



Contents at a Glance

Foreword	xviii
Introduction	xx
Chapter 1 Hacking a Business Case	1
Chapter 2 Hacking Ethically and Legally	13
Chapter 3 Building Your Hack Box	23
Chapter 4 Open Source Intelligence Gathering	55
Chapter 5 The Domain Name System	87
Chapter 6 Electronic Mail	135
Chapter 7 The World Wide Web of Vulnerabilities	191
Chapter 8 Virtual Private Networks	251
Chapter 9 Files and File Sharing	283
Chapter 10 UNIX	315
Chapter 11 Databases	355
Chapter 12 Web Applications	395
Chapter 13 Microsoft Windows	457
Chapter 14 Passwords	517
Chapter 15 Writing Reports	543
Index	561



Contents

Foreword		xviii
Introduction		xx
Chapter 1	Hacking a Business Case	1
	All Computers Are Broken	2
	The Stakes	4
	What's Stolen and Why It's Valuable	4
	The Internet of Vulnerable Things	4
	Blue, Red, and Purple Teams	5
	Blue Teams	5
	Red Teams	5
	Purple Teams	7
	Hacking is Part of Your Company's Immune System	9
	Summary	11
	Notes	12
Chapter 2	Hacking Ethically and Legally	13
	Laws That Affect Your Work	14
	Criminal Hacking	15
	Hacking Neighborly	15
	Legally Gray	16
	Penetration Testing Methodologies	17
	Authorization	18
	Responsible Disclosure	19
	Bug Bounty Programs	20
	Legal Advice and Support	21
	Hacker House Code of Conduct	22
	Summary	22

Chapter 3	Building Your Hack Box	23
	Hardware for Hacking	24
	Linux or BSD?	26
	Host Operating Systems	27
	Gentoo Linux	27
	Arch Linux	28
	Debian	28
	Ubuntu	28
	Kali Linux	29
	Verifying Downloads	29
	Disk Encryption	31
	Essential Software	33
	Firewall	34
	Password Manager	35
	Email	36
	Setting Up VirtualBox	36
	Virtualization Settings	37
	Downloading and Installing VirtualBox	37
	Host-Only Networking	37
	Creating a Kali Linux VM	40
	Creating a Virtual Hard Disk	42
	Inserting a Virtual CD	43
	Virtual Network Adapters	44
	Labs	48
	Guest Additions	51
	Testing Your Virtual Environment	52
	Creating Vulnerable Servers	53
	Summary	54
Chapter 4	Open Source Intelligence Gathering	55
	Does Your Client Need an OSINT Review?	56
	What Are You Looking For?	57
	Where Do You Find It?	58
	OSINT Tools	59
	Grabbing Email Addresses from Google	59
	Google Dorking the Shadows	62
	A Brief Introduction to Passwd and Shadow Files	62
	The Google Hacking Database	65
	Have You Been "Pwned" Yet?	66
	OSINT Framework Recon-ng	67
	Recon-ng Under the Hood	74
	Harvesting the Web	75
	Document Metadata	76
	Maltego	80
	Social Media Networks	81
	Shodan	83
	Protecting Against OSINT	85
	Summary	86

Chapter 5	The Domain Name System	87
	The Implications of Hacking DNS	87
	A Brief History of DNS	88
	The DNS Hierarchy	88
	A Basic DNS Query	89
	Authority and Zones	92
	DNS Resource Records	92
	BIND9	95
	DNS Hacking Toolkit	98
	Finding Hosts	98
	WHOIS	98
	Brute-Forcing Hosts with Recon-ng	100
	Host	101
	Finding the SOA with Dig	102
	Hacking a Virtual Name Server	103
	Port Scanning with Nmap	104
	Digging for Information	106
	Specifying Resource Records	108
	Information Leak CHAOS	111
	Zone Transfer Requests	113
	Information-Gathering Tools	114
	Fierce	115
	Dnsrecon	116
	Dnsenum	116
	Searching for Vulnerabilities and Exploits	118
	Searchsploit	118
	Other Sources	119
	DNS Traffic Amplification	120
	Metasploit	121
	Carrying Out a Denial-of-Service Attack	125
	DoS Attacks with Metasploit	126
	DNS Spoofing	128
	DNS Cache Poisoning	129
	DNS Cache Snooping	131
	DNSSEC	131
	Fuzzing	132
	Summary	134
Chapter 6	Electronic Mail	135
	The Email Chain	135
	Message Headers	137
	Delivery Status Notifications	138
	The Simple Mail Transfer Protocol	141
	Sender Policy Framework	143
	Scanning a Mail Server	145
	Complete Nmap Scan Results (TCP)	149
	Probing the SMTP Service	152

