



Contents

Acknowledgments	xi
A Note to the Reader	xii
Introduction	xiii
Part I: In the Beginning	1
Chapter 1 Understanding Communication Protocols	3
A Brief History of the Internet	3
Internet Protocol	5
IP Datagrams, Encapsulation, Size, and Fragmentation	8
IP Addresses, Classes, Subnet Masks	10
Subnetting, VLSM, and Unraveling IP the Easy Way	11
ARP/RARP Engineering: Introduction to Physical Hardware Address Mapping	22
ARP Encapsulation and Header Formatting	23
RARP Transactions, Encapsulation	24
RARP Service	25
Transmission Control Protocol	25
Sequencing and Windowing	26
TCP Packet Format and Header Snapshots	26
Ports, Endpoints, Connection Establishment	28
User Datagram Protocol	30
UDP Formatting, Encapsulation, and Header Snapshots	30
Multiplexing, Demultiplexing, and Port Connections	31
Internet Control Message Protocol	32
ICMP Format, Encapsulation, and Delivery	32
ICMP Messages, Subnet Mask Retrieval	33
ICMP Header Snapshots	36
Moving Forward	36

Chapter 2	NetWare and NetBIOS Technology	37
	NetWare: Introduction	37
	Internetwork Packet Exchange	37
	Sequenced Packet Exchange	44
	SPX Format, Header Snapshots	44
	Connection Management, Session Termination	45
	Watchdog Algorithm	45
	Error Recovery, Congestion Control	47
	Wrapping Up	47
	NetBIOS Technology: Introduction	47
	Naming Convention, Header Snapshots	48
	General, Naming, Session, and Datagram Services	48
	NetBEUI: Introduction	50
	NetBIOS Relationship	50
	Windows and Timers	50
	Conclusion	51
Part II:	Putting It All Together	53
Chapter 3	Understanding Communication Mediums	55
	Ethernet Technology	55
	Carrier Transmissions	56
	Ethernet Design, Cabling, Adapters	57
	Hardware Addresses, Frame Formats	60
	Token Ring Technology	60
	Operation	62
	Token Ring Design, Cabling	62
	Prioritization	62
	Fault Management	63
	Addresses, Frame Format	63
	Fiber Distributed Data Interface Technology	64
	Operation	65
	FDDI Design, Cabling	66
	Frame Format	66
	Analog Technology	67
	Problem Areas and Remedies	67
	System Registry	69
	Integrated Services Digital Network Technology	71
	ISDN Devices	71
	ISDN Service Types	72
	ISDN versus Analog	72
	Digital Subscriber Line	73
	Point-to-Point Technology	74
	PPP Operation	74
	Frame Structure	75
	Frame Relay Technology	76
	Operation, Devices, Data-Link Connection Identifiers, and Virtual Circuits	76

Congestion Notification and Error Checking	78
Local Management Interface	78
Frame Relay Frame Format	79
Looking Ahead	79
Part III: Uncovering Vulnerabilities	81
<hr/>	
Intuitive Intermission A Little Terminology	83
Who Are Hackers, Crackers, Phreaks, and Cyberpunks?	83
What Is Hacking?	84
Profiling the Hacker	87
Security Levels	88
Security Class C1: Test Condition Generation	88
Security Class C2: Test Condition Generation	89
Security Class B1: Test Condition Generation	90
Security Class B2: Test Condition Generation	91
Kickoff	92
Chapter 4 Well-Known Ports and Their Services	93
A Review of Ports	93
TCP and UDP Ports	94
Well-Known Port Vulnerabilities	94
Unidentified Ports and Services	109
What's Next	147
Chapter 5 Discovery and Scanning Techniques	149
Discovery	149
Whois Domain Search Query	151
Host PING Query	153
Internet Web Search Query	156
Social Engineering Query	156
Site Scans	157
Scanning Techniques	158
Scanner Packages	159
Sample Scan	173
Summary	180
Part IV: Hacking Security Holes	181
<hr/>	
Intuitive Intermission A Hacker's Genesis	183
Chapter 6 The Hacker's Technology Handbook	189
Networking Concepts	189
Open Systems Interconnection Model	189
Cable Types and Speeds versus Distances	191
Decimal, Binary, and Hex Conversions	192
Protocol Performance Functions	204
Networking Technologies	205
Media Access Control Addressing and Vendor Codes	205

Ethernet	206
Token Ring	215
Token Ring and Source Route Bridging	216
Token Ring and Source Route Translational Bridging	221
Fiber Distributed Data Interface	223
Routing Protocols	225
Distance Vector versus Link State Routing Protocols	226
Routing Information Protocol	228
Interior Gateway Routing Protocol	229
Appletalk Routing Table Maintenance Protocol	230
Open Shortest Path First Protocol	230
Important Commands	231
Append	232
Assign	233
Attrib	234
Backup	234
Break	235
Chcp	236
Chdir (CD)	236
Chkdsk	237
Cls	238
Command	238
Comp	239
Copy	239
Ctty	240
Date	241
Del(Erase)	241
Dir	242
Diskcomp	243
Diskcopy	243
Exe2bin	244
Exit	244
Fastopen	245
Fc	245
Fdisk	247
Find	247
Format	248
Graftabl	249
Graphics	249
Join	250
Keyb	251
Label	252
Mkdir (MD)	253
Mode	253
More	257
Nlsfunc	257
Path	257
Print	258
Prompt	259
Recover	260
Ren (Rename)	261

