristics and motivations behind both ethical and unethical hacking activities. It also explores the wide range of industry-related certifications available to those interested in a career in ethical hacking. Many of these certifications contain a professional ethics component—a potential barrier to those who choose to begin their career engaging in questionable computing activities.

The Impact of Unethical Hacking

Cracking is the term for illegally hacking into a computer system without the permission of the system's owner. **Hacking** is a term that is often used interchangeably with "cracking," but some hackers find it offensive. In the early days of computing, someone who was very proficient in coding and in creating solutions using computers was known as a **hacker**. This was typically a way of recognizing one's accomplishments. Over the past 30 to 40 years, however, "hacker" has devolved into a more pejorative term that refers to one who uses his technical skills to engage in illegal or unethical behavior. Legitimate hackers who wanted to hold on to the term "hackers" responded to this trend by coming up with the term **cracker** to denote those on the "dark side" of computing. The information security community has now widely adopted this distinction; however, outside of those with a certain level of expertise and insight, the two terms continue to be used interchangeably.

Whatever a computer cracker's motivations—a love of difficult challenges, curiosity, patriotism, a desire for recognition or financial gain or revenge—cracking a system is a crime. In the past, crackers tended not to be prosecuted; this was because the crime was internal, and companies didn't want to jeopardize their customers' confidence. Also, companies may not have been sure of how vulnerable they were and didn't want to advertise it to other crackers. The trend today is toward prompt prosecution and harsher sentencing for those caught compromising machines owned by others. Due to the growth of computer cracking, many companies are now hiring more employees with hacking skills who can identify crackers and protect the company's network.

In the 2010/2011 CSI Computer Crime and Security Survey, nearly half of the organizations that responded indicated they had been the victim of at least one targeted attack.¹ Over two-thirds had experienced a **malware infection**, the most frequent mode of attack. Likewise, in Verizon's 2012 Data Breach Investigations Report, 69 percent of the reported breaches involved the use of malware.² Interestingly enough, 79 percent of the victims were targets of opportunity, which indicates that organizations need better oversight of their security policies. Both of these surveys focused on the numbers of compromises recorded (reportedly in the millions of records) rather than on the resulting financial losses. The CSI survey indicates that companies are increasingly reluctant to share financial loss information as part of annual surveys, which makes it increasingly difficult to assess the financial impact.

This text is designed to give you the skills to defeat computer crackers.

Information security certifications include security management-related certifications, such as the Certified Information Systems Security Professional (CISSP) and the Certified Information Security Manager (CISM) certifications, which are sponsored by the ISC2 and ISACA organizations, respectively. Organizations such as SANS (System Administration, Networking, and Security) Institute and the EC-Council promote more technology-specific certifications. Each of these certifying groups offers ethical standards to keep its members within the realm of proper behavior. Such attention to ethics is especially important with respect to hacking, where the owner's permission and the hacker's intentions are often the only things separating what is ethical from what is unethical.

Hackers themselves tend to disagree as to what is ethical and unethical. Many hackers believe that cracking a network host or device is like cutting across the neighbor's lawn. As long as there is no harm done, the act is not an invasion of the neighbor's privacy or a violation of privacy rights. The courts have typically ruled that the preliminary steps of penetration testing, such as enumeration and scanning, are not illegal activities because they do not result in actual damages. Professional standards tend to be more stringent, however; failure to obtain the network owner's permission prior to engaging in these activities is more likely to be perceived as unethical behavior.

Hacker Motivations

Regardless of their profiles, knowledge, or skills, hackers are often motivated by a combination of the following:

- Curiosity
- Love of puzzles
- Desire for recognition or fame
- Revenge
- Financial gain
- Patriotism or politics

Curiosity Perhaps the strongest motivation is curiosity: “What happens when I do this?” or “How do these security measures work?” We are trained from childhood to be curious, open, and sharing. Crackers direct their innate curiosity toward finding the blind spots in the network systems we build.

Love of Puzzles Hackers gain great satisfaction in finding the solutions to complicated puzzles. A hacker has to control many variables and master many techniques to successfully crack systems. These same challenges motivate locksmiths and cat burglars in the physical security realm. Strong passwords, such as “Tr34\$>l drU,”(tr), can be devised that block most attack attempts, and locks can be keyed with “024642” pin combinations that are almost unpickable. Think how much fun it is to figure out how to solve these difficult puzzles!

Desire for Recognition or Fame Almost all hackers are motivated by a need for acceptance, acknowledgment, and fame—at least among their peers. It takes a person of average intelligence and skill many years to become even a poor hacker. Expertise in the field is rare and marvelous in ways not necessarily understood by those outside the field.



True, hackers may be deficient in social skills or fashion sense, but they are as susceptible to the lure of fame as anyone else. As members of an elite group possessing specialized technical skills, they believe they deserve recognition. Ethical hackers may believe they are merely the last line of defense against malicious individuals, but **script kiddies** (hackers with little knowledge or experience who run scripts they didn't write themselves) and Black Hat crackers actually enjoy their conquests and the notoriety it brings.

Revenge People who feel that they were wronged, or that their cause or group was wronged, can easily talk themselves into performing unethical acts by using the simplistic notion that a badly behaved person, business, or government deserves to be treated as poorly as possible. It is the cracker's way of getting even. Groups such as Anonymous, an international and loosely aligned group of crackers that engaged in a number of high visibility attacks against political targets in 2011, have heightened the public's awareness of the increased potential for a cyber-attack following events that these groups might find offensive. Little is known about Anonymous other than that it appears highly fluid and basically leaderless, coming together in distinct groups for a particular action and then falling back to regroup for the next action.

Financial Gain Money is a very common motivation among all classes of hacker, from the security expert on contract or salary to the script kiddie stealing and selling credit card information. Plainly, the education required and the time spent learning the craft are not without cost, so it makes sense that there is some expectation of remuneration. Although some hackers do their work for free, citing the Hacker's Ethic that information should be free and freely shared to all interested parties, many others are in it for the cash.

Patriotism and Other Causes Some hackers, known as **hacktivists**, are motivated by patriotism or nationalism or other causes. Their goal may be to secure a network from cyber-criminals. Alternatively, they may want to attack a network to disrupt services, thereby causing fear among specific "enemy" populations and communities.

Governments can engage in hacking as well. **Stuxnet**, a computer worm that seeded malware-infected USB drives in cars parked outside Iranian nuclear plants, is one of the better known examples of state-sponsored hacking. There, the goal was to break into the plants' centrifuges. In a paper written for a U.S. Army War College publication, Timothy Thomas has suggested that China has several state-sponsored schools that train students to become experts in the art of cyber-terrorism.⁶ Brodsky has pointed to the increased dependence on **SCADA (Supervisory Control and Data Acquisition)** systems to run critical infrastructure, which makes them a potential target of cyber-terrorism.⁷

Ethical Hacking

Most professions have ethical codes that bind their members into a set of shared values and help them gain the public's trust. The profession of network security is no exception, but it is still emerging from a set of conflicting values that arose from the two communities it draws on: the hobbyist/student community and the professional community (those on the IT career track). Many individuals involved in the profession, especially those who come from business rather than technical backgrounds, believe they need to distance themselves from the communities they (and most of the better penetration tools) came from. That's one of the causes within the profession: to differentiate the bad hackers who threaten the networks from good hackers who are paid to protect them. Coming up with a set of distinctions that distinguish

the ethical hacker from the unethical cracker will help the network security profession present to the world the benefits that it brings to society.



Evolution of Hacking

In the 1940s, universities, government, and large businesses started using computers, but few people knew about them. There were no computer science students. Most of the professionals who worked with computers used them to solve complicated mathematics problems. The modern concept of hacking began in the late 1950s, when students at the Massachusetts Institute of Technology (MIT) started using their access to the IBM mainframe housed at MIT to work on new programming languages and other experiments outside of their regular classes. This was not antisocial or illegal behavior, but the students, while developing their skills, became a community of hackers as well. In the 1950s, “hacker” was a word for a hobbyist in any technical area.

