

# CONTENTS IN DETAIL

<b>ACKNOWLEDGMENTS</b>	<b>xvii</b>
------------------------	-------------

<b>FOREWORD</b>	<b>xix</b>
-----------------	------------

<b>INTRODUCTION</b>	<b>xxi</b>
---------------------	------------

Why Read This Book? .....	xxii
Installing Python .....	xxii
What Is in the Book? .....	xxii
Part I: Networking Fundamentals .....	xxiii
Part II: Cryptography .....	xxiii
Part III: Social Engineering .....	xxiv
Part IV: Exploitation .....	xxiv
Part V: Controlling the Network .....	xxv
Reaching Out .....	xxv

<b>1</b>	
<b>SETTING UP</b>	<b>1</b>

Virtual Lab .....	2
Setting Up VirtualBox .....	3
Setting Up pfSense .....	3
Setting Up the Internal Network .....	5
Configuring pfSense .....	6
Setting Up Metasploitable .....	8
Setting Up Kali Linux .....	9
Setting Up the Ubuntu Linux Desktop .....	10
Your First Hack: Exploiting a Backdoor in Metasploitable .....	11
Getting the IP Address of the Metasploitable Server .....	12
Using the Backdoor to Gain Access .....	13

## **PART I**

### **NETWORK FUNDAMENTALS**

<b>2</b>		<b>17</b>
<b>CAPTURING TRAFFIC WITH ARP SPOOFING</b>		
How the Internet Transmits Data .....	17	
Packets .....	18	
MAC Addresses .....	18	
IP Addresses .....	18	
ARP Tables .....	20	
ARP Spoofing Attacks .....	21	
Performing an ARP Spoofing Attack .....	21	
Detecting an ARP Spoofing Attack .....	26	
Exercises .....	27	
Inspect ARP Tables .....	27	
Implement an ARP Spoofer in Python .....	28	
MAC Flooding .....	29	
<b>3</b>		<b>31</b>
<b>ANALYZING CAPTURED TRAFFIC</b>		
Packets and the Internet Protocol Stack .....	31	
The Five-Layer Internet Protocol Stack .....	33	
Viewing Packets in Wireshark .....	37	
Analyzing Packets Collected by Your Firewall .....	42	
Capturing Traffic on Port 80 .....	42	
Exercises .....	44	
pfSense .....	44	
Exploring Packets in Wireshark .....	45	
<b>4</b>		<b>47</b>
<b>CRAFTING TCP SHELLS AND BOTNETS</b>		
Sockets and Process Communication .....	48	
TCP Handshakes .....	48	
A TCP Reverse Shell .....	50	
Accessing the Victim Machine .....	52	
Scanning for Open Ports .....	52	
Exploiting a Vulnerable Service .....	54	
Writing a Reverse Shell Client .....	55	
Writing a TCP Server That Listens for Client Connections .....	56	
Loading the Reverse Shell onto the Metasploitable Server .....	57	
Botnets .....	58	
Exercises .....	61	
A Multiclient Bot Server .....	61	
SYN Scans .....	62	
Detecting XMas Scans .....	63	

## PART II CRYPTOGRAPHY

<b>5</b>		
<b>CRYPTOGRAPHY AND RANSOMWARE</b>		<b>67</b>
Encryption	68	
One-Time Pad	68	
Pseudorandom Generators	71	
Insecure Block Ciphers Modes	72	
Secure Block Ciphers Modes	74	
Encrypting and Decrypting a File	75	
Email Encryption	76	
Public-Key Cryptography	76	
Rivest–Shamir–Adleman Theory	77	
The RSA Math	77	
Encrypting a File with RSA	79	
Optimal Asymmetric Encryption Padding	81	
Writing Ransomware	82	
Exercises	85	
The Ransomware Server	85	
Extending the Ransomware Client	86	
Unsolved Codes	86	
<b>6</b>		
<b>TLS AND DIFFIE-HELLMAN</b>		<b>89</b>
Transport Layer Security	90	
Message Authentication	91	
Certificate Authorities and Signatures	92	
Certificate Authorities	93	
Using Diffie-Hellman to Compute a Shared Key	94	
Step 1: Generating the Shared Parameters	95	
Step 2: Generating the Public–Private Key Pair	96	
Why Can’t a Hacker Calculate the Private Key?	97	
Step 3: Exchanging Key Shares and Nonces	98	
Step 4: Calculating the Shared Secret Key	98	
Step 5: Key Derivation	99	
Attacking Diffie-Hellman	100	
Elliptic-Curve Diffie-Hellman	100	
The Math of Elliptic Curves	101	
The Double and Add Algorithm	102	
Why Can’t a Hacker Use $G_{xy}$ and $a_{xy}$ to Calculate the Private Key A?	103	
Writing TLS Sockets	104	
The Secure Client Socket	104	
The Secure Server Socket	106	

