
CONTENTS

Foreword	xxi
Preface Reloaded	xxiii
Preface from the First Edition	xxv
Acknowledgments	xxvii
About the Authors	xxxi
Chapter 1 Introduction	1
The Computer World and the Golden Age of Hacking	2
Why This Book?	4
Why Cover These Specific Tools and Techniques?	5
How This Book Differs	5
The Threat: Never Underestimate Your Adversary	7
Attacker Skill Levels: From Script Kiddies to the Elite	11
A Note on Terminology and Iconography	12
Hackers, Crackers, and Hats of Many Colors: Let's Just	
Use "Attackers" and "Bad Guys"	12
Pictures and Scenarios	14
Naming Names	14
Caveat: These Tools Could Hurt You	15
Setting Up a Lab for Experimentation	16
Additional Concerns	17

Organization of Rest of the Book	19
Getting Up to Speed with the Technology	19
Common Phases of the Attack	20
Future Predictions, Conclusions, and References	20
Yeah, But What's NEW?	20
Summary	23
er 2 Networking Overview: Pretty Much Everything You Need to Know About Networking to Follow the Rest of This Book	25
The OSI Reference Model and Protocol Layering	26
How Does TCP/IP Fit In?	28
Understanding TCP/IP	32
Transmission Control Protocol (TCP)	33
TCP Port Numbers	34
TCP Control Bits, the Three-Way Handshake, and Sequence Numbers	37
Other Fields in the TCP Header	41
User Datagram Protocol (UDP)	41
Is UDP Less Secure Than TCP?	43
Internet Protocol (IP) and Internet Control Message Protocol (ICMP)	44
IP: Drop That Acronym and Put Your Hands in the Air!	45
LANs and Routers	45
IP Addresses	46
Netmasks	47
Packet Fragmentation in IP	48
Other Components of the IP Header	49
ICMP	51
Other Network-Level Issues	53
Routing Packets	53
Network Address Translation	54
Firewalls: Network Traffic Cops and Soccer Goalies	56
Don't Forget About the Data Link and Physical Layers!	66
Ethernet: The King of Wireline Connectivity	67
ARP ARP ARP!!	68
Hubs and Switches	70
802.11: The King of Wireless Connectivity	72

Security Solutions for the Internet	
Application-Level Security	
The Secure Sockets Layer (SSL) and Transport Layer Security (TLS)	
Security at the IP Level: IPsec	
Conclusion	
Summary	
Chapter 3 Linux and UNIX Overview: Pretty Much Everything You Need to Know About Linux and UNIX to Follow the Rest of This Book	
Introduction	
Learning About Linux and UNIX	
Architecture	
Linux and UNIX File System Structure	
The Kernel and Processes	
Automatically Starting Up Processes: Init, Inetd, Xinetd, and Cron	
Manually Starting Processes	
Interacting with Processes	
Accounts and Groups	
The /etc/passwd File	
The /etc/group File	
Root: It's a Bird ... It's a Plane ... No, It's Super-User!	
Linux and UNIX Permissions	
SetUID Programs	
Linux and UNIX Trust Relationships	
Logs and Auditing	
Common Linux and UNIX Network Services	
Telnet: Command-Line Remote Access	
FTP: The File Transfer Protocol	
A Better Way: Secure Shell (SSH)	
Web Servers: HTTP	
Electronic Mail	
r-Commands	
Domain Name Services	
The Network File System (NFS)	
X Window System	
Conclusion	
Summary	

Windows NT/2000/XP/2003 Overview: Pretty Much Everything You Need to Know About Windows to Follow the Rest of This Book

Introduction	127
A Brief History of Time	128
The BAD (Before Active Directory) Old Days	130
Fundamental Concepts from BAD, or "This Stuff Still Matters, So Pay Attention"	131
Shares: Accessing Resources Across the Network	133
The Underlying Windows Operating System Architecture	133
User Mode	134
How Windows Password Representations Are Derived	137
Kernel Mode	139
From Service Packs and Hotfixes to Windows Update and Beyond	141
Accounts and Groups	142
Accounts	142
Groups	145
Privilege Control	147
Policies	149
Account Policy	149
User Properties Settings	151
Trust	152
Auditing	154
Object Access Control and Permissions	156
Ownership	156
NTFS and Its Permissions	156
Share Permissions	158
Weak Default Permissions and Hardening Guides	159
Network Security	160
Limitations in Basic Network Protocols and APIs	160
Windows 2000 and Beyond: Welcome to the New Millennium	162
What Windows 2000+ Has to Offer	163
Security Considerations in Windows 2000+	166
Architecture: Some Refinements over Windows NT	168
Accounts and Groups	169
Privilege Control	170
Policies	173

Windows 2000+ Trust	174
Auditing	175
Object Access Control	175
Conclusion	177
Summary	177

