

CONTENTS

Foreword	xvii
Commentary on the State of Network Security	xx
Acknowledgments	xxiii
Introduction	xxv

Part I

Casing the Establishment

Case Study: Giving Up the Goods	2
▼ 1 Footprinting	3
What Is Footprinting?	4
Why Is Footprinting Necessary?	4
Internet Footprinting	4
Step 1. Determine the Scope of Your Activities	6
Step 2. Network Enumeration	10
Step 3. DNS Interrogation	19
Step 4. Network Reconnaissance	24
Summary	28
▼ 2 Scanning	29
Determining If the System Is Alive	30
Determining Which Services Are Running or Listening	37
Scan Types	38
Identifying TCP and UDP Services Running	40
Windows-Based Port Scanners	46
Port Scanning Breakdown	50

Detecting the Operating System	54
Active Stack Fingerprinting	54
Passive Stack Fingerprinting	58
The Whole Enchilada: Automated Discovery Tools	60
Summary	61
▼ 3 Enumeration	63
Windows NT/2000 Enumeration	64
NT/2000 Network Enumeration	68
NT/2000 Host Enumeration	78
NT/2000 Applications and Banner Enumeration	91
Novell Enumeration	95
Browsing the Network Neighborhood	95
UNIX Enumeration	100
BGP Route Enumeration	109
Summary	112

Part II

System Hacking

Case Study: Stop and Smell the Roses on the Quest for Root . . .	114
▼ 4 Hacking Windows 95/98, Me, and XP Home Edition	115
Win 9x Remote Exploits	117
Direct Connection to Win 9x Shared Resources	117
Win 9x Backdoor Servers and Trojans	123
Known Server Application Vulnerabilities	128
Win 9x Denial of Service	128
Win 9x Local Exploits	129
Windows Millennium Edition (Me)	135
Win Me Remote Attacks	136
Win Me Local Attacks	136
Windows XP Home Edition	137
Internet Connection Firewall (ICF)	138
Integrated MS Passport Single Login for the Internet	139
Remote Control and Management	139
Summary	139
▼ 5 Hacking Windows NT	141
Overview	143
Where We're Headed	143
What About Windows 2000?	143

The Quest for Administrator	144
Remote Exploits: Denial of Service and Buffer Overflows . .	160
Privilege Escalation	164
Consolidation of Power	175
Exploiting Trust	185
Sniffers	190
Remote Control and Back Doors	194
Port Redirection	204
General Countermeasures to Privileged Compromise	207
Rootkit: The Ultimate Compromise	211
Covering Tracks	213
Disabling Auditing	214
Clearing the Event Log	214
Hiding Files	215
Summary	216
▼ 6 Hacking Windows 2000	219
Footprinting	220
Scanning	221
Enumeration	226
Penetration	228
NetBIOS-SMB Password Guessing	229
Eavesdropping on Password Hashes	229
SMBRelay	229
Attacks Against IIS 5	237
Remote Buffer Overflows	237
Denial of Service	237
Privilege Escalation	241
Pilfering	246
Grabbing the Windows 2000 Password Hashes	246
The Encrypting File System (EFS)	251
Exploiting Trust	257
Covering Tracks	258
Disabling Auditing	259
Clearing the Event Log	259
Hiding Files	259
Back Doors	260
Startup Manipulation	260
Remote Control	262
Keystroke Loggers	264
General Countermeasures: New Windows Security Tools	264
runas	267
The Future of Windows 2000	269

.NET Framework	269
Codename Whistler	269
Whistler Versions	269
Whistler Security Features	270
A Note on Raw Sockets and Other Unsubstantiated Claims	272
Summary	272
▼ 7 Novell NetWare Hacking	275
Attaching but Not Touching	276
Enumerate Bindery and Trees	278
Opening the Unlocked Doors	284
Authenticated Enumeration	286
Gaining Admin	291
Application Vulnerabilities	294
Spoofing Attacks (Pandora)	296
Once You Have Admin on a Server	299
Owning the NDS Files	301
Log Doctoring	306
Console Logs	308
Summary	311
▼ 8 Hacking UNIX	313
The Quest for Root	314
A Brief Review	314
Vulnerability Mapping	315
Remote Access vs. Local Access	315
Remote Access	316
Data Driven Attacks	320
I Want My Shell	327
Common Types of Remote Attacks	332
Local Access	354
After Hacking Root	372
Rootkits	372
Rootkit Recovery	384
Summary	385