The students used their unsupervised computer time to experiment, to find new ways of solving problems, and to invent applications that did things in a new computerized way. These early hackers had no malicious intent. They simply believed that there was always room for improvement. And so, when a new, simpler, more elegant solution was found, it was published widely and tested by many. There was little predefined structure to the experimentation. Many of the students took as much pride in their collaborative solutions as they did in their individual achievements. Given the open access and freedom they had, many of them indulged in programmed pranks or discovered ways to access others’ personal files to edit their code. But these pranks were published just as widely as the more socially acceptable results.

The first password hacks were a response to the Compatible Time Sharing System (CTSS), which was developed in the early 1960s and first loaded onto an IBM mainframe, again at MIT. This application enabled the safe sharing of computer time by different users so that all the processor’s cycles were used and there was no idle time. Usernames and logons kept people from anonymously accessing the computer, but this flew in the face of the freedoms that students had previously enjoyed. Some responded by trying to guess usernames and passwords. Finally, they broke into the CTSS system.

In the 1970s, a new sort of hacker, the phone phreak, appeared. Phone phreaks used various methods, collectively called **phreaking**, to access telephone networks in order to make free calls from pay phones. Eventually, they began combining traditional phreaking tools with computer programming languages. One popular phreaking program was Blue Beep. It works with MS-DOS and shell prompts of Windows, using PASCAL and other assembly languages. Its features include creating digital tones, controlling trunk lines, and scanning telephone exchanges.

In the 1980s, phreaks discovered that any server with a modem could potentially be entered. **War dialers** were developed to search for open modems. Once a hacker gained access to one server, it was often possible to access another server through the dedicated lines the servers shared. This was one way to access the fledgling Internet and its precursors—i.e., the bulletin boards run by CompuServe and AOL.

As personal computer prices dropped and users became more common, hacker communities grew, too, and the term “hacking” started to take on a new connotation. Hackers were no longer just young, socially inept males with an insatiable curiosity about computers. They

were now joined by malicious individuals who attempted to break into and damage sensitive corporate and government networks that they accessed through the use of modems.

Given that automation was the whole reason for computers in the first place, it is not surprising that, in the 1980s, people started creating applications that could spread themselves automatically (or nearly automatically) over the Internet and through e-mail systems. Viruses, worms, and Trojans started appearing in 1988. The thrill of having such simple codes wreak havoc on servers and workstations was intoxicating, and hackers have continued to develop viruses and worms to this day. In fact, they have turned to even more hazardous code over time because it is easy to find existing resources that need just minor modifications and little skill to alter, then send them back out. Examples of these viruses are the Bagel virus (which had dozens of variants), Nimda, and Code Red.

The presence of the resources and tools to create malware is a long-term problem that shows little evidence of resolving in the near future. Viruses are indiscriminate in their damaging effects, and any script kiddie can set one loose. Also, virus code is available on the Internet, and skilled crackers can use such code as a starting point to develop better ways to break into more specific targets.

Hackers' antisocial actions ultimately made it difficult to hold on to the original definition of "hacking"; people started to use the label "hacker" to describe computer experts working with malicious intent. This stereotype persists today and has raised the need for security experts to distance themselves from the criminal—the same way lawmen in the old West used their tin badges to separate themselves from the outlaws.

Vendor-Neutral Security Certifications

Table 1-1 shows the existing vendor-neutral security organizations and the certificates that they sponsor.

Table 1-1 Information security certification organizations and offerings

© Cengage Learning 2014

Certification Organization	Certification	Area of Focus
CompTia	Security+™	General security overview
General Information Assurance Certification (GIAC)	GIAC Information Security Fundamentals (GISF)	Security administration
	GIAC Security Essentials Certification (GSEF)	Security administration
	GIAC Information Security Professional (GISP)	Security management
	GIAC ISO-27000 Specialist (G2700)	Security audit
	GIAC Certified Forensics Examiner (GCFE)	Forensics
	GIAC Certified Firewall Analyst (GCFW)	Security administration
	GIAC Security Leadership Certification (GSLC)	Security management
	GIAC Legal Issues (GLEG)	Security legal
	GIAC Systems and Network Auditor (GSNA)	Security audit
	GIAC Secure Software Programmer-.net (GSSP-NET)	Software security
	GIAC Certified Forensics Analyst (GCFA)	Forensics

**Table 1-1 Information security certification organizations and offerings (continued)**

Certification Organization	Certification	Area of Focus
	GIAC Certified Intrusion Analyst (GCIA)	Security administration
	GIAC Certified Project Manager Certification (GCPM)	Security management
	GIAC Secure Software Programmer-JAVA (GSSP-JAVA)	Software security
	GIAC Certified Incident Handler (GCIH)	Security administration
	GIAC Certified UNIX Security Administrator (GCUX)	Security administration
	GIAC Certified Enterprise Defender (GCED)	Security administration
	GIAC Certified Penetration Tester (GCPT)	Security administration
	GIAC Web Application Penetration Tester (GWAPT)	Security administration
	GIAC Assessing Wireless Networks (GAWN)	Security administration
	GIAC Exploit Researcher and Advanced Penetration Tester (GXPN)	Security administration
	GIAC Reverse Engineering Malware (GREM)	Forensics
International Information Systems Security Certification Consortium (IS2)	Certified Authorization Professional (CAP)	Security certification
	Certified Information Systems Security Professional (CISSP)	Security management
	CISSP Information Systems Security Architecture Professional (CISSP-ISSAP)	Security design
	CISSP Information Systems Security Engineering Professional (CISSP-ISSEP)	Security engineering
	CISSP Information Systems Security Management Professional (CISSP-ISSMP)	Security management
	Certified Secure Software Lifecycle Professional (CSSLP)	Software security
	Systems Security Certified Practitioner (SSCP)	Security administration
International Council of E-Commerce Consultants (EC-Council)	Certified Ethical Hacker (CEH)	Penetration testing
	Computer Hacking Forensic Investigator (CHFI)	Forensics
	EC-Council Certified Security Analyst (ECSA)	Penetration testing
	Licensed Penetration Tester (LPT)	Penetration testing
	EC-Council Network Security Administrator (ENSA)	Security administration
ISACA	Certified Information Systems Auditor (CISA)	Security audit
	Certified Information Security Manager (CISM)	Security management
	Certified in the Governance of IT (CGEIT)	Security management
	Certified in Risk and Information Systems Control (CRISC)	Security risk management

part of a defensive strategy, organizations may want to hire external security professionals to try to hack their systems. They can derive further benefits from hiring ethical hackers to perform security audits, which provide solutions as well as identify potential problems.

Ethical hackers work to protect all IT areas—Web servers and shared printers as well as e-mail from end to end. The widespread adoption of smartphones, tablets, and other mobile devices as well as the move to the “cloud” are only the most recent additions to the information assets that organizations are responsible for. These organizations have also adopted social media and technically integrated Enterprise Resource Planning (ERP) systems that have blurred the boundaries of the traditional internal network, which has only increased the importance of the work of professional ethical hackers. Hackers must have experience in software engineering, network engineering, and system security. They must strive to increase their knowledge of tools and techniques to protect their networks and to check for forensics evidence when those networks are attacked.