Chapter 5 Phase 1: Reconnaissance

Low-Technology Reconnaissance: Social Engineering, Caller ID Spoofing, Physical Break-In, and Dumpster Diving	184
Social Engineering	184
Physical Break-In	190
Dumpster Diving	193
Search the Fine Web (STFW)	195
The Fine Art of Using Search Engines and Recon's Big Gun: Google	196
Listening in at the Virtual Water Cooler: Newsgroups	207
Searching an Organization's Own Web Site	208
Defenses Against Search Engine and Web-Based Reconnaissance	209
Whois Databases: Treasure Chests of Information	212
Researching .com, .net, .org, and .edu Domain Names	212
Researching Domain Names Other Than .com, .net, .org, .edu, .aero, .arpa, .biz, .coop, .info, .int, and .museum	215
IP Address Assignments Through ARIN and Related Sites	218
Defenses Against Whois Searches	219
The Domain Name System	220
Interrogating DNS Servers	225
Defenses From DNS-Based Reconnaissance	227
General-Purpose Reconnaissance Tools	230
Sam Spade: A General-Purpose Reconnaissance Client Tool	230
Web-Based Reconnaissance Tools: Research and Attack Portals	233
Conclusion	235
Summary	235

Chapter 6 Phase 2: Scanning

War Driving: Finding Wireless Access Points	240
War Driving Method 1: Active Scanning—Sending Probe Packets with NetStumbler	242
War Driving Method 2: Listening for Beacons and Other Traffic with Wellenreiter	245

War Driving Method 3: Forcing Deauthentication with ESSID-Jack	247
War-Driving Defenses	248
Going All the Way with a VPN	250
War Dialing: Looking for Modems in All the Right Places	252
A Toxic Recipe: Modems, Remote Access Products, and Clueless Users	253
SysAdmins and Insecure Modems	253
Finding Telephone Numbers to Feed into a War Dialer	254
Defenses Against War Dialing	258
Modem Policy	258
Network Mapping	261
Sweeping: Finding Live Hosts	262
Traceroute: What Are the Hops?	262
Defenses Against Network Mapping	267
Determining Open Ports Using Port Scanners	268
Nmap: A Full-Featured Port-Scanning Tool	269
Types of Nmap Scans	272
Defenses Against Port Scanning	294
Determining Firewall Filter Rules with Firewall	301
Vulnerability-Scanning Tools	307
A Whole Bunch of Vulnerability Scanners	310
Nessus: The Most Popular Free Vulnerability Scanner	
Available Today	310
Vulnerability-Scanning Defenses	316
Be Aware of Limitations of Vulnerability-Scanning Tools	318
Intrusion Detection System and Intrusion Prevention System Evasion	319
How Network-Based IDS and IPS Tools Work	320
How Attackers Can Evade Network-Based IDSs and IPSs	321
IDS and IPS Evasion at the Network Level	322
IDS and IPS Evasion at the Application Level	328
IDS and IPS Evasion Defenses	333
Conclusion	335
Summary	335
Phase 3: Gaining Access Using Application and Operating System Attacks	339
Script Kiddie Exploit Trolling	339
Pragmatism for More Sophisticated Attackers	340

Buffer Overflow Exploits	342
Stack-Based Buffer Overflow Attacks	343
Exploiting Stack-Based Buffer Overflows	353
Finding Buffer Overflow Vulnerabilities	353
Heap Overflows	358
The Exploit Mess and the Rise of Exploitation Engines	361
Advantages for Attackers	367
Benefits for the Good Guys, Too?	368
Buffer Overflow Attack Defenses	371
Password Attacks	377
Guessing Default Passwords	378
The Art and Science of Password Cracking	382
Let's Crack Those Passwords!	383
Defenses Against Password-Cracking Attacks	401
Web Application Attacks	406
Account Harvesting	407
Account Harvesting Defenses	410
Undermining Web Application Session Tracking and Other Variables	410
Attacking Session Tracking Mechanisms	412
Defending Against Web Application Session Tracking and Variable Alteration Attacks	421
SQL Injection	423
Defenses Against SQL Injection	428
Exploiting Browser Flaws	431
Defending Against Browser Exploits	434
Conclusion	435
Summary	435
Chapter 8 Phase 3: Gaining Access Using Network Attacks	439
Sniffing	439
Sniffing Through a Hub: Passive Sniffing	442
"Hey, Don't I Know You?" Passive OS Identification and Vulnerability Identification	446
Dsniff: A Sniffing Cornucopia	449
Sniffing Defenses	467
IP Address Spoofing	470
IP Address Spoofing Flavor 1: Simple Spoofing—Simply Changing the IP Address	470