Part III

Network Hacking

Case Study: Using All the Dirty Tricks to Get In	390
▼ 9 Dial-Up, PBX, Voicemail, and VPN Hacking	393
Preparing to Dial Up	394

Wardialing	396
Hardware	396
Legal Issues	397
Peripheral Costs	398
Software	398
Brute Force Scripting—The Home-Grown Way	413
PBX Hacking	424
Voicemail Hacking	428
Virtual Private Network (VPN) Hacking	434
Summary	438
▼ 10 Network Devices	441
Discovery	442
Detection	442
SNMP	449
Back Doors	452
Default Accounts	452
Lower the Gates (Vulnerabilities)	455
Shared vs. Switched	462
Detecting the Media You're On	463
Passwords on a Silver Platter: Dsniff	464
Sniffing on a Network Switch	466
Wireless Network Hacking	474
IEEE 802.11 Wireless LAN	475
WAP (Cellular Phone)	477
Summary	478
▼ 11 Firewalls	479
Firewall Landscape	480
Firewall Identification	480
Advanced Firewall Discovery	485
Scanning Through Firewalls	488
Packet Filtering	493
Application Proxy Vulnerabilities	496
WinGate Vulnerabilities	498
Summary	500
▼ 12 Denial of Service (DoS) Attacks	503
Motivation of DoS Attackers	504
Types of DoS Attacks	505
Bandwidth Consumption	505
Resource Starvation	506
Programming Flaws	506
Routing and DNS Attacks	506

Generic DoS Attacks	508
Sites Under Attack	510
UNIX and Windows NT DoS	513
Remote DoS Attacks	514
Distributed Denial of Service Attacks	518
Local DoS Attacks	523
Summary	524

Part IV

Software Hacking

Case Study: Silent and Deadly	528
▼ 13 Remote Control Insecurities	529
Discovering Remote Control Software	530
Connecting	531
Weaknesses	532
Virtual Network Computing (VNC)	539
Microsoft Terminal Server and Citrix ICA	543
Server	543
Clients	543
Data Transmission	544
Finding Targets	544
Attacking Terminal Server	546
Additional Security Considerations	549
Resources	550
Summary	551
▼ 14 Advanced Techniques	553
Session Hijacking	554
Back Doors	557
Trojans	578
Cryptography	581
Terminology	581
Classes of Attacks	582
Secure Shell (SSH) Attacks	582
Subverting the System Environment: Rootkits and Imaging Tools	584
Social Engineering	587
Summary	589
▼ 15 Web Hacking	591
Web Pilfering	592
Finding Well-Known Vulnerabilities	596
Automated Scripts, for All Those "Script Kiddies"	596
Automated Applications	598

Generic DoS Attacks	508
Sites Under Attack	510
UNIX and Windows NT DoS	513
Remote DoS Attacks	514
Distributed Denial of Service Attacks	518
Local DoS Attacks	523
Summary	524

Part IV

Software Hacking

Case Study: Silent and Deadly	528
▼ 13 Remote Control Insecurities	529
Discovering Remote Control Software	530
Connecting	531
Weaknesses	532
Virtual Network Computing (VNC)	539
Microsoft Terminal Server and Citrix ICA	543
Server	543
Clients	543
Data Transmission	544
Finding Targets	544
Attacking Terminal Server	546
Additional Security Considerations	549
Resources	550
Summary	551
▼ 14 Advanced Techniques	553
Session Hijacking	554
Back Doors	557
Trojans	578
Cryptography	581
Terminology	581
Classes of Attacks	582
Secure Shell (SSH) Attacks	582
Subverting the System Environment: Rootkits and Imaging Tools	584
Social Engineering	587
Summary	589
▼ 15 Web Hacking	591
Web Pilfering	592
Finding Well-Known Vulnerabilities	596
Automated Scripts, for All Those "Script Kiddies"	596
Automated Applications	598