SSL Stripping and HSTS Bypass .....	107
Exercise: Add Encryption to your Ransomware Server .....	107

## **PART III SOCIAL ENGINEERING**

### **7 PHISHING AND DEEPPAKES 113**

A Sophisticated and Sneaky Social Engineering Attack .....	114
Faking Emails .....	114
Performing a DNS Lookup of a Mail Server .....	115
Communicating with SMTP .....	115
Writing an Email Spoofer .....	117
Spoofing SMTPS Emails .....	119
Faking Websites .....	121
Creating Deepfake Videos .....	123
Accessing Google Colab .....	124
Importing the Machine Learning Models .....	125
Exercises .....	127
Voice Cloning .....	127
Phishing at Scale .....	128
SMTP Auditing .....	129

### **8 SCANNING TARGETS 131**

Link Analysis .....	132
Maltego .....	133
Leaked Credential Databases .....	136
SIM Jacking .....	137
Google Dorking .....	138
Scanning the Entire Internet .....	139
Masscan .....	139
Shodan .....	143
IPv6 and NAT Limitations .....	144
Internet Protocol Version 6 (IPv6) .....	144
NAT .....	145
Vulnerability Databases .....	146
Vulnerability Scanners .....	148
Exercises .....	151
nmap Scans .....	152
Discover .....	152
Writing Your Own OSINT Tool .....	154

## **PART IV EXPLOITATION**

### **9**

#### **FUZZING FOR ZERO-DAY VULNERABILITIES 159**

Case Study: Exploiting the Heartbleed OpenSSL Vulnerability .....	160
Creating an Exploit .....	160
Starting the Program .....	161
Writing the Client Hello Message .....	162
Reading the Server Response .....	164
Crafting the Malicious Heartbeat Request .....	165
Reading the Leaked Memory Contents .....	166
Writing the Exploit Function .....	167
Putting It Together .....	167
Fuzzing .....	168
A Simplified Example .....	168
Writing Your Own Fuzzer .....	169
American Fuzzy Lop .....	170
Symbolic Execution .....	174
A Symbolic Execution of the Test Program .....	175
Limitations of Symbolic Execution .....	175
Dynamic Symbolic Execution .....	176
Using DSE to Crack a Passcode .....	179
Creating an Executable Binary .....	179
Installing and Running Angr .....	180
The Angr Program .....	181
Exercises .....	182
Capture the Flag Games with Angr .....	182
Fuzzing Web Protocols .....	183
Fuzzing an Open Source Project .....	184
Implement Your Own Concolic Execution Engine .....	185

### **10**

#### **BUILDING TROJANS 187**

Case Study: Re-Creating Drovorub by Using Metasploit .....	188
Building the Attacker's Server .....	188
Building the Victim Client .....	190
Uploading the Implant .....	190
Using the Attacker Agent .....	191
Why We Need a Victim Kernel Module .....	192
Hiding an Implant in a Legitimate File .....	193
Creating a Trojan .....	193
Hosting the Trojan .....	197
Downloading the Infected File .....	197
Controlling the Implant .....	198

Evading Antivirus by Using Encoders .....	200
The Base64 Encoder .....	201
Writing a Metasploit Module .....	202
Shikata Ga Nai Encoder .....	204
Creating a Windows Trojan .....	206
Hiding the Trojan in Minesweeper .....	206
Hiding the Trojan in a Word Document (or Another Innocent File) .....	207
Creating an Android Trojan .....	208
Deconstructing the APK to View the Implant .....	208
Rebuilding and Signing the APK .....	211
Testing the Android Trojan .....	212
Exercises .....	215
Evil-Droid .....	216
Writing Your Own Python Implant .....	217
Obfuscate Your Implant .....	218
Build a Platform-Specific Executable .....	219