Open Relays	153	
The Post Office Protocol	155	
The Internet Message Access Protocol	157	
Mail Software	158	
Exim	159	
Sendmail	159	
Cyrus	160	
PHP Mail	160	
Webmail	161	
User Enumeration via Finger	162	
Brute-Forcing the Post Office	167	
The Nmap Scripting Engine	169	
CVE-2014-0160: The Heartbleed Bug	172	
Exploiting CVE-2010-4345	180	
Got Root?	183	
Upgrading Your Shell	184	
Exploiting CVE-2017-7692	185	
Summary	188	
Chapter 7	The World Wide Web of Vulnerabilities	191
The World Wide Web	192	
The Hypertext Transfer Protocol	193	
HTTP Methods and Verbs	195	
HTTP Response Codes	196	
Stateless	198	
Cookies	198	
Uniform Resource Identifiers	200	
LAMP: Linux, Apache, MySQL, and PHP	201	
Web Server: Apache	202	
Database: MySQL	203	
Server-Side Scripting: PHP	203	
Nginx	205	
Microsoft IIS	205	
Creepy Crawlers and Spiders	206	
The Web Server Hacker's Toolkit	206	
Port Scanning a Web Server	207	
Manual HTTP Requests	210	
Web Vulnerability Scanning	212	
Guessing Hidden Web Content	216	
Nmap	217	
Directory Busting	218	
Directory Traversal Vulnerabilities	219	
Uploading Files	220	
WebDAV	220	
Web Shell with Weevely	222	
HTTP Authentication	223	
Common Gateway Interface	225	

	Shellshock	226
	Exploiting Shellshock Using Metasploit	227
	Exploiting Shellshock with cURL and Netcat	228
	SSL, TLS, and Heartbleed	232
	Web Administration Interfaces	238
	Apache Tomcat	238
	Webmin	240
	phpMyAdmin	241
	Web Proxies	242
	Proxychains	243
	Privilege Escalation	245
	Privilege Escalation Using DirtyCOW	246
	Summary	249
Chapter 8	Virtual Private Networks	251
	What Is a VPN?	251
	Internet Protocol Security	253
	Internet Key Exchange	253
	Transport Layer Security and VPNs	254
	User Databases and Authentication	255
	SQL Database	255
	RADIUS	255
	LDAP	256
	PAM	256
	TACACS+	256
	The NSA and VPNs	257
	The VPN Hacker's Toolkit	257
	VPN Hacking Methodology	257
	Port Scanning a VPN Server	258
	Hping3	259
	UDP Scanning with Nmap	261
	IKE-scan	262
	Identifying Security Association Options	263
	Aggressive Mode	265
	OpenVPN	267
	LDAP	275
	OpenVPN and Shellshock	277
	Exploiting CVE-2017-5618	278
	Summary	281
Chapter 9	Files and File Sharing	283
	What Is Network-Attached Storage?	284
	File Permissions	284
	NAS Hacking Toolkit	287
	Port Scanning a File Server	288
	The File Transfer Protocol	289

	The Trivial File Transfer Protocol	291
	Remote Procedure Calls	292
	RPCinfo	294
	Server Message Block	295
	NetBIOS and NBT	296
	Samba Setup	298
	Enum4Linux	299
	SambaCry (CVE-2017-7494)	303
	Rsync	306
	Network File System	308
	NFS Privilege Escalation	309
	Searching for Useful Files	311
	Summary	312
Chapter 10	UNIX	315
	UNIX System Administration	316
	Solaris	316
	UNIX Hacking Toolbox	318
	Port Scanning Solaris	319
	Telnet	320
	Secure Shell	324
	RPC	326
	CVE-2010-4435	329
	CVE-1999-0209	329
	CVE-2017-3623	330
	Hacker's Holy Grail EBBSHAVE	331
	EBBSHAVE Version 4	332
	EBBSHAVE Version 5	335
	Debugging EBBSHAVE	335
	R-services	338
	The Simple Network Management Protocol	339
	Ewok	341
	The Common UNIX Printing System	341
	The X Window System	343
	Cron and Local Files	347
	The Common Desktop Environment	351
	EXTREMEPARR	351
	Summary	353
Chapter 11	Databases	355
	Types of Databases	356
	Flat-File Databases	356
	Relational Databases	356
	Nonrelational Databases	358
	Structured Query Language	358
	User-Defined Functions	359
	The Database Hacker's Toolbox	360
	Common Database Exploitation	360