Replace	261
Restore	262
Rmdir (Rd)	263
Select	263
Set	264
Share	265
Sort	265
Subst	266
Sys	267
Time	267
Tree	268
Type	268
Ver	269
Verify	269
Vol	269
Xcopy	270
Looking Ahead	271
Chapter 7 Hacker Coding Fundamentals	273
The C Programming Language	273
Versions of C	274
Classifying the C Language	275
Structure of C	276
Comments	277
Libraries	277
C Compilation	278
Data Types	279
Operators	283
Functions	285
C Preprocessor Commands	290
Program Control Statements	293
Input and Output	297
Pointers	301
Structures	304
File I/O	311
Strings	321
Text Handling	328
Time	331
Header Files	337
Debugging	338
Float Errors	339
Error Handling	339
Casting	343
Prototyping	344
Pointers to Functions	345
Sizeof	347
Interrupts	347
Signal	350
Dynamic Memory Allocation	351
Atexit	354
Increasing Speed	355

Directory Searching	356
Accessing Expanded Memory	359
Accessing Extended Memory	363
TSR Programming	373
Conclusion	405
Chapter 8 Port, Socket, and Service Vulnerability Penetrations	407
Example Case Synopsis	407
Backdoor Kits	408
Implementing a Backdoor Kit	411
Common Backdoor Methods in Use	411
Packet Filters	412
Stateful Filters	417
Proxies and Application Gateways	422
Flooding	423
Log Bashing	434
Covering Online Tracks	434
Covering Keylogging Trails	436
Mail Bombing, Spamming, and Spoofing	447
Password Cracking	449
Decrypting versus Cracking	450
Remote Control	455
Step 1: Do a Little Research	456
Step 2: Send the Friendly E-Message	456
Step 3: Claim Another Victim	457
Sniffing	459
Spoofing IP and DNS	470
Case Study	471
Trojan Infection	480
Viral Infection	489
Wardialing	490
Web Page Hacking	492
Step 1: Conduct a Little Research	494
Step 2: Detail Discovery Information	495
Step 3: Launch the Initial Attack	498
Step 4: Widen the Crack	499
Step 5: Perform the Web Hack	499
Part V: Vulnerability Hacking Secrets	503
<hr/>	
Intuitive Intermission A Hacker's Vocation	505
Chapter 9 Gateways and Routers and Internet Server Daemons	507
Gateways and Routers	507
3Com	508
Ascend/Lucent	516
Cabletron/Enterasys	524
Cisco	533

Intel	541
Nortel/Bay	549
Internet Server Daemons	554
Apache HTTP	555
Lotus Domino	556
Microsoft Internet Information Server	558
Netscape Enterprise Server	560
Novell Web Server	564
O'Reilly WebSite Professional	567
Conclusion	572
Chapter 10 Operating Systems	573
UNIX	574
AIX	576
BSD	586
HP/UX	602
IRIX	612
Linux	616
Macintosh	645
Microsoft Windows	649
Novell NetWare	668
OS/2	678
SCO	694
Solaris	697
Conclusion	700
Chapter 11 Proxies and Firewalls	701
Internetworking Gateways	701
BorderWare	701
FireWall-1	706
Gauntlet	710
NetScreen	714
PIX	719
Raptor	727
WinGate	730
Conclusion	736
Part VI: The Hacker's Toolbox	737
Intuitive Intermission The Evolution of a Hacker	739
Chapter 12 TigerSuite: The Complete Internetworking Security Toolbox	749
Tiger Terminology	749
Introduction to TigerSuite	754
Installation	754
Program Modules	758
System Status Modules	759
TigerBox Toolkit	766
TigerBox Tools	766
TigerBox Scanners	772
TigerBox Penetrators	775

TigerBox Simulators	775
Sample Real-World Hacking Analysis	777
Step 1: Target Research	778
Step 2: Discovery	782
Step 3: Social Engineering	784
Step 4: Hack Attacks	786
Conclusion	786
Appendix A IP Reference Table and Subnetting Charts	789
Appendix B Well-Known Ports and Services	793
Appendix C All-Inclusive Ports and Services	799
Appendix D Detrimental Ports and Services	839
Appendix E What's on the CD	845
Tiger Tools 2000	846
TigerSuite (see Chapter 12)	846
Chapter 5	847
jakal	847
nmap	847
SAFEsuite	848
SATAN	848
Chapter 8	848
Backdoor Kits	848
Flooders	848
Log Bashers	848
Mail Bombers and Spammers	849
Password Crackers	849
Remote Controllers	852
Sniffers	853
Spoofers	855
Trojan Infectors	855
Viral Kits	856
Wardialers	856
Chapters 9, 10, and 11	857
Tools	857
Appendix F Most Common Viruses	859
Appendix G Vendor Codes	877
Glossary	919
References	927
Index	929