

# CONTENTS IN DETAIL

<b>FOREWORD</b> by Peter Van Eeckhoutte	<b>xix</b>
-----------------------------------------	------------

<b>ACKNOWLEDGMENTS</b>	<b>xxiii</b>
------------------------	--------------

<b>INTRODUCTION</b>	<b>xxv</b>
---------------------	------------

A Note of Thanks . . . . .	xxvi
About This Book . . . . .	xxvi
Part I: The Basics . . . . .	xxvii
Part II: Assessments . . . . .	xxvii
Part III: Attacks . . . . .	xxvii
Part IV: Exploit Development . . . . .	xxviii
Part V: Mobile Hacking . . . . .	xxviii

<b>0</b>	
<b>PENETRATION TESTING PRIMER</b>	<b>1</b>

The Stages of the Penetration Test . . . . .	2
Pre-engagement . . . . .	2
Information Gathering . . . . .	4
Threat Modeling . . . . .	4
Vulnerability Analysis . . . . .	4
Exploitation . . . . .	4
Post Exploitation . . . . .	4
Reporting . . . . .	5
Summary . . . . .	6

## **PART I** **THE BASICS**

<b>1</b>	
<b>SETTING UP YOUR VIRTUAL LAB</b>	<b>9</b>

Installing VMware . . . . .	9
Setting Up Kali Linux . . . . .	10
Configuring the Network for Your Virtual Machine . . . . .	13
Installing Nessus . . . . .	17
Installing Additional Software . . . . .	20
Setting Up Android Emulators . . . . .	22
Smartphone Pentest Framework . . . . .	27
Target Virtual Machines . . . . .	28
Creating the Windows XP Target . . . . .	29
VMware Player on Microsoft Windows . . . . .	29
VMware Fusion on Mac OS . . . . .	31
Installing and Activating Windows . . . . .	32

Installing VMware Tools . . . . .	35
Turning Off Windows Firewall . . . . .	37
Setting User Passwords . . . . .	37
Setting a Static IP Address . . . . .	38
Making XP Act Like It's a Member of a Windows Domain . . . . .	39
Installing Vulnerable Software . . . . .	40
Installing Immunity Debugger and Mona . . . . .	46
Setting Up the Ubuntu 8.10 Target . . . . .	48
Creating the Windows 7 Target . . . . .	48
Creating a User Account . . . . .	48
Opting Out of Automatic Updates . . . . .	50
Setting a Static IP Address . . . . .	51
Adding a Second Network Interface . . . . .	52
Installing Additional Software . . . . .	52
Summary . . . . .	54

## **2 USING KALI LINUX 55**

Linux Command Line . . . . .	56
The Linux Filesystem . . . . .	56
Changing Directories . . . . .	56
Learning About Commands: The Man Pages . . . . .	57
User Privileges . . . . .	58
Adding a User . . . . .	58
Adding a User to the sudoers File . . . . .	59
Switching Users and Using sudo . . . . .	59
Creating a New File or Directory . . . . .	60
Copying, Moving, and Removing Files . . . . .	60
Adding Text to a File . . . . .	61
Appending Text to a File . . . . .	61
File Permissions . . . . .	61
Editing Files . . . . .	62
Searching for Text . . . . .	63
Editing a File with vi . . . . .	63
Data Manipulation . . . . .	64
Using grep . . . . .	65
Using sed . . . . .	65
Pattern Matching with awk . . . . .	66
Managing Installed Packages . . . . .	66
Processes and Services . . . . .	67
Managing Networking . . . . .	67
Setting a Static IP Address . . . . .	68
Viewing Network Connections . . . . .	69
Netcat: The Swiss Army Knife of TCP/IP Connections . . . . .	69
Check to See If a Port Is Listening . . . . .	70
Opening a Command Shell Listener . . . . .	70
Pushing a Command Shell Back to a Listener . . . . .	71
Automating Tasks with cron Jobs . . . . .	72
Summary . . . . .	73

<b>3</b>		
<b>PROGRAMMING</b>		<b>75</b>
Bash Scripting . . . . .		75
Ping . . . . .		76
A Simple Bash Script . . . . .		76
Running Our Script . . . . .		77
Adding Functionality with if Statements . . . . .		77
A for Loop . . . . .		78
Streamlining the Results . . . . .		79
Python Scripting . . . . .		81
Connecting to a Port . . . . .		83
if Statements in Python . . . . .		83
Writing and Compiling C Programs . . . . .		84
Summary . . . . .		85

