

CONTENTS IN DETAIL

FOREWORD by Charlie Miller	xv
PREFACE	xvii
ACKNOWLEDGMENTS	xix
1	
SETTING UP YOUR PYTHON ENVIRONMENT	1
Installing Kali Linux.	2
WingIDE.	3
2	
THE NETWORK: BASICS	9
Python Networking in a Paragraph	10
TCP Client.	10
UDP Client	11
TCP Server	12
Replacing Netcat	13
Kicking the Tires	19
Building a TCP Proxy	20
Kicking the Tires	25
SSH with Paramiko.	26
Kicking the Tires	29
SSH Tunneling.	30
Kicking the Tires	33
3	
THE NETWORK: RAW SOCKETS AND SNIFFING	35
Building a UDP Host Discovery Tool	36
Packet Sniffing on Windows and Linux	36
Kicking the Tires	38
Decoding the IP Layer	38
Kicking the Tires	41
Decoding ICMP	42
Kicking the Tires	45

4		
	OWNING THE NETWORK WITH SCAPY	47
	Stealing Email Credentials.	48
	Kicking the Tires	50
	ARP Cache Poisoning with Scapy.	51
	Kicking the Tires	54
	PCAP Processing	55
	Kicking the Tires	59
5		
	WEB HACKERY	61
	The Socket Library of the Web: urllib2	62
	Mapping Open Source Web App Installations.	63
	Kicking the Tires	64
	Brute-Forcing Directories and File Locations	65
	Kicking the Tires	68
	Brute-Forcing HTML Form Authentication	69
	Kicking the Tires	74
6		
	EXTENDING BURP PROXY	75
	Setting Up.	76
	Burp Fuzzing	78
	Kicking the Tires	83
	Bing for Burp	87
	Kicking the Tires	91
	Turning Website Content into Password Gold	93
	Kicking the Tires	97
7		
	GITHUB COMMAND AND CONTROL	101
	Setting Up a GitHub Account.	102
	Creating Modules	103
	Trojan Configuration	104
	Building a GitHub-Aware Trojan	105
	Hacking Python’s import Functionality	107
	Kicking the Tires	108
8		
	COMMON TROJANING TASKS ON WINDOWS	111
	Keylogging for Fun and Keystrokes.	112
	Kicking the Tires	114
	Taking Screenshots.	115
	Pythonic Shellcode Execution.	116
	Kicking the Tires	117
	Sandbox Detection.	118

9		
FUN WITH INTERNET EXPLORER		123
Man-in-the-Browser (Kind Of)		124
Creating the Server		127
Kicking the Tires		128
IE COM Automation for Exfiltration		128
Kicking the Tires		134
10		
WINDOWS PRIVILEGE ESCALATION		137
Installing the Prerequisites		138
Creating a Process Monitor		139
Process Monitoring with WMI		139
Kicking the Tires		141
Windows Token Privileges		141
Winning the Race		144
Kicking the Tires		146
Code Injection		147
Kicking the Tires		149
11		
AUTOMATING OFFENSIVE FORENSICS		151
Installation		152
Profiles		152
Grabbing Password Hashes		153
Direct Code Injection		156
Kicking the Tires		161
INDEX		163