Port Scanning a Database Server	361
MySQL	362
Exploring a MySQL Database	362
MySQL Authentication	373
PostgreSQL	374
Escaping Database Software	377
Oracle Database	378
MongoDB	381
Redis	381
Privilege Escalation via Databases	384
Summary	392
Chapter 12 Web Applications	395
The OWASP Top 10	396
The Web Application Hacker's Toolkit	397
Port Scanning a Web Application Server	397
Using an Intercepting Proxy	398
Setting Up Burp Suite Community Edition	399
Using Burp Suite Over HTTPS	407
Manual Browsing and Mapping	412
Spidering	415
Identifying Entry Points	418
Web Vulnerability Scanners	418
Zed Attack Proxy	419
Burp Suite Professional	420
Skipfish	421
Finding Vulnerabilities	421
Injection	421
SQL Injection	422
SQLmap	427
Drupageddon	433
Protecting Against SQL Injection	433
Other Injection Flaws	434
Broken Authentication	434
Sensitive Data Exposure	436
XML External Entities	437
CVE-2014-3660	437
Broken Access Controls	439
Directory Traversal	440
Security Misconfiguration	441
Error Pages and Stack Traces	442
Cross-Site Scripting	442
The Browser Exploitation Framework	445
More about XSS Flaws	450
XSS Filter Evasion	450
Insecure Deserialization	452
Known Vulnerabilities	453
Insufficient Logging and Monitoring	453

	Privilege Escalation	454
	Summary	455
Chapter 13	Microsoft Windows	457
	Hacking Windows vs. Linux	458
	Domains, Trees, and Forests	458
	Users, Groups, and Permissions	461
	Password Hashes	461
	Antivirus Software	462
	Bypassing User Account Control	463
	Setting Up a Windows VM	464
	A Windows Hacking Toolkit	466
	Windows and the NSA	467
	Port Scanning Windows Server	467
	Microsoft DNS	469
	Internet Information Services	470
	Kerberos	471
	Golden Tickets	472
	NetBIOS	473
	LDAP	474
	Server Message Block	474
	ETERNALBLUE	476
	Enumerating Users	479
	Microsoft RPC	489
	Task Scheduler	497
	Remote Desktop	497
	The Windows Shell	498
	PowerShell	501
	Privilege Escalation with PowerShell	502
	PowerSploit and AMSI	503
	Meterpreter	504
	Hash Dumping	505
	Passing the Hash	506
	Privilege Escalation	507
	Getting SYSTEM	508
	Alternative Payload Delivery Methods	509
	Bypassing Windows Defender	512
	Summary	514
Chapter 14	Passwords	517
	Hashing	517
	The Password Cracker's Toolbox	519
	Cracking	519
	Hash Tables and Rainbow Tables	523
	Adding Salt	525
	Into the <i>/etc/shadow</i>	526
	Different Hash Types	530

MD5	530
SHA-1	531
SHA-2	531
SHA256	531
SHA512	531
bcrypt	531
CRC16/CRC32	532
PBKDF2	532
Collisions	533
Pseudo-hashing	533
Microsoft Hashes	535
Guessing Passwords	537
The Art of Cracking	538
Random Number Generators	539
Summary	540
Chapter 15 Writing Reports	543
What Is a Penetration Test Report?	544
Common Vulnerabilities Scoring System	545
Attack Vector	545
Attack Complexity	546
Privileges Required	546
User Interaction	547
Scope	547
Confidentiality, Integrity, and Availability Impact	547
Report Writing as a Skill	549
What Should a Report Include?	549
Executive Summary	550
Technical Summary	551
Assessment Results	551
Supporting Information	552
Taking Notes	553
Dradis Community Edition	553
Proofreading	557
Delivery	558
Summary	559
Index	561