<b>4</b>		
<b>USING THE METASPLOIT FRAMEWORK</b>		<b>87</b>
Starting Metasploit . . . . .		88
Finding Metasploit Modules . . . . .		90
The Module Database . . . . .		90
Built-In Search . . . . .		91
Setting Module Options . . . . .		94
RHOST . . . . .		94
RPORT . . . . .		95
SMBPIPE . . . . .		95
Exploit Target . . . . .		95
Payloads (or Shellcode) . . . . .		96
Finding Compatible Payloads . . . . .		96
A Test Run . . . . .		97
Types of Shells . . . . .		98
Bind Shells . . . . .		98
Reverse Shells . . . . .		98
Setting a Payload Manually . . . . .		99
Msfcli . . . . .		101
Getting Help . . . . .		101
Showing Options . . . . .		101
Payloads . . . . .		102
Creating Standalone Payloads with Msfvenom . . . . .		103
Choosing a Payload . . . . .		104
Setting Options . . . . .		104
Choosing an Output Format . . . . .		104
Serving Payloads . . . . .		105
Using the Multi/Handler Module . . . . .		105
Using an Auxiliary Module . . . . .		107
Summary . . . . .		109

## **PART II ASSESSMENTS**

### **5 INFORMATION GATHERING 113**

Open Source Intelligence Gathering . . . . .	114
Netcraft . . . . .	114
Whois Lookups . . . . .	115
DNS Reconnaissance . . . . .	116
Searching for Email Addresses . . . . .	118
Maltego . . . . .	119
Port Scanning . . . . .	123
Manual Port Scanning . . . . .	124
Port Scanning with Nmap . . . . .	125
Summary . . . . .	132

### **6 FINDING VULNERABILITIES 133**

From Nmap Version Scan to Potential Vulnerability . . . . .	133
Nessus . . . . .	134
Nessus Policies . . . . .	134
Scanning with Nessus . . . . .	138
A Note About Nessus Rankings . . . . .	140
Why Use Vulnerability Scanners? . . . . .	141
Exporting Nessus Results . . . . .	141
Researching Vulnerabilities . . . . .	142
The Nmap Scripting Engine . . . . .	142
Running a Single NSE Script . . . . .	144
Metasploit Scanner Modules . . . . .	146
Metasploit Exploit Check Functions . . . . .	147
Web Application Scanning . . . . .	148
Nikto . . . . .	149
Attacking XAMPP . . . . .	149
Default Credentials . . . . .	150
Manual Analysis . . . . .	151
Exploring a Strange Port . . . . .	151
Finding Valid Usernames . . . . .	153
Summary . . . . .	153

### **7 CAPTURING TRAFFIC 155**

Networking for Capturing Traffic . . . . .	156
Using Wireshark . . . . .	156
Capturing Traffic . . . . .	156
Filtering Traffic . . . . .	158
Following a TCP Stream . . . . .	159
Dissecting Packets . . . . .	160

ARP Cache Poisoning . . . . .	160
ARP Basics . . . . .	161
IP Forwarding . . . . .	163
ARP Cache Poisoning with Arpspoof . . . . .	164
Using ARP Cache Poisoning to Impersonate the Default Gateway . . . . .	165
DNS Cache Poisoning . . . . .	167
Getting Started . . . . .	168
Using Dnsspoof . . . . .	169
SSL Attacks . . . . .	170
SSL Basics . . . . .	170
Using Ettercap for SSL Man-in-the-Middle Attacks . . . . .	171
SSL Stripping . . . . .	173
Using SSLstrip . . . . .	174
Summary . . . . .	175

## **PART III ATTACKS**

### **8 EXPLOITATION 179**

Revisiting MS08-067 . . . . .	180
Metasploit Payloads . . . . .	180
Meterpreter . . . . .	181
Exploiting WebDAV Default Credentials . . . . .	182
Running a Script on the Target Web Server . . . . .	183
Uploading a Msfvenom Payload . . . . .	183
Exploiting Open phpMyAdmin . . . . .	186
Downloading a File with TFTP . . . . .	187
Downloading Sensitive Files . . . . .	188
Downloading a Configuration File . . . . .	188
Downloading the Windows SAM . . . . .	189
Exploiting a Buffer Overflow in Third-Party Software . . . . .	190
Exploiting Third-Party Web Applications . . . . .	191
Exploiting a Compromised Service . . . . .	193
Exploiting Open NFS Shares . . . . .	194
Summary . . . . .	196

