

CONTENTS

<i>Acknowledgments</i>	<i>xiii</i>
<i>Introduction</i>	<i>xix</i>

Reference Center

Common Commands	RC 2
Common Ports	RC 7
IP Addressing	RC 9
Dotted Decimal Notation	RC 9
Classes	RC 9
Subnet Masks	RC 11
CIDR (Classless Inter-Domain Routing)	RC 12
Loopback	RC 12
Private Addresses	RC 12
Protocol Headers	RC 12
Online Resources	RC 15
Hacking Tools	RC 15
Web Resources	RC 18
Mailing Lists	RC 19
Conferences and Events	RC 19
Useful Netcat Commands	RC 20
ASCII Table	RC 22
HTTP Codes	RC 28
Important Files	RC 30

Part I

Hacking Techniques and Defenses

■ 1 Footprinting	3
Search Engines	4
Domain Registrars	8
Regional Internet Registries	12
DNS Reverse-Lookups	14

Mail Exchange	15
Zone Transfers	16
Traceroute	18
Summary	19
■ 2 Scanning and Identification	21
Pinging	23
Ping Sweeping	23
TCP Pinging	24
Port Scanning	25
TCP Connect	25
TCP SYN/Half-Open	26
FIN	27
Reverse Ident	28
XMAS	28
NULL	29
RPC	29
IP Protocol	30
ACK	30
Window	31
UDP	31
Fingerprinting	32
Summary	34
■ 3 Enumeration	35
Enumerate Remote Services	36
FTP (File Transfer Protocol): 21 (TCP)	37
SSH (Secure Shell): 22 (TCP)	38
Telnet: 23 (TCP)	38
SMTP (Simple Mail Transfer Protocol): 25 (TCP)	39
DNS (Domain Name System): 53 (TCP/UDP)	41
Finger: 79 (TCP)	42
HTTP (Hypertext Transfer Protocol): 80 (TCP)	43
POP3 (Post Office Protocol 3): 110 (TCP)	45
Portmapper: 111 (TCP)	45
NNTP (Network News Transfer Protocol): 119 (TCP)	47
Samba: 137 to 139 (TCP and UDP)	48
IMAP2/IMAP4 (Internet Message Access Protocol 2/4): 143 (TCP)	49
SNMP (Simple Network Management Protocol): 161, 162 (UDP)	50

HTTPS (Secure Hypertext Transfer Protocol): 443 (TCP)	51
NNTPS (Secure Network News Transfer Protocol): 563 (TCP)	52
IMAPS (Secure Internet Message Access Protocol): 993 (TCP)	52
POP3S (Secure Post Office Protocol 3): 995 (TCP)	53
MySQL: 3306 (TCP)	53
Automated Banner-Grabbing	54
Summary	56
■ 4 Remote Hacking	57
Remote Services	58
Intrusion Tactics	58
Remote Service Vulnerabilities	62
Application Vulnerabilities	103
Nessus	104
Obtaining a Shell	105
Port Redirection	108
Cracking /etc/shadow	109
Summary	110
■ 5 Privilege Escalation	111
Exploiting Local Trust	112
Group Memberships and Incorrect File Permissions	112
"." in PATH	114
Software Vulnerabilities	115
Kernel Flaws	115
Local Buffer Overflows	116
Improper Input Validation	116
Symbolic Links	117
Core Dumps	117
Misconfigurations	118
Summary	118
■ 6 Hiding	119
Clean Logs	120
Shell History	120
Cleaning /var	121
Backdoors	122
Setuid and Setgid Shells Owned by root	123
Changing a Local Account's uid to 0	123

.rhosts	124
SSH's authorized_keys	125
Trojans	126
Rootkits	126
Summary	128

Part II

Host Hardening

■ 7	Default Settings and Services	131
	Set Password Policies	132
	Remove or Disable Unnecessary Accounts	132
	Remove "." from the PATH Variable	132
	Check the Contents of /etc/hosts.equiv	133
	Check for .rhosts Files	133
	Disable Stack Execution	133
	Use TCP Wrappers	133
	Harden inetd and xinetd Configurations	134
	Disable Unnecessary Services	134
	Disable inetd or xinetd If No Services Are Enabled	135
	Ensure Logging Is Turned On	135
	Harden Remote Services	135
	WU-FTP	135
	SSH	136
	Sendmail	136
	BIND (DNS)	138
	Apache (HTTP and HTTPS)	139
	Samba	140
	NFS	141
	Summary	141
■ 8	User and File-System Privileges	143
	File Permissions: A Quick Tutorial	144
	World-Readable Files	145
	World-Writable Files	146
	Files Owned by bin and sys	146
	The umask Value	146
	Important Files	147
	Files in /dev	149
	Disk Partitions	149
	setuid and setgid Files	150
	Implement the wheel Group	150

Sudo	151
Summary	151
■ 9 Logging and Patching	153
Logging	154
Log Files	154
Log Rotation	156
Free Space in /var	157
Patching	157
Summary	158

Part III

Special Topics

■ 10 Nessus Attack Scripting Language (NASL)	161
Running NASL Scripts from the Command Line ...	162
Writing Nessus Plug-ins Using NASL	162
Example Vulnerability	162
The Plug-in	163
Running the Plug-in	166
Summary	167
■ 11 Wireless Hacking	169
Introduction to WEP	170
Antennas	171
Popular Tools	172
Airsnot	172
Kismet	173
Fata-Jack	173
Securing Wireless Networks	174
Summary	175
■ 12 Hacking with the Sharp Zaurus PDA	177
Kismet	178
Wellenreiter II	179
Nmap	179
Qpenmapfe	179
Bing	180
OpenSSH	180
Hping2	181
VNC Server	182
Keypebble VNC Viewer	183

Smbmount	183
Tcpdump	183
Wget	184
ZEthereal	184
zNessus	184
MTR	185
Dig	185
Perl	186
Online Resources for the Zaurus	186
Summary	186
■ Index	187