Chapter Summary

- Computer cracking is illegally hacking into a computer system without the permission of the system’s owner.
- Hackers are commonly classified in two groups: White Hat, or “good” and ethical hackers, and Black Hat, or “bad” and malicious hackers.
- The eight major profiles of hackers include novices, cyber-punks, internals, old-guard hackers, coders, professional criminals, information warriors (aka cyber-terrorists), and hacktivists.
- Ethical hackers and unethical hackers use the same reading materials and techniques; what distinguishes between the two groups is simply the permission of the network owner and the choice of whether to defend or attack.
- Hackers may be motivated by a love of difficult challenges, curiosity, a desire for recognition, a desire for financial gain, a need for revenge, or patriotism.
- The modern concept of hacking began in the late 1950s when some students at MIT started using their access to the MIT mainframe in order to work on new programming languages and other experiments outside of their regular classes. With the advent of logon accounts and passwords in the 1960s, hackers went from exploring computers to hacking passwords. The 1970s saw the rise of the phreaks, and the 1980s saw a tremendous growth in computer crime and abuse with the introduction of viruses, worms, and Trojan horses.
- Although there are several vendor-neutral and vendor-specific certifications available to computer security professionals, there is no national certification standard.
- Professional security experts, technologists, and hackers must develop a public code of ethics. Without the assurance a code provides, potential clients may resist employing ethical hackers who could defend their networks and computer systems from crackers.
- An ethical hacker is a security professional who applies hacking skills for defensive purposes. This person accesses a computer system or network with the authorization of the system’s owner and without causing damage to the system.



Key Terms

cloud computing Computing that occurs beyond the edges of the trusted network.

cracker Someone who engages in cracking.

cracking The act of illegally hacking into a computer system without the permission of the system's owner.

hacker A term originally meant to describe a programmer or someone skilled at computers and code writing. The term has evolved and is sometimes used as a more pejorative term to describe a cracker.

hactivist Hacker or cracker who is motivated by patriotism, nationalism, or some other deeply held civic or social belief and who may either secure networks from cyber-criminals or disrupt services, thereby causing fear among specific "enemy" populations and communities.

malware infection When a host computer or device is surreptitiously loaded via various routes, including infected attachments or from visiting malicious Web sites. The objective of malware is to activate functionality on the device that is not sanctioned by the device owner. Malware can take many forms, including viruses, Trojans, worms, and rootkits.

phreaking Cracking the phone network to make free long-distance calls, for example. Also refers to security cracking, especially (but not exclusively) on communications networks.

SCADA (Supervisory Control and Data Acquisition) Systems designed to run critical infrastructure.

script kiddies A subset of hacking enthusiasts who, having little knowledge or experience, find and run scripts that others have made available through various media. Script kiddies are universally despised by experienced programmers. When an individual is singled out as being or acting like a script kiddie, this is a derogatory usage.

Stuxnet A computer worm that seeded malware-infected USB drives in cars parked outside Iranian nuclear plants with the goal of breaking into centrifuges.

war dialer A script that tells a modem to dial a range of phone numbers and then identifies those that are connected to remote computers. The phone number range is defined by the user, then the program proceeds to dial these numbers, one after the other, attempting to establish a remote connection.

Review Questions

1. Using the White Hat/Black Hat model, which kind of hacker is more likely to create a Web site to teach new hackers how to hack a network?
2. Using the White Hat/Black Hat model, which kind of hacker is more likely to work as a network administrator?
3. Using the White Hat/Black Hat model, which kind of hacker is more likely to be politically motivated?

4. Using the White Hat/Black Hat model, which kind of hacker is more likely to sell credit card numbers to criminals online?
5. When presenting a talk to a group of business leaders, are you more likely to use the White Hat/Black Hat model or the Hacker Profiles model to explain the dangers posed by hackers? If the business leaders were the chief information officers of their respective companies, would you reverse your decision? Write a short essay explaining your answers.
6. If your Web site is hacked and all the pages call up the same anti-war slogan and picture, which profile of hacker has hit your site?
7. If it is discovered that the CEO's e-mail browser is set to automatically copy all her outgoing mail to an unknown account called *asmith@thecompany.com*, what profile of hacker is probably responsible?
8. Which hacker profile is most likely to try out attack scripts found on the Internet "just to see what happens"?
9. What is the name for a group of compromised computers that can be used in a distributed denial of service attack?
10. What are the motivations for the hacker profile "professional criminal"?
11. A security tester can make a network impenetrable. True or False?
12. An ethical hacker is a person who performs most of the same activities a cracker does but only late at night. True or False?
13. The System Administration, Network, and Security (SANS) Institute offers training and IT security certifications through Global Information Assurance Certification (GIAC). True or False?
14. The GIAC program offers a certification that focuses on reverse-engineering malware. True or False?
15. In the United States, all the state legal systems view port scanning as noninvasive or nondestructive in nature and deem it legal. True or False?
16. According to the Hacker Profile model, old-guard hackers brag incessantly about their successful exploits. True or False?

Match each of the following terms with the correct statement below.

- a. script
 - b. port scanning
 - c. novice
 - d. ethical hacker
17. Name a way to find open ports on a system.
 18. Who copies code from knowledgeable programmers instead of creating the code himself/herself?

19. Name the set of instructions that runs in sequence to perform tasks on a computer system.
20. Who is sometimes employed by companies to perform penetration tests.



Hands-On Project



Project 1-1

In this project, you set up the Linux computer that you will be using in many of the projects throughout the book. There are a variety of free tutorials available on the Internet that will help you with this task. Entering the name of the Linux variety you want to explore in your favorite search engine, followed by the term “installation tutorial,” should reveal an array of resources that will be useful in this exercise as well as those coming in subsequent chapters.

You need the following:

- An x86 computer with a minimum of 256MB RAM, the equivalent of a Pentium III 900 MHz processor or better, a 20GB hard drive, a high-speed cable or DSL phone modem, and a 10/100 Ethernet network interface card. Please note that these specifications should be viewed as minimum requirements; you will get better performance if you have more RAM, a faster processor, and so on.
- A current version of a popular, robust Linux distribution, such as Fedora, Red Hat Enterprise, CentOS, Mandriva, SUSE, or Ubuntu. The hands-on projects in this book assume an installation of Fedora Core 6, and the steps are written accordingly. However, other Linux distributions can be used, with minor modifications to the steps, as needed.
- An Internet connection
 1. Perform a default installation of the Linux OS. For the purposes of this book, you won't need to review or customize partitions, and you can accept the default partitioning scheme that the installation program selects.
 2. When installation is complete, use the OS's package manager to install any available software updates. This will help ensure that your system contains important security updates and bug fixes. For example, in Fedora, you can start the update process by entering `yum update` at a Terminal window (you'll need to log in as root) or by clicking **Applications**, pointing to **System Tools**, and clicking **Software Updater** to run the Software Updater program.

References

1. Computer Security Institute. “CSI 2010/2011 Computer Crime and Security Survey.” *gocsi.com*. Retrieved April 9, 2012 @ <http://gocsi.com/survey>.
2. Verizon. “2012 Data Breach Investigations Report.” *verizonbusiness.com*. Retrieved April 9, 2012 @ www.verizonbusiness.com/about/events/2012dbir/index.xml.

3. Bednarz, A. "Profiling Cybercriminals: A Promising but Immature Science." *Network-World* 29 November 2004. Retrieved April 9, 2012 @ www.networkworld.com/supp/2004/cybercrime/112904profile.html.
4. Mitnick, Kevin. "They Call Me a Criminal." *Guardian Unlimited*. February 22, 2000. Retrieved April 9, 2012 @ www.guardian.co.uk/Archive/Article/0,4273,3966123,00.html.
5. Black Hat. "Black Hat Briefings and Training: About Black Hat." *blackhat.com*. Retrived April 9, 2012 @ <http://blackhat.com/html/about.html>.
6. Thomas, T. "Google Confronts China's Three Warfares." *Parameters*. Summer, 2010. U.S. Army War College.
7. Brodsky, J., and R. Radvanovsky. "Control Systems Security." *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*. Ed. T. Holt and B. Schell. IGI Global, p. 187.

- Operating systems
- Network structure
- Hardware configuration
- Available services
- Business strategies
- Employee phone lists
- Staffing structure of the organization
- Internal newsletters
- All available published information about the company, either on its Web site or by other writers

These types of information allow a hacker to figure out the targeted organization's security weaknesses and identify the best possible techniques and tools to conduct attacks.