### **9 PASSWORD ATTACKS 197**

Password Management . . . . .	197
Online Password Attacks . . . . .	198
Wordlists . . . . .	199
Guessing Usernames and Passwords with Hydra . . . . .	202
Offline Password Attacks . . . . .	203
Recovering Password Hashes from a Windows SAM File . . . . .	204
Dumping Password Hashes with Physical Access . . . . .	206
LM vs. NTLM Hashing Algorithms . . . . .	208
The Trouble with LM Password Hashes . . . . .	209

John the Ripper . . . . .	210
Cracking Linux Passwords . . . . .	212
Cracking Configuration File Passwords . . . . .	212
Rainbow Tables . . . . .	213
Online Password-Cracking Services . . . . .	213
Dumping Plaintext Passwords from Memory with Windows Credential Editor . . . . .	213
Summary . . . . .	214

## **10**

### **CLIENT-SIDE EXPLOITATION** **215**

Bypassing Filters with Metasploit Payloads . . . . .	216
All Ports . . . . .	216
HTTP and HTTPS Payloads . . . . .	217
Client-Side Attacks . . . . .	218
Browser Exploitation . . . . .	219
PDF Exploits . . . . .	225
Java Exploits . . . . .	230
browser_autopwn . . . . .	235
Winamp . . . . .	237
Summary . . . . .	240

## **11**

### **SOCIAL ENGINEERING** **243**

The Social-Engineer Toolkit . . . . .	244
Spear-Phishing Attacks . . . . .	245
Choosing a Payload . . . . .	246
Setting Options . . . . .	247
Naming Your File . . . . .	247
Single or Mass Email . . . . .	247
Creating the Template . . . . .	248
Setting the Target . . . . .	248
Setting Up a Listener . . . . .	249
Web Attacks . . . . .	250
Mass Email Attacks . . . . .	253
Multipronged Attacks . . . . .	255
Summary . . . . .	255

## **12**

### **BYPASSING ANTIVIRUS APPLICATIONS** **257**

Trojans . . . . .	258
Msfnvenom . . . . .	258
How Antivirus Applications Work . . . . .	260
Microsoft Security Essentials . . . . .	261
VirusTotal . . . . .	262
Getting Past an Antivirus Program . . . . .	263
Encoding . . . . .	263
Custom Cross Compiling . . . . .	266
Encrypting Executables with Hyperion . . . . .	269
Evading Antivirus with Veil-Evasion . . . . .	270

Hiding in Plain Sight . . . . .	274
Summary . . . . .	274

## **13 POST EXPLOITATION 277**

Meterpreter . . . . .	278
Using the upload Command . . . . .	279
getuid . . . . .	279
Other Meterpreter Commands . . . . .	280
Meterpreter Scripts . . . . .	280
Metasploit Post-Exploitation Modules . . . . .	281
Railgun . . . . .	283
Local Privilege Escalation . . . . .	283
getsystem on Windows . . . . .	283
Local Escalation Module for Windows . . . . .	284
Bypassing UAC on Windows . . . . .	285
Udev Privilege Escalation on Linux . . . . .	287
Local Information Gathering . . . . .	291
Searching for Files . . . . .	291
Keylogging . . . . .	292
Gathering Credentials . . . . .	292
net Commands . . . . .	294
Another Way In . . . . .	295
Checking Bash History . . . . .	295
Lateral Movement . . . . .	296
PSEXec . . . . .	296
Pass the Hash . . . . .	298
SSHExec . . . . .	299
Token Impersonation . . . . .	300
Incognito . . . . .	301
SMB Capture . . . . .	302
Pivoting . . . . .	304
Adding a Route in Metasploit . . . . .	305
Metasploit Port Scanners . . . . .	306
Running an Exploit through a Pivot . . . . .	306
Socks4a and ProxyChains . . . . .	307
Persistence . . . . .	309
Adding a User . . . . .	309
Metasploit Persistence . . . . .	310
Creating a Linux cron Job . . . . .	311
Summary . . . . .	311

## **14 WEB APPLICATION TESTING 313**

Using Burp Proxy . . . . .	314
SQL Injection . . . . .	319
Testing for SQL Injection Vulnerabilities . . . . .	320
Exploiting SQL Injection Vulnerabilities . . . . .	321
Using SQLMap . . . . .	321
XPath Injection . . . . .	323

Local File Inclusion . . . . .	324
Remote File Inclusion . . . . .	327
Command Execution . . . . .	327
Cross-Site Scripting . . . . .	329
Checking for a Reflected XSS Vulnerability . . . . .	330
Leveraging XSS with the Browser Exploitation Framework . . . . .	331
Cross-Site Request Forgery . . . . .	335
Web Application Scanning with w3af . . . . .	335
Summary . . . . .	337

