

Table of Contents

Preface	1
Chapter 1: Installing and Configuring Kali Linux	7
Technical requirements	7
Kali Linux tool categories	8
Downloading Kali Linux	10
Using Kali Linux	14
Running Kali using a Live DVD	15
Installing on a hard disk	15
Installing Kali on a physical machine	15
Installing Kali on a virtual machine	20
Installing Kali on a virtual machine from the ISO image	20
Installing Kali Linux on a virtual machine using the Kali Linux VM image provided	26
Saving or moving the virtual machine	30
Installing Kali on a USB disk	30
Configuring the virtual machine	33
VirtualBox guest additions	33
Setting up networking	35
Setting up a wired connection	35
Setting up a wireless connection	36
Updating Kali Linux	39
Setting up Kali Linux AMI on Amazon AWS Cloud	40
Summary	52
Questions	53
Further reading	53
Chapter 2: Setting Up Your Test Lab	55
Technical requirements	55
Physical or virtual?	56
Setting up a Windows environment in a VM	57
Installing vulnerable servers	62
Setting up Metasploitable 2 in a VM	62
Setting up Metasploitable 3 in a VM	64
Installing Packer	65
Installing Vagrant	68
Pre-built Metasploit 3	69
Setting up BadStore in a VM	70
Installing additional tools in Kali Linux	77
Network services in Kali Linux	78
HTTP	78

MySQL	80
SSH	81
Additional labs and resources	82
Summary	84
Questions	85
Further reading	85
Chapter 3: Penetration Testing Methodology	87
Technical requirements	87
Penetration testing methodology	88
OWASP testing guide	89
PCI penetration testing guide	89
Penetration Testing Execution Standard	90
NIST 800-115	91
Open Source Security Testing Methodology Manual	91
General penetration testing framework	92
Reconnaissance	92
Scanning and enumeration	93
Scanning	94
ARP scanning	94
The network mapper (Nmap)	94
Nmap half-open/stealth scan	95
Nmap OS-detection	96
Nmap service-detection	96
Nmap ping sweeps	96
Enumeration	97
SMB shares	98
DNS zone transfer	98
DNSRecon	98
Packet captures	99
tcpdump	100
Wireshark	100
Gaining access	101
Exploits	101
Exploits for Linux	101
Exploits for Windows	102
Escalating privileges	106
Maintaining access	106
Covering your tracks	107
Reporting	108
Summary	108
Chapter 4: Footprinting and Information Gathering	109
Open Source Intelligence	110
Using public resources	110
Querying the domain registration information	111
Analyzing the DNS records	113

Host	113
dig	115
DMitry	115
Maltego	118
Getting network routing information	126
tcptraceroute	126
tctrace	128
Utilizing the search engine	129
SimplyEmail	129
Google Hacking Database (GHDB)	131
Metagoofil	134
Automated footprinting and information gathering tools	137
Devploit	137
Red Hawk v2	141
Using Shodan to find internet connected devices	145
Search queries in Shodan	146
Blue-Thunder-IP-Locator	147
Summary	150
Questions	151
Further reading	151
Chapter 5: Scanning and Evasion Techniques	153
Technical requirements	153
Starting off with target discovery	154
Identifying the target machine	154
ping	155
fping	158
hping3	160
OS fingerprinting	163
p0f	164
Introducing port scanning	167
Understanding TCP/IP protocol	168
Understanding TCP and UDP message formats	170
The network scanner	173
Nmap	174
Nmap target specification	176
Nmap TCP scan options	179
Nmap UDP scan options	180
Nmap port specification	181
Nmap output options	183
Nmap timing options	186
Useful Nmap options	186
Service version detection	187
Operating system detection	187
Disabling host discovery	189

Aggressive scan	189
Nmap for scanning the IPv6 target	190
The Nmap scripting engine	191
Nmap options for firewall/IDS evasion	196
Scanning with Netdiscover	197
Automated scanning with Striker	198
Anonymity using Nipe	202
Summary	205
Questions	205
Further Reading	206
Chapter 6: Vulnerability Scanning	207
Technical requirements	208
Types of vulnerabilities	208
Local vulnerability	208
Remote vulnerability	209
Vulnerability taxonomy	210
Automated vulnerability scanning	211
Vulnerability scanning with Nessus 7	211
Installing the Nessus vulnerability scanner	211
Vulnerability scanning with OpenVAS	221
Linux vulnerability scanning with Lynis	228
Vulnerability scanning and enumeration using SPARTA	233
Summary	240
Questions	240
Further reading	240
Chapter 7: Social Engineering	241
Technical requirements	242
Modeling human psychology	242
Attack process	243
Attack methods	244
Impersonation	244
Reciprocation	244
Influential authority	245
Scarcity	245
Social relationships	246
Curiosity	247
Social Engineering Toolkit	247
Anonymous USB attack	249
Credential-harvesting	253
Malicious Java applet	257
Summary	262
Chapter 8: Target Exploitation	263