Reconnaissance is not illegal by definition, nor are many specific reconnaissance techniques. That's because these kinds of activities do not result in actual damages, for which the organization would be able to prosecute. The following sections sort through the various areas of reconnaissance, identifying which are legal and which may prove illegal or unethical.

Legal Reconnaissance

It is completely legal to look up all the information that's available about a company on the Internet, including its phone numbers, office hours, and addresses. In addition, many organizations publicize very detailed information about their technical environments when seeking trained IT staff; looking up this information is legal as well. Calling the organization with a problem that requires customer service assistance is legal (even if it is a made-up problem). Interviewing a member of the staff for a school project is legal. Physically entering a facility, including attending a tour of the facility, is legal. Making friends with somebody who works there or used to work there is legal. Company representatives would have to be exceptionally paranoid not to answer the phone "just in case it is a hacker performing recon." All these methods—and many others like them—are completely legal and are done for various reasons all the time.

Questionable Reconnaissance

Local laws vary, but in much of the world, performing a passive port scan is legal. Reading the names on the mail that's sitting on a mail cart or scanning a document that's lying on a desk may be legal. Picking up trash in the parking lot and looking at it before you toss it out or hand it off to a company representative is probably legal. Picking up a copy of the company's employee newsletter is probably legal. Asking for a phone list or a business card or product specs is probably legal. Looking through a garbage can is probably legal. Conducting a stake-out to discover the movements of key individuals may be illegal; however, if the hacker is not trespassing or otherwise attracting attention, it may be legal. **War driving**—checking for unsecured wireless networks—is legal in some places and not in others. Leveraging these legal types of activities can often be just as fruitful, in terms of providing a toehold into the organization, as other activities that may cross the line into illegal or unethical behavior.



Illegal Reconnaissance

There are a number of plainly illegal reconnaissance techniques. Developing a “front” company and acting as a representative of that company for the specific purpose of robbing or defrauding a target company, in addition to being quite expensive and time consuming, is probably illegal. Stealing garbage is illegal in some locales. Entering a home or office to look for information is illegal, although it often goes undetected if nothing is removed. Surreptitiously installing a **keylogger**—a tool that records users’ keystrokes—on a vulnerable machine is illegal. Leaving a **sniffer**, which intercepts and reads data packets, on a network is illegal.

Impact of Context on Reconnaissance

Context is important in ethical hacking. For example, ethical hackers conducting criminal or homeland security investigations may engage in some reconnaissance activities that would normally be considered illegal under other circumstances. Although these special circumstances may be legally sanctioned, those with an interest in personal privacy and liberty may consider them unethical, regardless of the context.

When practicing reconnaissance, it is important to remember that any information about the target is potentially of value. During the collection phase of reconnaissance, sanctioned or ethical hackers are not always able to predict how that information will be used. Therefore, hackers strive to gather every detail—all e-mails, passwords, phone numbers, and codes—and then apply different scenarios or contexts to leverage the information that is collected.

Depending on the technology used and the nature of the investigation, reconnaissance methods fall into three categories: social engineering, dumpster diving, and Internet footprinting. Each of these categories is composed of various methods that are variously risky and variously legal. Hackers use these methods, together or separately, to collect information about their targets.

Social Engineering

Social engineering involves an act of deception on the part of an attacker, which is meant to trick well-meaning individuals into providing access to unauthorized information or systems. Social engineering is typically considered unethical behavior but is sometimes used by ethical hackers as part of a penetration test.

Social engineering works, for the most part, because people are trusting and want to be helpful, which is part of our social conditioning. Suspiciousness and selfishness are not traits we teach our children, nor do most adults cultivate those traits. But being trusting and helpful opens an avenue of risk. Security policies and vulnerability checks do provide some basic and limited protection, but humans remain the weakest link in the security chain. Individual employees must be responsible for protecting their usernames and complex passwords; for securing their paperwork, files, and phone conversations; and for carefully selecting their circles of people they can trust.

Kevin Mitnick, a once-notorious, now well-respected hacker, made up for his lousy technical skills with some sophisticated social engineering skills. In his book *The Art of Deception*, Mitnick wrote, “Social engineering uses influence and persuasion to deceive people by

convincing them that the social engineer is someone he isn't, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology."¹ Sometimes, social engineering is only part of an attack. The infamous ILOVEYOU worm attack back in 2000 was caused by a virus, but it also involved social engineering, exploiting the curiosity that causes people to click on an e-mail attachment.

The success or failure of social engineering depends on the ability of hackers to manipulate human psychology, contacts, and physical workstations. Training and employee-awareness programs are critically important to reduce social engineers' ability to manipulate others.

Social Engineering Techniques

To access information about individuals, a social engineer must gain the trust or acquiescence of that person. This is done by deploying any of the following social engineering techniques:

- Impersonation
- Bribery
- Deception
- Conformity
- Reverse social engineering

Impersonation Impersonation can occur at an individual level, such as pretending to be Tom Cruise to get into a cool nightclub, or it can occur on a functional level, such as dressing like a service person to get past the security controls at Disney World. On the individual level, posing as an actual employee requires at least some of the ID information connected to that person. This can be pretty difficult to acquire and has the drawback that you might encounter somebody who knows the person you're impersonating. Functional-level impersonation is easier and may require less preparation. In either case, the hacker poses as a legitimate user or an employee who has the authority to collect information.

Examples of functional-level impersonation include:

- Approaching a user, claiming to be a system administrator or an IT support executive, then asking for passwords
- Wearing a baseball cap with the name of a local phone company on it and dressing as a phone company technician to get into a locked wiring closet
- Making a phone call to state that the system is acting erratically and that the victim must authenticate his or her username and password for verification
- Posing as a flustered, uncertain, but legitimate user and making a phone call to a help desk to ask for information
- Calling the third-shift sysadmin at 6:30 a.m. claiming to be the IT director (who never arrives at the office until 10:00 a.m.) and requesting that a specific line of code be run on the command line of the mail server

Before engaging in this kind of social engineering, a hacker usually performs basic research about the target company to avoid creating suspicion. It is easier to engage in this kind of impersonation in larger and more geographically diverse organizations than in smaller organizations where employees are more likely to know one another.



Bribery Bribery can be an effective way to collect information. Here, the hacker pits an employee's greed against his or her loyalty to the organization. Once a bribe has been accepted, blackmail is a common tactic for keeping the target employee working for the hacker. While looking for victims, a social engineer asks the following questions about employees:

- Do they work at a level of the company that might provide useful information?
- Are they in financial difficulty?
- Are they addicted to gambling, alcohol, or drugs?
- Are they unsatisfied with the organization?
- Are they focused on short-term gains with the company?
- Are they morally compromisable?

Bribery is a time-consuming technique that requires a lot of research on the target individual. There is also a potentially expensive front-end matter to consider. During the research, the hacker will probably be required to invest time and resources in the person or persons being bribed. The major risk to bribery is that the employee, though ready and willing to perform, is unable to provide any useful information—or that they may change their mind, either before or after that segment of the plan is complete. The hacker's risk level stays high, and there is at least one individual within the organization who knows some foul plan is in effect.

Deception Deception involves actually joining the organization as an employee or consultant. This pits the “virtuous” hacker against the “evil” company and requires a good helping of self-delusion on the part of the hacker.

Conformity This method depends on people's tendency to believe that they are “typical” and that an apparent similarity between themselves and other (unknown) persons is an actual similarity. The attacker may use this sense of conformity to convince victims that they have a lot in common and that they share the same values. Establishing this sense of rapport is used to gain the confidence of the victim. Once the desired information is obtained, the attacker will likely disengage. This is another area that an ethical hacker may choose to pursue as part of a penetration testing engagement. If so, it should be done with the knowledge that those who are the target of attention are likely to feel victimized regardless of the fact that the ethical hacker had no malicious intent.

