

AT A GLANCE

Part I Casing the Establishment

▼ 1	Footprinting	7
▼ 2	Scanning	47
▼ 3	Enumeration	83

Part II Endpoint and Server Hacking

▼ 4	Hacking Windows	159
▼ 5	Hacking UNIX	231
▼ 6	Cybercrime and Advanced Persistent Threats	313

Part III Infrastructure Hacking

▼ 7	Remote Connectivity and VoIP Hacking	373
▼ 8	Wireless Hacking	465
▼ 9	Hacking Hardware	497

Part IV Application and Data Hacking

▼ 10	Web and Database Hacking	529
▼ 11	Mobile Hacking	591
▼ 12	Countermeasures Cookbook	669

Part V Appendixes

- ▼ A Ports 691
- ▼ B Top 10 Security Vulnerabilities 699
- ▼ C Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks 701
- ▼ Index 707

Part I: Getting the Facts

- ▼ 1 Footprinting 7
- ▼ 2 Scanning 47
- ▼ 3 Enumeration 83

Part II: Local System Hacking

- ▼ 4 Hacking Windows 159
- ▼ 5 Hacking Linux 231
- ▼ 6 Cybercrime and Advanced Persistent Threats 313

Part III: Wireless Hacking

- ▼ 7 Remote Connectivity and VoIP Hacking 373
- ▼ 8 Wireless Hacking 465
- ▼ 9 Hacking Hardware 497

Part IV: Network Hacking

- ▼ 10 Web and Database Hacking 529
- ▼ 11 Mobile Hacking 591
- ▼ 12 Communications Cookbook 659

CONTENTS

Foreword	xix
Acknowledgments	xxi
Introduction	xxiii

Part I Casing the Establishment

Case Study	2
IAAAS—It's All About Anonymity, Stupid	2
Tor-menting the Good Guys	2
▼ 1 Footprinting	7
What Is Footprinting?	8
Why Is Footprinting Necessary?	10
Internet Footprinting	10
Step 1: Determine the Scope of Your Activities	10
Step 2: Get Proper Authorization	10
Step 3: Publicly Available Information	11
Step 4: WHOIS & DNS Enumeration	27
Step 5: DNS Interrogation	36
Step 6: Network Reconnaissance	43
Summary	46
▼ 2 Scanning	47
Determining If the System Is Alive	48
ARP Host Discovery	49
ICMP Host Discovery	51
TCP/UDP Host Discovery	55
Determining Which Services Are Running or Listening	61
Scan Types	62
Identifying TCP and UDP Services Running	64

Detecting the Operating System	72
Making Guesses from Available Ports	73
Active Stack Fingerprinting	74
Passive Stack Fingerprinting	77
Processing and Storing Scan Data	79
Managing Scan Data with Metasploit	79
Summary	82
▼ 3 Enumeration	83
Service Fingerprinting	85
Vulnerability Scanners	87
Basic Banner Grabbing	90
Enumerating Common Network Services	92
Summary	154

Part II Endpoint and Server Hacking

Case Study: International Intrigue	158
▼ 4 Hacking Windows	159
Overview	161
What's Not Covered	161
Unauthenticated Attacks	162
Authentication Spoofing Attacks	162
Remote Unauthenticated Exploits	177
Authenticated Attacks	184
Privilege Escalation	185
Extracting and Cracking Passwords	186
Remote Control and Back Doors	200
Port Redirection	204
Covering Tracks	206
General Countermeasures to Authenticated Compromise	209
Windows Security Features	213
Windows Firewall	213
Automated Updates	213
Security Center	214
Security Policy and Group Policy	215
Microsoft Security Essentials	217
The Enhanced Mitigation Experience Toolkit	218
Bitlocker and the Encrypting File System	218
Windows Resource Protection	219
Integrity Levels, UAC, and PMIE	220
Data Execution Prevention (DEP)	222
Windows Service Hardening	223

