

CONTENTS

<i>Acknowledgments</i>	<i>xvii</i>
<i>HackNotes: The Series</i>	<i>xix</i>
<i>Introduction</i>	<i>xxiii</i>

Reference Center

Common System Commands	RC 2
Windows System and Network Commands ...	RC 2
Windows Enumeration Commands and Tools	RC 3
Common DOS Commands	RC 5
UNIX System and Network Commands	RC 6
Specific UNIX Enumeration Commands	RC 9
Netcat Remote Shell Commands	RC 10
Router Commands	RC 11
IP Addressing and Subnetting	RC 12
Network Ranges	RC 12
Usable Hosts and Networks	RC 12
Private, Nonroutable IP Ranges	RC 13
Password and Log File Locations	RC 13
Most Useful Ports and Services in the Hacking Process	RC 14
Common Remote-Access Trojans and Ports	RC 16
Common Trojan Ports	RC 17
Dangerous File Attachments “Drop List”	RC 18
Common and Default Passwords	RC 20
Decimal, Hex, Binary, ASCII Conversion Table	RC 21
Windows and UNIX Hacking Steps	RC 24
Must-Have Free (or Low Cost) Tools	RC 29

Part I**Network Security Principles and Methodologies**

■ 1	Security Principles and Components	3
	Asset and Risk Based INFOSEC Lifecycle Model ...	4
	ARBIL Outer Wheel	4
	ARBIL Inner Wheel	6
	Confidentiality, Integrity, and Availability— the CIA Model	7
	Confidentiality	7
	Integrity	8
	Availability	8
	A Glimpse at the Hacking Process	8
	Attack Trees	9
	Information Security Threats List	9
	INFOSEC Target Model	10
	Vulnerability List	10
	Network Security Safeguards and Best Practices ...	12
	Network Security Best Practices	13
	Summary	16
■ 2	INFOSEC Risk Assessment and Management	17
	Risk Management Using the SMIRA Process	18
	What Is Risk Management?	21
	What Is Risk Assessment?	21
	Risk Assessment Components	23
	Risk Assessment Terminology and Component Definitions	26
	Asset	26
	Threat	28
	Threat Agent/Actor and Threat Act	28
	Threat Indicators	29
	Vulnerability	29
	Threat Consequences	30
	Impact	30
	Risk	30
	Safeguards and Controls	30
	Conducting a Risk Assessment	32
	Summary	34

Part II

Hacking Techniques and Defenses

■ 3	Hacking Concepts	37
	Hacking Model	38
	Reconnaissance	38
	Compromise	41
	Leverage	42
	Targeting List	43
	Attack Trees	44
	Infrastructure	45
	Application	46
	Summary	47
■ 4	Reconnaissance	49
	Collect and Assess	50
	Identification of the Enterprise	50
	Identification of Registered Domains	51
	Identification of Addresses	51
	Scan	52
	DNS Discovery	53
	ICMP Scan	54
	TCP Scan	55
	UDP Scan	56
	Enumerate	57
	Services Enumeration	57
	Advanced Stack Enumeration	61
	Source Port Scanning	62
	Application Enumeration	63
	Service Enumeration	63
	Banner Nudges	69
	Client Connections	70
	Summary	71
■ 5	Attack, Compromise, and Escalate	73
	UNIX Exploits	74
	Remote UNIX Attacks	75
	Remote Attacks on Insecure Services	78
	Local UNIX Attacks	84
	Windows Exploits	87

Windows 9x/ME	87
Remote Attacks—Windows 9x/ME	87
Local Attacks—Windows 9x/ME	89
Windows NT/2000	90
Remote Attacks—Windows NT/2000	91
Local Attacks—Windows	94
Native Application Attacks— Windows NT/2000	99
Summary	104

Part III

Special Topics

■ 6	Wireless Network Security	107
	Wireless Networks	108
	Overview of 802.11 Wireless Standards	108
	Attacking the Wireless Arena	110
	The Future of 802.11 Security	117
	Summary	118
■ 7	Web Application Security	119
	A Dangerous Web	120
	Beyond Firewalls	120
	Overall Web Security	121
	Securing the Servers and Their Environments	121
	Securing Web Applications	123
	Categories of Web Application Security	123
	Authentication	124
	Authorization	125
	Session Management	127
	Input Parameters	128
	Encryption	131
	Miscellaneous	132
	General Web Application Assessment/Hacking	134
	Methodology	135
	Summary	139
■ 8	Common Intruder Tactics	141
	Social Engineering	142
	They Seem Legitimate!	144
	Final Thoughts on Social Engineering	147

Network Sniffing—What Are Sniffers?	147
Why Will a Hacker Use Them?	148
Commonly Used Sniffers	148
How Do You Detect Sniffers?	153
Exploiting Software Design and Implementation	
Flaws	157
Buffers—What Are They?	158
Developing the Exploit Code	162
Final Thoughts on Design and Implementation Flaws	163
War Dialing and PBX Hacking	163
Overview of Security Implications	164
Types of Dial-Up Systems to Protect	165
Top Three War Dialing Tools	173
Summary	175
 ■ 9 Incident Response	177
Signs of Being Hacked	178
Trojan Horse Programs	178
Rootkits	180
Identifying a Compromise	181
Network	182
User Accounts and User Groups	182
File Systems/Volumes and Processes	184
Logging	186
Incident Recovery Checklist	187
Stage One: Identify and Disable	187
Stage Two: Notify and Plan	188
Stage Three: Implement Countermeasures and Heighten Awareness	188
Stage Four: Recover and Rebuild	189
Stage Five: Wrap Up and Analyze	190
Summary	191
 ■ 10 Security Assessment/Hardening Checklists	193
System Assessment and Hardening Concepts	194
System and Host Hardening Methodology	196
Checklists	196
Microsoft Windows	197
UNIX	199
Web Server	203
FTP Service	205

	DNS	206
	Mail	206
	Router	207
	Wired Network	209
	Wireless Network	211
	Physical Security	212
	Summary	215
■	Appendix: Web Resources	217
	Various Security News and Informational Sites	218
	Exploits and Hacking Information	219
	Various Word Lists for Brute-Forcing	219
	Default Password Lists	219
	Lookup Port Numbers	220
	Information about Trojan Horses	220
	Education/Certification/Organizations	220
	Publications	221
	Security Mailing Lists	221
	Conferences	221
	Government Affiliated	221
	Miscellaneous Interesting Items	222
■	Index	223