## **15 WIRELESS ATTACKS 339**

Setting Up . . . . .	339
Viewing Available Wireless Interfaces . . . . .	340
Scan for Access Points . . . . .	341
Monitor Mode . . . . .	341
Capturing Packets . . . . .	342
Open Wireless . . . . .	343
Wired Equivalent Privacy . . . . .	343
WEP Weaknesses . . . . .	346
Cracking WEP Keys with Aircrack-ng . . . . .	347
Wi-Fi Protected Access . . . . .	350
WPA2 . . . . .	351
The Enterprise Connection Process . . . . .	351
The Personal Connection Process . . . . .	351
The Four-Way Handshake . . . . .	352
Cracking WPA/WPA2 Keys . . . . .	353
Wi-Fi Protected Setup . . . . .	356
Problems with WPS . . . . .	356
Cracking WPS with Bully . . . . .	357
Summary . . . . .	357

## **PART IV EXPLOIT DEVELOPMENT**

### **16 A STACK-BASED BUFFER OVERFLOW IN LINUX 361**

Memory Theory . . . . .	362
Linux Buffer Overflow . . . . .	364
A Vulnerable Program . . . . .	365
Causing a Crash . . . . .	366
Running GDB . . . . .	367
Crashing the Program in GDB . . . . .	372



Controlling EIP . . . . .	373
Hijacking Execution . . . . .	375
Endianness . . . . .	376
Summary . . . . .	378

**17**  
**A STACK-BASED BUFFER OVERFLOW IN WINDOWS 379**

Searching for a Known Vulnerability in War-FTP . . . . .	380
Causing a Crash . . . . .	382
Locating EIP . . . . .	384
Generating a Cyclical Pattern to Determine Offset . . . . .	385
Verifying Offsets . . . . .	388
Hijacking Execution . . . . .	390
Getting a Shell . . . . .	395
Summary . . . . .	400

**18**  
**STRUCTURED EXCEPTION HANDLER OVERWRITES 401**

SEH Overwrite Exploits . . . . .	403
Passing Control to SEH . . . . .	407
Finding the Attack String in Memory . . . . .	408
POP POP RET . . . . .	411
SafeSEH . . . . .	412
Using a Short Jump . . . . .	416
Choosing a Payload . . . . .	418
Summary . . . . .	419

**19**  
**FUZZING, PORTING EXPLOITS, AND METASPLOIT MODULES 421**

Fuzzing Programs . . . . .	421
Finding Bugs with Code Review . . . . .	422
Fuzzing a Trivial FTP Server . . . . .	422
Attempting a Crash . . . . .	424
Porting Public Exploits to Meet Your Needs . . . . .	427
Finding a Return Address . . . . .	429
Replacing Shellcode . . . . .	430
Editing the Exploit . . . . .	430
Writing Metasploit Modules . . . . .	432
A Similar Exploit String Module . . . . .	435
Porting Our Exploit Code . . . . .	435
Exploitation Mitigation Techniques . . . . .	439
Stack Cookies . . . . .	440
Address Space Layout Randomization . . . . .	440
Data Execution Prevention . . . . .	441
Mandatory Code Signing . . . . .	441
Summary . . . . .	442

# **PART V MOBILE HACKING**

## **20 USING THE SMARTPHONE PENTEST FRAMEWORK 445**

Mobile Attack Vectors . . . . .	446
Text Messages . . . . .	446
Near Field Communication . . . . .	446
QR Codes . . . . .	447
The Smartphone Pentest Framework . . . . .	447
Setting Up SPF . . . . .	447
Android Emulators . . . . .	449
Attaching a Mobile Modem . . . . .	449
Building the Android App . . . . .	449
Deploying the App . . . . .	450
Attaching the SPF Server and App . . . . .	452
Remote Attacks . . . . .	453
Default iPhone SSH Login . . . . .	453
Client-Side Attacks . . . . .	454
Client-Side Shell . . . . .	454
USSD Remote Control . . . . .	456
Malicious Apps . . . . .	458
Creating Malicious SPF Agents . . . . .	459
Mobile Post Exploitation . . . . .	464
Information Gathering . . . . .	464
Remote Control . . . . .	465
Pivoting Through Mobile Devices . . . . .	466
Privilege Escalation . . . . .	471
Summary . . . . .	472

## **RESOURCES 473**

## **INDEX 477**