- Compiler-based Enhancements 226
 - Coda: The Burden of Windows Security 227
 - Summary 228
 - ▼ 5 Hacking UNIX 231
 - The Quest for Root 232
 - A Brief Review 232
 - Vulnerability Mapping 233
 - Remote Access vs. Local Access 234
 - Remote Access 234
 - Data-driven Attacks 239
 - I Want My Shell 255
 - Common Types of Remote Attacks 259
 - Local Access 278
 - After Hacking Root 294
 - Rootkit Recovery 309
 - Summary 310
 - ▼ 6 Cybercrime and Advanced Persistent Threats 313
 - What Is an APT? 315
 - Operation Aurora 318
 - Anonymous 320
 - RBN 321
 - What APTs Are NOT? 322
 - Examples of Popular APT Tools and Techniques 323
 - Common APTs Indicators 363
 - Summary 368

Part III Infrastructure Hacking

- Case Study: Read It and WEP 370
- ▼ 7 Remote Connectivity and VoIP Hacking 373
 - Preparing to Dial Up 375
 - Wardialing 377
 - Hardware 377
 - Legal Issues 378
 - Peripheral Costs 378
 - Software 379
 - Brute-Force Scripting—The Homegrown Way 393
 - A Final Note About Brute-Force Scripting 403
 - PBX Hacking 405
 - Voicemail Hacking 409

	Virtual Private Network (VPN) Hacking	414
	Basics of IPSec VPNs	415
	Hacking the Citrix VPN Solution	422
	Voice over IP Attacks	440
	Attacking VoIP	441
	Summary	463
▼ 8	Wireless Hacking	465
	Background	466
	Frequencies and Channels	467
	Session Establishment	467
	Security Mechanisms	468
	Equipment	471
	Wireless Adapters	471
	Operating Systems	472
	Miscellaneous Goodies	472
	Discovery and Monitoring	474
	Finding Wireless Networks	475
	Sniffing Wireless Traffic	478
	Denial of Service Attacks	479
	Encryption Attacks	481
	WEP	481
	Authentication Attacks	485
	WPA Pre-Shared Key	485
	WPA Enterprise	490
	Summary	496
▼ 9	Hacking Hardware	497
	Physical Access: Getting in the Door	498
	Hacking Devices	505
	Default Configurations	509
	Owned Out of the Box	509
	Standard Passwords	509
	Bluetooth	510
	Reverse Engineering Hardware	511
	Mapping the Device	511
	Sniffing Bus Data	515
	Sniffing the Wireless Interface	518
	Firmware Reversing	518
	ICE Tools	523
	Summary	526

Part IV Application and Data Hacking

	Case Study	528
▼ 10	Web and Database Hacking	529
	Web Server Hacking	530
	Sample Files	532
	Source Code Disclosure	532
	Canonicalization Attacks	533
	Server Extensions	534
	Buffer Overflows	536
	Denial of Service	537
	Web Server Vulnerability Scanners	538
	Web Application Hacking	540
	Finding Vulnerable Web Apps with Google (Googledorks)	540
	Web Crawling	541
	Web Application Assessment	542
	Common Web Application Vulnerabilities	556
	Database Hacking	570
	Database Discovery	570
	Database Vulnerabilities	572
	Other Considerations	587
	Summary	589
▼ 11	Mobile Hacking	591
	Hacking Android	593
	Android Fundamentals	594
	Hacking Your Android	600
	Hacking Other Androids	616
	Android as a Portable Hacking Platform	635
	Defending Your Android	639
	iOS	640
	Know Your iPhone	641
	How Secure Is iOS?	643
	Jailbreaking: Unleash the Fury!	644
	Hacking Other iPhones: Fury Unleashed!	651
	Summary	667
▼ 12	Countermeasures Cookbook	669
	General Strategies	671
	(Re)move the Asset	671
	Separation of Duties	672
	Authenticate, Authorize, and Audit	673
	Layering	675
	Adaptive Enhancement	675

Orderly Failure	676
Policy and Training	677
Simple, Cheap, and Easy	677
Example Scenarios	678
Desktop Scenarios	678
Server Scenarios	679
Network Scenarios	684
Web Application and Database Scenarios	685
Mobile Scenarios	686
Summary	688

Part V Appendixes

▼ A Ports	691
▼ B Top 10 Security Vulnerabilities	699
▼ C Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks	701
Countermeasures	704
▼ Index	707