

CODE HACKING:

A Developer's Guide to Network Security

- Teaches developers to think like hackers so they can develop effective, defensive code
- Explains hacking techniques, and provides insight into understanding how to prevent hacking issues in your code
- Teaches developers how to write and use scanners, sniffers, exploits, and how to write network security test harnesses for application and infrastructure



Contents

Acknowledgments	xiii
-----------------	------

1 Introduction	1
-----------------------	----------

Consequences of Intrusion	7
Indirect Threats	9
A Short Tour of Social Engineering	11
The Changing World of Development	13
A Word on Hacking....	18
A Word on Hackers....	19
Endnotes	21

2 Networking	23
---------------------	-----------

A Brief History Lesson	23
OSI	24
Network Access Layer	26
Ethernet	27
What's in a 802.3 Ethernet Frame?	29
The Internet Layer	30
IP, the Internet Protocol	30
ARP	31
RARP	31
Inside an IP Packet	31
IP Addressing	34
Subnetting	37
Routing	39
Hacking IP	42

ARP Spoofing	42
IP Spoofing	43
IP Fragmentation Attacks	44
TCP/IP	45
Three-Way Handshaking with TCP	46
Examining a TCP Header Segment	48
TCP Session Hijacking	50
TCP Denial of Service	51
TCP Land Attack	51
UDP	52
UDP Denial of Service	53
UDP Flooding (Fraggle Attack)	53
ICMP	54
Ping of Death	55
Ping Flooding	55
Smurf Attack	56
A Ping Example	56
Multipurpose ICMP	65
ICMPv4 and ICMPv6	66
Internet Application Network Architectures	66
The Demilitarized Zone	70
Network Address Translation—NAT	75
DNS	76
What Is DNS?	76
Implementing DNS Servers	78
DNS Vulnerabilities	78
Zone Transfers	79
DNS Spoofing	80
Endnotes	80

3 Tools of the Trade	81
Tools of the Trade	81
Whois	82

NSLookup	85
Sam Spade	86
nbtstat	88
NetCat	90
Key Logging	91
Building a Simple Port Scanner	96
Building Netstat	115
Using Netstat	120
Scanning by Stealth	121
NMap	123
Packet Sniffing	127
Mapping a Route through the Internet	131
Endnotes	137

4 Encryption and Password Cracking	139
Keeping Secrets	140
Encryption over the Wire	140
Symmetric Encryption	141
Hashing Algorithms	145
Public Key Cryptography	149
Man in the Middle	150
PKI	151
A Guide to Using Encryption Software	152
Encryption Weaknesses	155
Application Layer Security	157
History of SSL Hacks	159
Using Credentials	162
Cracking Application Passwords	173
An Introduction to VPNs	176
Flaws in PPTP	178
Sniffing Password Hashes	178
Endnotes	179

5	Hacking the Web	181
	How Web Sites and Applications Are Attacked	182
	Footprinting the Site	182
	Robots.txt	185
	Web Servers and Server-Side Attacks	185
	Web Server Technologies: How to Exploit and Protect Them	187
	Common Gateway Interface (CGI)	188
	Hacking Perl-Coded CGI Applications	188
	Buffer Overflow Attacks	190
	Client-Side Attacks	198
	ActiveX	198
	Safe for Scripting?	199
	Hacking Java Applets	200
	Cross-Site Scripting	202
	Cookie Interception	205
	SQL Injection	209
	Beyond the Initial Statement	214
	Calling System-Stored Procedures and More	217
6	Cracks, Hacks, and Counterattacks	219
	IPC\$	221
	Writing Plug-Ins	229
	Hacking FTP	232
	Password Cracking	232
	FTP Bounce Attacks	234
	Example FTP Attacks	235
	Client Attacks	238
	Malicious Web Content	238
	Streaming Media	241
	Analyzing MS Blaster	242
	Windows Shatter Attacks	246
	Vulnerability Detection with Nessus and Nikto	257
	A Short Summary of IIS Exploits	266

Trojans and Backdoors	268
DNS Spoofing	270
Summary	274
Endnotes	274
7 Firewalls	275
Common Implementation	276
Firewall Types	279
Packet Filter-Based Firewalls	280
Application (Proxy) Firewalls	281
Stateful Packet Inspection Firewalls	281
Adaptive Proxy Firewall Systems	282
NAT and PAT	282
Security Advantages of NAT and PAT	289
iptables	290
State	296
Using iptables for NAT	304
Mangle	306
Administration and Design for Maintenance	306
GUIs	307
Conclusions	310
8 Passive Defense	311
Shape of the Network	313
Introducing Snort	315
Snort's Software Architecture	316
Packet Sniffing Using Snort	316
Examining the config File	318
Examining Rules Building	322
The Snort Preprocessor Pipeline	328
Inside a Snort Preprocessor	331
Using Output Plug-Ins/Analyzing Data with ACID	334
IDS Evasion Techniques	336

Honeynets	338
Endnotes	342

9 Wireless Networking 343

802.11x	345
Structure of 802.11 MAC	348
Types of WLANs	349
Associating with a WLAN	349
WEP	352
Problems with WEP?	353
Initialization Vectors	353
CRC	355
WEP Attacks	355
Passive Attack to Decrypt Traffic	355
Active Attack to Inject Traffic	356
Active Attack Example, or Getting the WLAN to Decrypt Packets	356
Tools	357
Hardware Issues (for the Attacker)	357
WLAN Utilities	358
WEP Cracking	359
Secure WLAN Solutions	360
A New Standard	360
WPA	361
Wireless Security Is Improving	362

Appendix A About the CD-ROM 365

CD-ROM Folders	365
Overall System Requirements	365

Appendix B GNU General Public License 367

Index 375