Reverse Social Engineering Reverse social engineering is a sting operation in which the hacker pretends he's an authority figure invested with the power to solve peoples' problems. The thing is, the problems were caused by the hacker himself. Here's how it works:

1. First, the hacker manufactures a problem, such as a denial of service (DoS) attack that shuts down the network for a time.
2. Then, the hacker advertises himself as an expert who can solve this sort of problem. The victim might be prompted to communicate with the hacker for relief, and the hacker uses this opportunity to solve the victim's problem.

3. Now, the hacker is believed to be a trusted assistant or expert in the field of network security, and he is therefore given more access to the network in question, including many critical systems.
4. Finally, the hacker is able to collect information from users and perhaps install hidden running processes on the systems to which he now has access.

Most social engineering attacks are opportunistic; the hacker uses whatever technique he or she thinks fits the situation. For example, impersonating a user and calling a help desk for assistance might not be the way to go if the aim is to collect confidential information from a sysop. All social engineering techniques are affected by ease of physical entry into the target organization or of communication with the victims within the organization.

Physical Intrusion

Physical intrusion refers to social engineers actually entering an organization's premises with the sole purpose of collecting information. The social engineering aspect of physical intrusion results from the use of impersonation or other forms of deception to gain access to areas to which the attacker should not be entitled.

First, the social engineer must scope out the premises. "Casing the joint" usually includes:

- Learning the organization's schedules
- Knowing the floor plan of the building or buildings
- Engaging in surveillance or research to understand the existing security procedures

Learning an organization's schedules or patterns includes knowing which people are likely to be there at any one time, their jobs, and their work styles. It is also good to know who holds which keys and where these people are at various times of the day. The more a hacker knows about the usual behaviors of the people who work in the building, the less likely he or she will arouse suspicion or set off alarms.

Failing to secure a building's floor plans might provide an attacker with an opportunity to get to the right place quickly while under stress. As in any complex plan, the less left to chance and improvisation, the better the results.

Knowing the security measures that are in place also helps hackers know where the security system breaks down. Social engineers normally have close contact with employees on the inside before entering an organization's building, and they can get a lot of baseline information from those employees. A friendly employee is likely to be unaware of the useful information he or she is imparting and will consider such divulged information to be just "office war stories." However, this information lets the hacker know the company's physical security, network security, and response policy to intrusion. There is no reason to assume that a single hacker cannot have multiple contacts within an organization; he or she could have a network of interested friends inside a company's firewall.

Once the hacker acquires some information about the organization, he or she can develop fake identification cards. Many companies use a laminated card with the employee's information on it. This is very easy to duplicate with a word processor and a laminator—at a copy shop, for example. Before creating the fake ID, the social engineer must decide whether to pose as an employee, a contractor, or an authority figure. Large companies with lots of employees, contractors, and social churn are the easiest to infiltrate. Because nobody is



Internet sites are often used as platforms for phishing expeditions, as well as for phony “prize-distribution” ploys. It is easy to make professional-looking Web sites in very little time—so easy, in fact, that it is sometimes difficult to tell the phishing sites from the genuine ones. Users should check if the form is an https page, which indicates it uses encryption to guard transmitted data. Fake sites don’t tend to care if data is at risk during transmission and so will not provide any safeguards. Users should not send sensitive data to sites with which they are not well acquainted. Phishing sites take advantage of users’ tendency to employ the same username and password for many similar sites, then they go looking for the other sites to which the users are subscribed. The level of sophistication that phishers bring to their techniques is such that even information security professionals can fail to identify a malicious link, which is why phishing is one of the more common risks experienced by today’s organizations.

Instant Messaging Instant messaging hacking scripts are prevalent in many public IM platforms. Here, the social engineer attempts to befriend the victim to gather information and/or introduce the victim to a Web link he might want to visit. Usually, these sites are pornography related. Actual people usually contact one another through mutual friends or by searching profiles for pertinent keywords. Random contacts that are actual people with legitimate interests declare their intentions outright: “I saw on your profile that you like model trains. I do, too. How do you make miniature farm animals for your trains?” They might be selling toy horses, but they say that up front. In contrast, there are automated scripts that run on ICQ and Yahoo IM. In some cases, it is possible to have a 20-minute IM session with a set of automated responses! But they are easy to catch as well. Because they are automated, they are not able to respond to open-ended questions, such as “What kind of tea do you like?” Their responses are noticeably inappropriate, so it is easy to block them early in the conversation. It is also possible to set the IM client to accept only contacts from an approved list.

Telephone Communication Social engineers have an array of tools with which to exploit telephone communication for malicious purposes. They may manipulate background sounds and their own voices to produce the required effect—for example, using a light, feminine voice instead of a brusque voice with a thick accent. Social engineers also have tools to generate false entries in caller-ID technology, making it appear that a call is coming from a legitimate source.

Help desk personnel are vulnerable targets because they have been granted more access to information than the average employee and are required to give information to people quickly, with a minimum of digression. In fact, they are often under time pressure to successfully answer as many calls as they can.

When calling a particular employee, it can be more effective to call another employee and be transferred to the potential victim. This makes the caller appear more trustworthy than if she had called the victim directly.

Social engineers often impersonate technicians who contact target users to inform them, for example, that they may have been overbilled for telephone charges. After they convince the user to accept that premise, they ask for more personal information.

Countering Social Engineering

To prevent or mitigate social engineering, you must educate the users. Education must be included in your security policy, and new users must be made aware of the policy. All users in a system must take the following precautions to counter social engineering attempts:

- Do not provide any information to unknown people.
- Do not disclose any confidential information to anyone over the telephone without confirming the legitimacy of the person on the other end of the line.
- Do not type passwords or other confidential information in front of unknown people.
- Do not submit information to any insecure Web site.
- Do not use the same username and password for all accounts.
- Verify the credentials of persons asking for passwords, and recognize that authentic administrators often do not need your password to access your files.
- Keep confidential documents locked.
- Lock or shut down computers when away from the workstation.
- Establish protocols that require help desk employees to provide information only after they have gained proper authentication.



Dumpster Diving

Dumpster diving—the act of combing through an organization’s refuse—often provides the mother lode of sensitive information as well as actual hardware and software. Hackers look specifically for sales receipts and paperwork that contain personal data or credit card information. This information can be sold to others who will do damage with it, or it can be used by the hacker himself. Shredded documents can lead to data leaks when all the shredders are strip shredders and the resultant strips are disposed of in a single bag. Although cross-cut shredders are more secure, the complicated jigsaw puzzle they create can be reconstructed by whoever wishes to put in the time. Many people believe that all companies carefully shred and dispose of their personal information, but this is not necessarily true. In many places, documents considered less sensitive are dropped directly into publicly available receptacles. Drafts of letters, even mail-merge documents with hundreds of recipients, are routinely left whole in the trash. Company directory sheets, catalog lists, unused or misprinted labels, and policy manuals are not recognized as sensitive data, so they are left whole in the trash as well, but consider the consequences of a criminal retrieving this information. They are not concerned with whether the labels are printed properly; they are interested in the names and addresses, phone numbers, and employee IDs that appear there.

Importance of Proper Discarding of Refuse

An organization’s security policy must carefully specify what is sensitive information and what isn’t, and then specify how to treat refuse. Some documents may not be considered sensitive, like employee handbooks and company policy statements. But these can often tell hackers what kind of physical and network security to expect when doing an intrusion.

There are various ways to dispose of trash paper, such as using cross-cut shredders or locked trash receptacles. As a result of the Health Insurance Portability and Accountability Act (HIPAA) and similar federal legislation, such as the Sarbanes-Oxley (SOX) Act, a cottage industry of document-destruction services has emerged. These services involve backing trucks up to organizations, collecting locked bins, shredding the information, and then issuing certificates of destruction to the organization, both as a form of insurance policy against misuse of these documents and to provide evidence of compliance to regulators or auditors.