Vulnerability research	264
Vulnerability and exploit repositories	265
Advanced exploitation toolkit	267
MSFConsole	268
MSFCLI	270
Ninja 101 drills	271
Scenario 1	272
Scenario 2	273
SMB usernames	273
VNC blank authentication scanners	274
PostGRESQL logins	275
Scenario 3	276
Bind shells	277
Reverse shells	278
Meterpreters	279
Writing exploit modules	284
Summary	290
Chapter 9: Privilege Escalation and Maintaining Access	291
Technical requirements	291
Privilege-escalation	291
Local escalation	292
Password-attack tools	297
Offline attack tools	298
John the Ripper	298
Ophcrack	303
samdump2	304
Online attack tools	306
CeWL	306
Hydra	308
Mimikatz	310
Maintaining access	313
Operating-system backdoors	313
Cymothoa	313
The Meterpreter backdoor	316
Summary	319
Chapter 10: Web Application Testing	321
Technical requirements	321
Web analysis	322
Nikto	322
OWASP ZAP	325
Burp Suite	327
Paros proxy	341
W3AF	342
WebScarab	345

Cross-Site Scripting	347
Testing for XSS	347
SQL injection	351
Manual SQL injection	353
Automated SQL injection	355
sqlmap	355
Command-execution, directory-traversal, and file-inclusion	359
Directory-traversal and file-inclusion	360
Command execution	363
Summary	368
Further reading	368
Chapter 11: Wireless Penetration Testing	369
Technical requirements	370
Wireless networking	370
Overview of 802.11	370
The Wired Equivalent Privacy standard	371
Wi-Fi Protected Access (WPA)	372
Wireless network reconnaissance	374
Antennas	374
Iwlist	374
Kismet	375
WAIDPS	378
Wireless testing tools	381
Aircrack-ng	381
WPA pre-shared key-cracking	382
WEP-cracking	390
PixieWPS	395
Wifite	395
Fern Wifi-Cracker	397
Evil Twin attack	401
Post cracking	406
MAC-spoofing	406
Persistence	407
Sniffing wireless traffic	410
Sniffing WLAN traffic	411
Passive sniffing	416
Summary	419
Chapter 12: Mobile Penetration Testing with Kali NetHunter	421
Technical requirements	421
Kali NetHunter	422
Deployment	422
Network deployment	422
Wireless deployment	422
Host deployment	423

Installing Kali NetHunter	423
NetHunter icons	424
NetHunter tools	426
Nmap	427
Metasploit	430
MAC changer	433
Third-party Android applications	434
The NetHunter Terminal Application	434
DriveDroid	435
USB Keyboard	435
Shodan	436
Router Keygen	437
cSploit	438
Wireless attacks	440
Wireless scanning	440
WPA/WPA2 cracking	441
WPS cracking	443
Evil AP attack	445
Mana evil AP	445
HID attacks	450
DuckHunter HID attacks	453
Summary	454
Questions	454
Further reading	454
Chapter 13: PCI DSS Scanning and Penetration Testing	455
PCI DSS v3.2.1 requirement 11.3	457
Scoping the PCI DSS penetration test	458
Gathering client requirements	459
Creating the customer requirements form	460
Preparing the test plan	461
The test plan checklist	463
Profiling test boundaries	464
Defining business objectives	465
Project management and scheduling	466
Tools for executing the PCI DSS penetration test	467
Summary	469
Questions	470
Further reading	470
Chapter 14: Tools for Penetration Testing Reporting	471
Technical requirements	472
Documentation and results verification	472
Types of reports	473
The executive report	474

The management report	475
The technical report	476
Network penetration testing report	477
Preparing your presentation	478
Post-testing procedures	478
Using the Dradis framework for penetration testing reporting	480
Penetration testing reporting tools	486
Faraday IDE	487
MagicTree	488
Summary	489
Questions	489
Further reading	489
Assessments	491
Other Books You May Enjoy	495
Index	499
