Table of Contents

Preface vii

Chapter 1: Theory on Adversarial Operations and Principles of Computer Conflict 1

Adversarial theory 2

CIAAAN 3

Game theory 4

Principles of computer conflict 6

Offense versus defense 8

Principle of deception 15

Principle of physical access 17

Principle of humanity 19

Principle of economy 20

Principle of planning 21

Principle of innovation 24

Principle of time 25

Summary 27

References 28

Chapter 2: Preparing for Battle 31

Essential considerations 32

Communications 32

Long-term planning 34

Expertise 36

Operational planning 37

Defensive perspective 40

Signal collection 41

Data management 46
Analysis tooling 52
Defensive KPIs 55
Offensive perspective 55
Scanning and exploitation 56
Payload development 59
Auxiliary tooling 61
Offensive KPIs 62
Summary 63
References 64
Chapter 3: Invisible is Best (Operating in Memory) 71
Gaining the advantage 72
Offensive perspective 75
Process injection 75
In-memory operations 79
Defensive perspective 85
Detecting process injection 86
Preparing for attacker techniques 89
The invisible defense 91
Summary 92
References 93
Chapter 4: Blending In 97
Offensive perspective 99
Persistence options 99
LOLbins 100
DLL search order hijacking 101
Executable file infection 102
Covert command and control channels 103
ICMP C2 105
DNS C2 106
Domain fronting 107
Combining offensive techniques 108
Defensive perspective 110
C2 detection 111
ICMP C2 detection 111
DNS C2 detection 112
Persistence detection 116
Detecting DLL search order hijacking 117
Detecting backdoored executables 117
Honey tricks 118
Honey tokens 119

Honeypots 120
Summary 121
References 122
Chapter 5: Active Manipulation 125
Offensive perspective 126
Clearing logs 126
Hybrid approach 130
Rootkits 131
Defensive perspective 133
Data integrity and verification 133
Detecting rootkits 134
Manipulating attackers 136
Keeping attackers distracted 138
Tricking attackers 140
Summary 144
References 144
Chapter 6: Real-Time Conflict 147
Offensive perspective 148
Situational awareness 149
Understanding the system 150
Clear the Bash history 151
Abusing Docker 152
Gleaning operational information 152
Keylogging 152
Screenshot spy 154
Getting passwords 155
Searching files for secrets 156
Backdooring password utilities 157
Pivoting 160
SSH agent hijacking 160
SSH ControlMaster hijacking 161
RDP hijacking 162
Hijacking other administrative controls 162
Defensive perspective 163
Exploring users, processes, and connections 164
Root cause analysis 165
Killing malicious processes 165
Killing connections and banning IPs 165
Network quarantine 166
Rotating credentials 168
Restricting permissions 170
Chattr revisited 170

chroot 171
Using namespaces 171
Controlling users 172
Shut it down 173
Hacking back 173
Hunting attacker infrastructure 174
Exploiting attacker tools 174
Summary 175
References 175
Chapter 7: The Research Advantage 179
Gaming the game 180
Offensive perspective 181
The world of memory corruption 181
Targeting research and prep 183
Target exploitation 184
Creative pivoting 185
Defensive perspective 188
Tool exploitation 189
Threat modeling 189
Operating system and application research 191
Log and analyze your own data 192
Attribution 193
Summary 194
References 194
Chapter 8: Clearing the Field 197
Offensive perspective 198
Exfiltration 199
Protocol tunneling 199
Steganography 200
Anonymity networks 201
Ending the operation 206
Program security versus operational security 206
Taking down infrastructure 206
Rotating offensive tools 207
Retiring and replacing techniques 207
Defensive perspective 208
Responding to an intrusion 208
The big flip 210
The remediation effort 212
A post-mortem after the incident 213
Forward looking 213
Publish results 214

Summary 214
References 215
Other Books You May Enjoy 219
Index 225