Old hardware cannot be shredded and takes up space; thus, these items are frequently thrown out, or given to employees to take home. Hackers search for outdated hardware, such as tapes, CD-ROMs, and hard disks. There are various tools available to hackers, such as forensics programs, that can restore data from damaged data-storage devices. Information recovery services such as Kroll have demonstrated that it is really physical destruction of storage devices that can best ensure that sensitive information cannot be recreated.

Prevention of Dumpster Diving

To prevent dumpster diving attacks or mitigate their value to the attacker, do the following:

- Develop a written recycling and trash-handling policy that is part of the overall security policy.
- Use the policy to develop a consistent, systematic method for handling trash.
- Demand that all papers be shredded. Cross-cut shredders with narrow cuts are the best because they minimize the possibility of reconstructing documents.
- Erase all data from tapes, floppies, flash drives, and hard disks. Because data can be recovered even from formatted hard disks and tapes, stipulate that the application that's adopted to erase media use at least government-approved wiping algorithms. These overwrite data with random data at least eight times, therefore minimizing hackers' success in salvaging information. Most effective, however, are those techniques that involve the physical destruction of the media.
- Don't simply break CD-ROMs, given that data can be recovered from broken disks. Place them in a microwave and heat them, which destroys the integrity of the substrate and makes the data irrecoverable.

Internet Footprinting

Internet **footprinting** is a technical reconnaissance method that interests budding hackers and network security specialists alike. Hackers like it because it is clean, legal, and safe; security specialists often choose it over all other methods of surveillance because of the increased avenues of information leakage experienced by modern organizations. This kind of profiling helps the social engineer understand the target system's Internet, intranet, and remote-access setups. It is easy to implement and almost undetectable by the victim.

There are five Internet footprinting methods:

- Social networking
- Web searching
- Network enumeration

- Domain Name System–based reconnaissance
- Network-based reconnaissance

Social Networking

The advent of social networking services such as Facebook and Twitter has created an array of potential risks to organizations. An example would be a network administrator who posts on his Facebook page that he is about to embark on a vacation. A hacker who reads that post can call the help desk posing as the network administrator with less chance he will be discovered. Another example would be a Human Resources employee who is having trouble filling a job position that calls for expertise in a less commonly used version of UNIX and therefore sends out a tweet asking members of the network to be on the lookout. Although this may be an effective way of identifying prospective candidates, it also provides a hacker with information about the technical specifics of the organization's infrastructure.

Web Searching

Internet footprinting involves collecting information about a target system, and today the majority of organizations have Web sites that contain crucial information. All the material on an organization's Web site is legally available, even if it is sensitive.

Hackers use a variety of Web-based resources to find information about potential targets:

- E-mail
- Search engines
- Hypertext Markup Language (HTML) source code
- Newsgroups
- Security-related Web sites
- Newsletters

None of the information contained in these sources is legally protected, although “invitation only” newsgroups and membership Web sites require authentication, from e-mail and IP address to full name and street address. Some membership sites are “pay sites,” meaning that there is a payment schedule to view the site contents. The fact that a site is a pay site does not guarantee that it requires a high level of authentication to achieve membership.

Search Engines People obtain relevant information from search engines by submitting simple queries. People with more knowledge can discover far more than basic information, however. For example, let's say a hacker wants to learn about an organization located in Atlanta. The hacker needs to collect as much information about the company as she possibly can, and the basics are available through search engines. Public information, which may seem harmless, can actually aid hackers.

There are hundreds of search engines available on the Internet; some of the most well-known ones are Google, Yahoo, and Bing. These search engines may provide the hacker bent on finding out about the Atlanta-based organization with valuable information about the organization's physical plant or its organizational structure, all while sitting halfway across the country. Prior to the 9/11 attacks, it was not uncommon for organizations to publish building diagrams and other highly sensitive information. Organizations have since



become increasingly sophisticated about security issues and are now much more likely to consider the security implications of information they publish on the Web.

Using a search engine, such as Google, to look for disgruntled employees of a targeted company might lead to information that allows the hacker to infiltrate the company. Consider the following search results:

- About 28,700,000 hits for “Google employer”
- About 224,000 hits for “Google employer terminated”
- About 1,190,000 hits for “Google employer fraud”

If you were trying to infiltrate Google itself, there might be something here. This is just an example of how any company or organization may be vulnerable to seemingly innocent Web searches.

The pages indexed on search engines and the refresh rates of the databases used vary widely. Many pages stay in a search engine’s indexes long after the actual pages are taken down, and some specialized search engines, such as the Wayback Machine (*www.waybackmachine.org*), keep copies of sites going back many years.

HTML Source Code You can view the source code of any Web page from the View, View Source (or Page Source) drop-down menu in your browser. In Firefox, the frames are also displayed on the page. Not all pages are useful, and pages displayed by server-side programming—such as ColdFusion, ASP.NET, JavaServer Pages (.jsp), or PHP Hypertext Processor (PHP)—are nothing like the code that produced them.

A hacker searches HTML source code for hints about a site’s organization that are contained in the comments entries. These may provide critical information about the target. For example, the HTML source code for a Submit button on a particular Web page could contain a comment specifying the database where the information about users is stored, or some hint about the username and password details. Knowing the format of usernames or passwords can be useful, just as knowing the site’s organization can be useful.

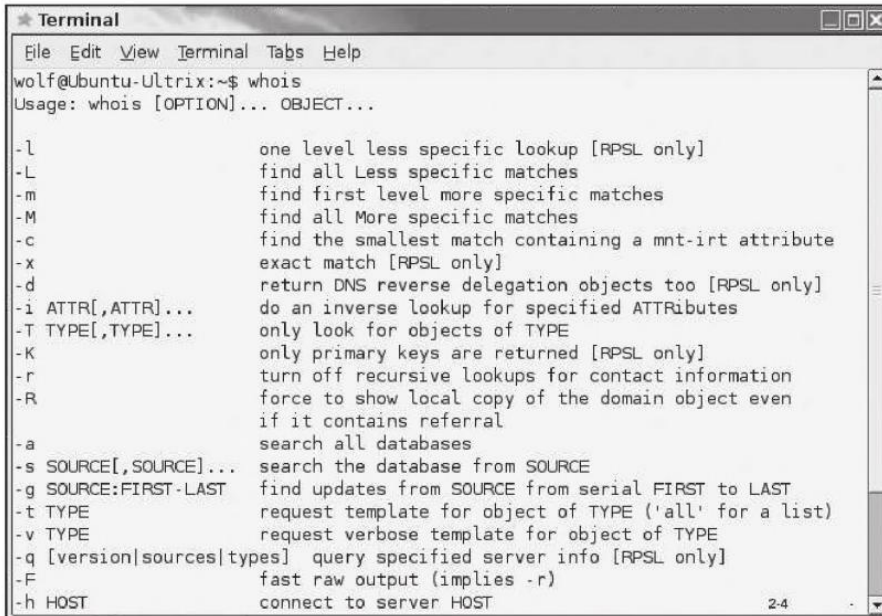
On your own Web site, you may wish to add a default or index page (e.g., ADatabaseSite/Admin/Modules/index.htm) in every subdirectory. This way, a blank index.htm page will appear when somebody attempts to test a subdirectory, rather than a list of the directory’s contents. This directory structure is from an open source PHP application. The designers put blank index.htm files in all the code folders, so even if a hacker got into the folder, there would be nothing for him or her to see. Files that tell Web spiders what to index and what not to index are designed to keep search engine spiders from indexing sensitive material, and they do not work if the spider is designed to index everything.

