

# CONTENTS IN DETAIL

<b>FOREWORD</b>	<b>XV</b>
<b>PREFACE</b>	<b>XVII</b>
<b>ACKNOWLEDGMENTS</b>	<b>XIX</b>
<b>1</b>	
<b>SETTING UP YOUR PYTHON ENVIRONMENT</b>	<b>1</b>
Installing Kali Linux . . . . .	2
Setting Up Python 3 . . . . .	3
Installing an IDE . . . . .	5
Code Hygiene . . . . .	5
<b>2</b>	
<b>BASIC NETWORKING TOOLS</b>	<b>9</b>
Python Networking in a Paragraph . . . . .	10
TCP Client . . . . .	10
UDP Client . . . . .	11
TCP Server . . . . .	12
Replacing Netcat . . . . .	13
Kicking the Tires . . . . .	17
Building a TCP Proxy . . . . .	19
Kicking the Tires . . . . .	24
SSH with Paramiko . . . . .	26
Kicking the Tires . . . . .	30
SSH Tunneling . . . . .	30
Kicking the Tires . . . . .	34
<b>3</b>	
<b>WRITING A SNIFFER</b>	<b>35</b>
Building a UDP Host Discovery Tool . . . . .	36
Packet Sniffing on Windows and Linux . . . . .	36
Kicking the Tires . . . . .	38
Decoding the IP Layer . . . . .	38
The ctypes Module . . . . .	39
The struct Module . . . . .	41
Writing the IP Decoder . . . . .	43
Kicking the Tires . . . . .	45
Decoding ICMP . . . . .	46
Kicking the Tires . . . . .	50

<b>4</b>		
<b>OWNING THE NETWORK WITH SCAPY</b>		<b>53</b>
Stealing Email Credentials. . . . .		54
Kicking the Tires . . . . .		57
ARP Cache Poisoning with Scapy. . . . .		57
Kicking the Tires . . . . .		62
pcap Processing. . . . .		63
Kicking the Tires . . . . .		69
<b>5</b>		
<b>WEB HACKERY</b>		<b>71</b>
Using Web Libraries. . . . .		72
The urllib2 Library for Python 2.x . . . . .		72
The urllib Library for Python 3.x . . . . .		73
The requests Library. . . . .		74
The lxml and BeautifulSoup Packages . . . . .		74
Mapping Open Source Web App Installations. . . . .		76
Mapping the WordPress Framework . . . . .		76
Testing the Live Target . . . . .		80
Kicking the Tires . . . . .		81
Brute-Forcing Directories and File Locations . . . . .		82
Kicking the Tires . . . . .		85
Brute-Forcing HTML Form Authentication . . . . .		85
Kicking the Tires . . . . .		90
<b>6</b>		
<b>EXTENDING BURP PROXY</b>		<b>93</b>
Setting Up. . . . .		94
Burp Fuzzing . . . . .		95
Kicking the Tires . . . . .		101
Using Bing for Burp . . . . .		104
Kicking the Tires . . . . .		108
Turning Website Content into Password Gold . . . . .		110
Kicking the Tires . . . . .		113
<b>7</b>		
<b>GITHUB COMMAND AND CONTROL</b>		<b>117</b>
Setting Up a GitHub Account. . . . .		118
Creating Modules . . . . .		119
Configuring the Trojan . . . . .		120
Building a GitHub-Aware Trojan . . . . .		121
Hacking Python's import Functionality . . . . .		123
Kicking the Tires . . . . .		124

<b>8</b>		
<b>COMMON TROJANING TASKS ON WINDOWS</b>		<b>127</b>
Keylogging for Fun and Keystrokes . . . . .		128
Kicking the Tires . . . . .		130
Taking Screenshots . . . . .		131
Pythonic Shellcode Execution . . . . .		132
Kicking the Tires . . . . .		134
Sandbox Detection . . . . .		135
<b>9</b>		
<b>FUN WITH EXFILTRATION</b>		<b>139</b>
Encrypting and Decrypting Files . . . . .		140
Email Exfiltration . . . . .		142
File Transfer Exfiltration . . . . .		144
Exfiltration via a Web Server . . . . .		145
Putting It All Together . . . . .		148
Kicking the Tires . . . . .		150
<b>10</b>		
<b>WINDOWS PRIVILEGE ESCALATION</b>		<b>153</b>
Installing the Prerequisites . . . . .		154
Creating the Vulnerable BlackHat Service . . . . .		154
Creating a Process Monitor . . . . .		156
Process Monitoring with WMI . . . . .		157
Kicking the Tires . . . . .		158
Windows Token Privileges . . . . .		159
Winning the Race . . . . .		161
Kicking the Tires . . . . .		164
Code Injection . . . . .		164
Kicking the Tires . . . . .		166
<b>11</b>		
<b>OFFENSIVE FORENSICS</b>		<b>169</b>
Installation . . . . .		170
General Reconnaissance . . . . .		171
User Reconnaissance . . . . .		173
Vulnerability Reconnaissance . . . . .		176
The volshell Interface . . . . .		177
Custom Volatility Plug-Ins . . . . .		177
Kicking the Tires . . . . .		182
Onward! . . . . .		184
<b>INDEX</b>		<b>185</b>