Chapter 9 Phase 3: Denial-of-Service Attacks

IP Address Spoofing Flavor 2: Predicting TCP Sequence Numbers to Attack UNIX r-Commands	473
IP Address Spoofing Flavor 3: Spoofing with Source Routing	477
IP Spoofing Defenses	479
Session Hijacking	482
Another Way: Host-Based Session Hijacking	483
Session Hijacking with Ettercap	486
Attacking Wireless Access Points	488
Session Hijacking Defenses	491
Netcat: A General-Purpose Network Tool	491
Netcat for File Transfer	493
Netcat for Port Scanning	495
Netcat for Making Connections to Open Ports	496
Netcat for Vulnerability Scanning	497
Using Netcat to Create a Passive Backdoor Command Shell	498
Using Netcat to Actively Push a Backdoor Command Shell	499
Relaying Traffic with Netcat	501
Persistent Netcat Listeners and Netcat Honeypots	506
Netcat Defenses	509
Conclusion	510
Summary	510
Chapter 9 Phase 3: Denial-of-Service Attacks	513
Locally Stopping Services	515
Defenses from Locally Stopping Services	516
Locally Exhausting Resources	517
Defenses from Locally Exhausting Resources	518
Remotely Stopping Services	518
Defenses from Remotely Stopping Services	522
Remotely Exhausting Resources	523
SYN Flood	523
Smurf Attacks	529
Distributed Denial-of-Service Attacks	533
DDoS: A Look at the Future?	541
Distributed Denial-of-Service Defenses	542
Conclusion	543
Summary	544

Chapter 10 Phase 4: Maintaining Access: Trojans, Backdoors, and Rootkits ... Oh My!

Trojan Horses	54
Backdoors	54
Netcat as a Backdoor on UNIX Systems	55
The Devious Duo: Backdoors Melded into Trojan Horses	55
Roadmap for the Rest of the Chapter	55
Nasty: Application-Level Trojan Horse Backdoor Tools	55
Remote-Control Backdoors	55
Also Nasty: The Rise of the Bots	56
Distributing Bots: The Worm-Bot Feedback Loop	57
Additional Nastiness: Spyware Everywhere!	57
Defenses Against Application-Level Trojan Horse Backdoors, Bots, and Spyware	58
Bare Minimum: Use Antivirus and Antispyware Tools	58
Looking for Unusual TCP and UDP Ports	58
Knowing Your Software	58
User Education Is Also Critical	58
Even Nastier: User-Mode Rootkits	58
What Do User-Mode Rootkits Do?	58
Linux/UNIX User-Mode Rootkits	58
Windows User-Mode Rootkits	59
Defending Against User-Mode Rootkits	60
Don't Let the Bad Guys Get Super-User Access in the First Place!	60
Uh-oh ... They Rootkitted Me. How Do I Recover?	60
Nastiest: Kernel-Mode Rootkits	60
The Power of Execution Redirection	61
File Hiding with Kernel-Mode Rootkits	61
Process Hiding with Kernel-Mode Rootkits	61
Network Hiding with Kernel-Mode Rootkits	61
Some Particular Examples of Kernel-Mode Rootkits	61
Defending Against Kernel-Mode Rootkits	61
Fighting Fire with Fire: Don't Do It!	61
Don't Let Them Get Root in the First Place!	61
Control Access to Your Kernel	61
Looking for Traces of Kernel-Mode Rootkits by Hand	61
Automated Rootkit Checkers	61
File Integrity Checkers Still Help!	61

Antivirus Tools Help Too!	622
Trusted CDs for Incident Handling and Investigations	622
Conclusion	623
Summary	623
Chapter 11 Phase 5: Covering Tracks and Hiding	627
Hiding Evidence by Altering Event Logs	628
Attacking Event Logs in Windows	629
Attacking System Logs and Accounting Files in Linux and UNIX	632
Altering Linux and UNIX Shell History Files	635
Defenses Against Log and Accounting File Attacks	637
Activate Logging, Please	637
Setting Proper Permissions	638
Using a Separate Logging Server	638
Encrypting Your Log Files	640
Making Log Files Append Only	640
Protecting Log Files Using Write-Once Media	640
Creating Difficult-to-Find Files and Directories	641
Creating Hidden Files and Directories in UNIX	641
Creating Hidden Files in Windows	643
Defenses from Hidden Files	646
Hiding Evidence on the Network: Covert Channels	647
Tunneling	649
Covert Channels and Malware	655
Defenses Against Covert Channels	665
Conclusion	668
Summary	668
Chapter 12 Putting It All Together: Anatomy of an Attack	671
Scenario 1: Crouching Wi-Fi, Hidden Dragon	673
Scenario 2: Death of a Telecommuter	685
Scenario 3: The Manchurian Contractor	696
Conclusion	708
Summary	709

Chapter 13 The Future, References, and Conclusions

Where Are We Heading?	71
Scenario 1: Yikes!	71
Scenario 2: A Secure Future	71
Scenario 1, Then Scenario 2	71
Keeping Up to Speed	71
Web Sites	71
Mailing Lists	71
Conferences	72
Final Thoughts ... Live Long and Prosper	72
Summary	72

Index