Newsgroups Newsgroups are a relic of the 1980s technology that used to constitute the Web. They are text-based online groups in which users discuss subjects that interest them. Newsgroups are part of an online bulletin board system called USENET, which contains

might be able to use that information to conduct social engineering attacks on the company or one of its contractors. Remember, trusted partner companies, clients, and contractors are all potential paths into a target company.

whois CLI Command The WHOIS Web application is also available at the command-line interface (CLI) of POSIX systems like UNIX, Solaris, and Linux. Use the command `whois options target`.

Figure 2-4 shows the `whois` command options.



```

Terminal
File Edit View Terminal Tabs Help
wolf@Ubuntu-Ultrix:~$ whois
Usage: whois [OPTION]... OBJECT...

-l          one level less specific lookup [RPSL only]
-L          find all Less specific matches
-m          find first level more specific matches
-M          find all More specific matches
-c          find the smallest match containing a mnt-irt attribute
-x          exact match [RPSL only]
-d          return DNS reverse delegation objects too [RPSL only]
-i ATTR[,ATTR]...
            do an inverse lookup for specified ATTRibutes
-T TYPE[,TYPE]...
            only look for objects of TYPE
-K          only primary keys are returned [RPSL only]
-r          turn off recursive lookups for contact information
-R          force to show local copy of the domain object even
            if it contains referral
-a          search all databases
-s SOURCE[,SOURCE]...
            search the database from SOURCE
-g SOURCE:FIRST-LAST
            find updates from SOURCE from serial FIRST to LAST
-t TYPE
            request template for object of TYPE ('all' for a list)
-v TYPE
            request verbose template for object of TYPE
-q [version|sources|types]
            query specified server info [RPSL only]
-F          fast raw output (implies -r)
-h HOST
            connect to server HOST
  
```

Figure 2-4 CLI view of the `whois` command (on Ubuntu Linux)

Source: Microsoft Paint

Domain Name System–Based Reconnaissance

When a Web site is established, the address bar shows the host name—for example, `www.somedomain.com`. This is also referred to as the “friendly name” because it is easily understood by humans. IP addresses used by TCP/IP are not as easily understood. The systems that run the Internet use only IP addresses—either the dotted decimal IPv4 address, such as `71.81.18.32`, or the IPv6 address, such as `2002:4751:1220::1/48`. Therefore, a host name has to be converted into an IP address in order for the requestor to connect to the requested host. DNS servers are responsible for resolving host names to corresponding IP addresses.

When you type a host name, the Web browser connects to the primary DNS server—either the DHCP-assigned DNS server or a manually assigned DNS server of the LAN administrator’s choice—to resolve the IP address. If the primary DNS server is not able to resolve the IP address, it sends the request to a remote DNS server, known as the secondary DNS server. When a secondary DNS server resolves the IP address, the primary DNS server updates its

database with that IP address mapping. This allows a primary DNS server to resolve the IP address the next time, without having to contact the secondary DNS server.

Network troubleshooters and hackers use various techniques to extract information about a DNS server and the host names that are resolved by that DNS server. The most important DNS-based reconnaissance techniques are DNS lookup and DNS zone transfer.

DNS Lookup DNS lookup tools help Internet users discover the DNS names of target computers. Hackers can perform this type of lookup based on either the host name or the IP address. There are several Web sites that provide DNS lookup tools. Here are their Web addresses:

- *www.dnsstuff.com*
- *www.network-tools.com*
- *www.networksolutions.com*

DNS Zone Transfer Every DNS server has a name space, known as a zone. A zone stores data about domain names. Zone transfer is a DNS feature that lets a secondary DNS server update its database with the list of domain names in another, primary DNS server. Zone transfer helps a secondary DNS server provide DNS services to users whenever a primary DNS server is not functioning properly.

An incorrectly configured DNS server may allow any Internet user to perform a zone transfer. The consequences of such activities are critical, because an Internet user with malicious intent can transfer the information in the zone and then use it to collect information for hacking purposes.

Hackers use the following commands to perform DNS zone transfers:

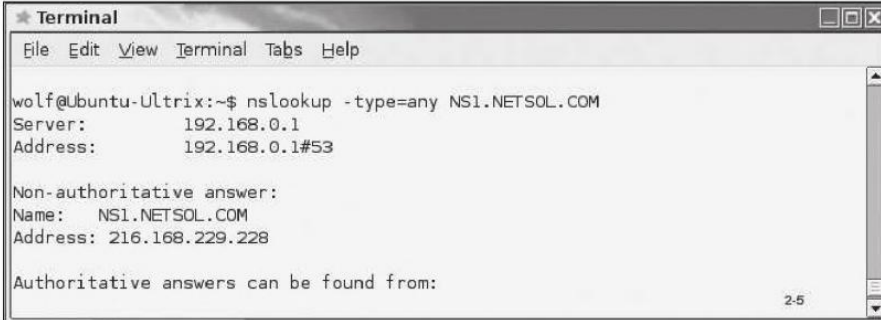
- `nslookup`
- `host`
- `dig`

***nslookup* command** The `nslookup` utility allows anyone to query a DNS server for information, such as host names and IP addresses. The `nslookup` command can be used in both Windows and Linux operating systems. If you execute `nslookup` without arguments or options, the program displays data that is related to the default nameserver. This is the interactive mode.

To use the `nslookup` command to gather information about hosts other than the default nameserver, you must specify the name or the IP address of the target host. This is the noninteractive mode. In noninteractive mode, the `nslookup` program scans the DNS server of the specified host and displays the located entries in the zone. You can use various arguments with `nslookup` to customize the information search. To gather information about hosts and IP addresses in a domain, simply use the following syntax:

```
Nslookup -type=any domain_name
```

Figure 2-5 shows an example of the `nslookup` command's output for one of Network Solutions' nameservers.



```

★ Terminal
File Edit View Terminal Tabs Help

wolf@Ubuntu-Ultrix:~$ nslookup -type=any NS1.NETSOL.COM
Server:          192.168.0.1
Address:         192.168.0.1#53

Non-authoritative answer:
Name:   NS1.NETSOL.COM
Address: 216.168.229.228

Authoritative answers can be found from:

```

Figure 2-5 Nslookup command output for *NetworkSolutions.com*'s NS1 nameserver

Source: Microsoft Paint

In the above syntax, the argument *any* directs nslookup to return all types of information about the target. Note that there is no MX or NX information here. That probably means that the mail and news servers are elsewhere. You can store the output of the nslookup program, the DNS zone information, in a text file on the local computer. To do so, use the following syntax:

```
Nslookup-type=any domain_name >file_name
```

host command The host command is a utility program that permits you to perform a DNS lookup. The basic host command gives you the information (in verbose mode) shown in Figure 2-6.



```

★ Terminal
File Edit View Terminal Tabs Help

wolf@Ubuntu-Ultrix:~$ host -v network solutions.com
Trying "network solutions.com"
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 16104
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;network solutions.com.          IN      A

;; ANSWER SECTION:
network solutions.com.  300     IN      A       205.178.187.13

Received 54 bytes from 192.168.0.1#53 in 60 ms
Trying "network solutions.com"
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 21572
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;network solutions.com.          IN      AAAA

;; AUTHORITY SECTION:
network solutions.com.  300     IN      SOA     ns1.net sol.com. dnsadmin.netw
solutions.com. 2006042004 7200 3600 604800 3600

Received 94 bytes from 192.168.0.1#53 in 26 ms
Trying "network solutions.com"
;; connection timed out; no servers could be reached
wolf@Ubuntu-Ultrix:~$

```

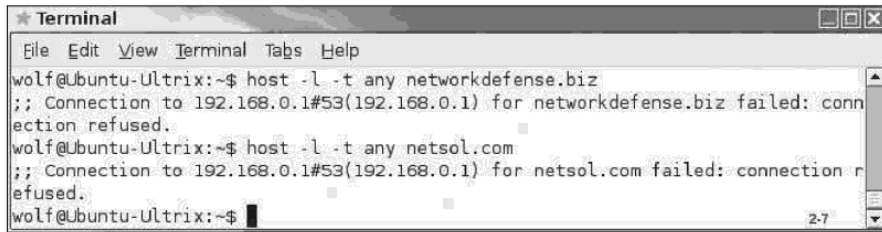
Figure 2-6 host command output for *NetworkSolutions.com*