## 11

### **BUILDING AND INSTALLING LINUX ROOTKITS 221**

Writing a Linux Kernel Module .....	222
Backing Up Your Kali Linux Virtual Machine .....	222
Writing the Code .....	223
Compiling and Running Your Kernel Module .....	224
Modifying System Calls .....	226
How System Calls Work .....	226
Hooking Syscalls .....	229
Hooking the Shutdown Syscall .....	230
Hiding Files .....	234
The linux_dirent struct .....	234
Writing the Hooking Code .....	235
Using Armitage to Exploit a Host and Install a Rootkit .....	237
Scanning the Network .....	238
Exploiting a Host .....	239
Installing a Rootkit .....	240
Exercises .....	240
The Keylogger .....	240
Self-Hiding Module .....	243

## 12

### **STEALING AND CRACKING PASSWORDS 245**

SQL Injection .....	246
Stealing Passwords from a Website's Database .....	247
Enumerating Reachable Files on the Web Server .....	248
Performing SQL Injection .....	248

Writing Your Own SQL Injection Tool .....	250
Understanding HTTP Requests .....	250
Writing the Injection Program .....	252
Using SQLMap .....	254
Hashing Passwords .....	256
The Anatomy of the MD5 Hash .....	257
Cracking Hashes .....	259
Salting Hashes with a Nonce .....	260
Building a Salted Hash Cracker .....	260
Popular Hash Cracking and Brute-Forcing Tools .....	261
John the Ripper .....	261
Hashcat .....	262
Hydra .....	263
Exercises .....	264
NoSQL Injection .....	264
Brute-Forcing Web Logins .....	265
Burp Suite .....	266

## 13

### **SERIOUS CROSS-SITE SCRIPTING EXPLOITATION 269**

Cross-Site Scripting .....	270
How JavaScript Can Be Malicious .....	271
Stored XSS Attacks .....	273
Reflected XSS Attacks .....	275
Finding Vulnerabilities with OWASP Zed Attack Proxy .....	276
Using Browser Exploitation Framework Payloads .....	278
Injecting the BeEF Hook .....	278
Performing a Social Engineering Attack .....	279
Moving from Browser to Machine .....	281
Case Study: Exploiting an Old Version of the Chrome Browser .....	281
Installing Rootkits via Website Exploitation .....	282
Exercise: Hunting for Bugs in a Bug Bounty Program .....	285

## **PART V CONTROLLING THE NETWORK**

### 14

### **PIVOTING AND PRIVILEGE ESCALATION 289**

Pivoting from a Dual-Homed Device .....	290
Configuring a Dual-Homed Device .....	290
Connecting a Machine to Your Private Network .....	293
Pivoting with Metasploit .....	294
Writing an Attacker Proxy .....	297

Extracting Password Hashes on Linux .....	298
Where Linux Stores Usernames and Passwords .....	299
Performing a Dirty COW Privilege Escalation Attack .....	300
Exercises .....	303
Adding NAT to Your Dual-Homed Device .....	303
Suggested Reading on Windows Privilege Escalation .....	304

## **15 MOVING THROUGH THE CORPORATE WINDOWS NETWORK 305**

Creating a Windows Virtual Lab .....	306
Extracting Password Hashes with Mimikatz .....	306
Passing the Hash with NT LAN Manager .....	309
Exploring the Corporate Windows Network .....	310
Attacking the DNS Service .....	311
Attacking Active Directory and LDAP Services .....	313
Writing an LDAP Query Client .....	314
Using SharpHound and Bloodhound for LDAP Enumeration .....	317
Attacking Kerberos .....	318
The Pass-the-Ticket Attack .....	320
The Golden Ticket and DC Sync Attacks .....	321
Exercise: Kerberoasting .....	322

## **16 NEXT STEPS 323**

Setting Up a Hardened Hacking Environment .....	324
Remaining Anonymous with Tor and Tails .....	324
Setting Up a Virtual Private Server .....	326
Setting Up SSH .....	326
Installing Your Hacking Tools .....	328
Hardening the Server .....	329
Auditing Your Hardened Server .....	331
Other Topics .....	332
Software-Defined Radios .....	332
Attacking Cellular Infrastructure .....	333
Escaping the Air Gap .....	333
Reverse Engineering .....	334
Physical Hacking Tools .....	334
Forensics .....	334
Hacking Industrial Systems .....	335
Quantum Computation .....	335
Connect with Others .....	335

## **INDEX 337**