Source: Microsoft Paint

You must specify the domain name as an argument in this command. A server name on which the host utility must search for information should also be specified, but the server name is an optional argument. If the server name is not specified, then the host utility checks the servers listed in the `/etc/resolv.conf` file. To perform a DNS lookup and zone transfer, use the following syntax:

```
host -l -t any domain_name
```

In this syntax, the `-l` option performs the DNS zone transfer activity, and the `-t any` argument helps the host utility collect all available information. Figure 2-7 shows an attempted DNS zone transfer.



```

* Terminal
File Edit View Terminal Tabs Help
wolf@Ubuntu-Ultrix:~$ host -l -t any networkdefense.biz
;; Connection to 192.168.0.1#53(192.168.0.1) for networkdefense.biz failed: connection refused.
wolf@Ubuntu-Ultrix:~$ host -l -t any netsol.com
;; Connection to 192.168.0.1#53(192.168.0.1) for netsol.com failed: connection refused.
wolf@Ubuntu-Ultrix:~$
  
```

Figure 2-7 Attempted DNS zone transfer

Source: Microsoft Paint

You can also direct the host utility to find and gather information about e-mail servers or nameservers. If you want to use the host utility to retrieve information about e-mail servers, use the following syntax:

```
host -l -t mx domain_name
```

To collect information about nameservers, use the following syntax:

```
host -l -t ns domain_name
```

To store this zone transfer information into a file, use the following syntax:

```
host -l -t any domain_name > file_name
```

dig command Domain information groper (dig) is another command used to collect DNS-related data. To collect this DNS information, use the following syntax:

```
dig domain_name any
```

DNS-based reconnaissance aids hackers in determining potential computers on the target network. Upon identifying potential target computers, hackers must also identify the network infrastructure of the target network.

Network-Based Reconnaissance

Network-based reconnaissance is the process of identifying active computers and services on a target network. To accomplish this, hackers use a variety of network utilities, such as ping, traceroute, and netstat.

ping Utility The ping utility is part of the Internet Control Message Protocol (ICMP) and helps to verify whether a host is active. It transmits data packets, known as ICMP echo packets, to the specified host. It then receives packets from that host. If the sent packet and received packet are the same, then the target host is active. ICMP is an integral component

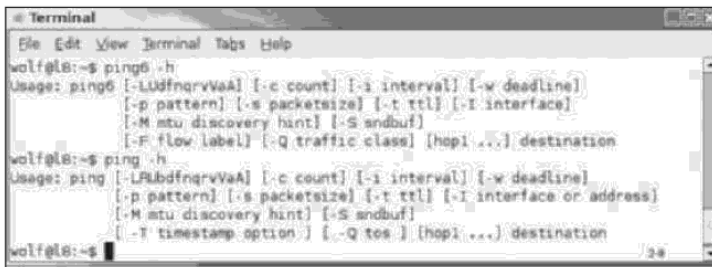
of a number of network management tools, which creates a tension between the risks and benefits of this tool. Some organizations have chosen to balance this risk by limiting the use of the ping utility to internal traffic while blocking it externally at the firewall.

When using the ping utility on a host, the host allots some of its memory resources to handle the ping query and return packets. This is used by network administrators and users to check if a specific host is reachable while troubleshooting network connectivity. This is also one of the avenues used by hackers to slow down the performance of specific targets by sending thousands of pings at the target. The target rises to the occasion by allotting all of its memory resources to answering pings.

The ping command is available for all platforms. There are two ping utilities available for a Linux or Unix machine: ping and ping6. The ping utility is the standard IPv4 version, and ping6 is the IPv6 version. To ping on a target host, use the following syntax:

ping target_host

In this syntax, *target_host* can refer to either the host name or the IP address of the target computer. Figure 2-8 shows the basic option sets for ping and ping6.



```

Terminal
wolf@id:~$ ping6 -h
Usage: ping6 [-LldfnqrvaA] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface]
            [-M mtu discovery hint] [-S sndbuf]
            [-F flow label] [-Q traffic class] [hop1...] destination
wolf@id:~$ ping -h
Usage: ping [-LldfnqrvaA] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
            [-M mtu discovery hint] [-S sndbuf]
            [-T timestamp option] [-Q tos] [hop1...] destination
  
```

Figure 2-8 Option sets for ping and ping6 utilities

Source: Microsoft Paint

You can use three commands to find a file in UNIX/Linux. The `whereis` command shows you where the files appear in your PATH (the directories in which you are allowed to read, write, or execute an application or other file). The `which` command displays the location of the application that will execute when you type its name on the command line. (Both of these commands, along with their outputs, are shown in Figure 2-9.) There are many reasons you might find multiple executable files with the same name—for example, you might be developing an application and have multiple versions in test. However, the default executable (especially those like *ping*, which are installed by default on most POSIX systems) will be in the PATH of almost all users.



```

Terminal
wolf@id:~$ whereis ping6
ping6: /bin/ping6 /usr/share/man/man8/ping6.8.gz
wolf@id:~$ whereis ping
ping: /bin/ping /usr/share/man/man8/ping.8.gz
wolf@id:~$ whereis ping6
ping6: /bin/ping6 /usr/share/man/man8/ping6.8.gz
wolf@id:~$ which ping
/bin/ping
wolf@id:~$ which ping6
/bin/ping6
wolf@id:~$
  
```

Figure 2-9 The `whereis` and `which` commands

Source: Microsoft Paint

- Social engineering works because people are, for the most part, trusting and helpful. The success or failure of social engineering depends on the hacker's ability to manipulate human psychology, contacts, and physical workstations. Social engineering techniques include impersonation, bribery, deception, conformity, and reverse social engineering. All of these techniques are accomplished through physical entry into the target organization or through communication with users at the target organization.
- To counter social engineering, organizations must establish security policies and conduct mandatory security training. Users must act as a human firewall against intrusion by protecting confidential information, paying attention to their surroundings, and noting any unusual interactions.
- Dumpster diving can provide hackers with sensitive information as well as hardware and software. Discarded paper should be shredded, ideally with a cross-cut shredder, and kept in locked dumpsters. Data from tape, floppy disks, hard disks, and CD-ROMs should be erased and destroyed before it is discarded. An increasingly common approach involves hiring external experts to assume responsibility for document destruction, which gives organizations a degree of risk transference as well as mitigation.
- Internet footprinting methods include: exploitation of social networking applications, Web searching, network enumeration, DNS-based reconnaissance, and network-based reconnaissance. These are the most frequently used methods of surveillance, attractive to hackers because they are clean, legal, and safe.
- The advent of social networking services such as Facebook and Twitter has created an array of potential risks to organizations, whose members may inadvertently provide useful organizational information.
- During Web searching, hackers collect information about a target organization by reading Web pages produced by that organization and other online documents about the organization. The hacker's research tools may include search engines, HTML source code, newsgroups, security-related Web sites, and newsletters.
- Network enumeration is the process of identifying domain names and other resources on the target network. Using a tool called WHOIS, hackers can gather information such as IP addresses and contact names.
- DNS-based reconnaissance uses information available from DNS servers about the IP addresses of target network domain names and alternate domains that might be on or connected to the target network. This method uses DNS lookup tools available on specialized Web sites and other tools available on various local machine platforms.
- Network-based reconnaissance is the process of identifying active computers and services on a target network via tools such as ping, traceroute, and netstat.

Key Terms

DNS lookup Tools that help Internet users discover the DNS names of target computers.

dumpster diving Searching through the refuse of a target with the goal of finding any information that could be used to compromise networks or systems.