## Contents

<table>
<thead>
<tr>
<th>Chapter 1</th>
<th>Medical Records (In)security</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 2</td>
<td>Stealing Research</td>
<td>29</td>
</tr>
</tbody>
</table>

### Chapter 1 Medical Records (In)security
- An Introduction to Simulating Advanced Persistent Threat
- Background and Mission Briefing
- Payload Delivery Part 1: Learning How to Use the VBA Macro
  - How NOT to Stage a VBA Attack
  - Examining the VBA Code
  - Avoid Using Shellcode
  - Automatic Code Execution
  - Using a VBA/VBS Dual Stager
  - Keep Code Generic Whenever Possible
  - Code Obfuscation
  - Enticing Users
- Command and Control Part 1: Basics and Essentials
- The Attack
  - Bypassing Authentication
- Summary
- Exercises

### Chapter 2 Stealing Research
- Background and Mission Briefing
- Payload Delivery Part 2: Using the Java Applet for Payload Delivery
  - Java Code Signing for Fun and Profit
  - Writing a Java Applet Stager
  - Create a Convincing Pretext
  - Signing the Stager
### Contents

Notes on Payload Persistence 41  
  Microsoft Windows 41  
  Linux 42  
  OSX 45  
Command and Control Part 2: Advanced Attack Management 45  
  Adding Stealth and Multiple System Management 45  
  Implementing a Command Structure 47  
  Building a Management Interface 48  
The Attack 49  
  Situational Awareness 50  
  Using AD to Gather Intelligence 50  
  Analyzing AD Output 51  
  Attack Against Vulnerable Secondary System 52  
  Credential Reuse Against Primary Target System 53  
Summary 54  
Exercises 55

**Chapter 3**  
**Twenty-First Century Heist**  
57  
What Might Work? 57  
Nothing Is Secure 58  
Organizational Politics 58  
APT Modeling versus Traditional Penetration Testing 59  
Background and Mission Briefing 59  
Command and Control Part III: Advanced  
  Channels and Data Exfiltration 60  
  Notes on Intrusion Detection and the Security Operations Center 64  
  The SOC Team 65  
  How the SOC Works 65  
  SOC Reaction Time and Disruption 66  
  IDS Evasion 67  
  False Positives 67  
Payload Delivery Part III: Physical Media 68  
  A Whole New Kind of Social Engineering 68  
  Target Location Profiling 69  
  Gathering Targets 69  
The Attack 72  
Summary 75  
Exercises 75

**Chapter 4**  
**Pharma Karma**  
77  
Background and Mission Briefing 78  
Payload Delivery Part IV: Client-Side Exploits 1 79  
  The Curse That Is Flash 79  
  At Least You Can Live Without It 81  
Memory Corruption Bugs: Dos and Don’ts 81  
Reeling in the Target 83
### Command and Control Part IV: Metasploit Integration

- Metasploit Integration Basics 86
- Server Configuration 86
- Black Hats/White Hats 87
- What Have I Said About AV? 88
- Pivoting 89

### The Attack

- The Hard Disk Firewall Fail 90
- Metasploit Demonstration 90
- Under the Hood 91
- The Benefits of Admin 92
- Typical Subnet Cloning 96
- Recovering Passwords 96
- Making a Shopping List 99

#### Summary 101

#### Exercises 101

---

### Chapter 5 Guns and Ammo

**Background and Mission Briefing** 104

**Payload Delivery Part V: Simulating a Ransomware Attack** 106

- What Is Ransomware? 106
- Why Simulate a Ransomware Attack? 107
- A Model for Ransomware Simulation 107
- Asymmetric Cryptography 108
- Remote Key Generation 109
- Targeting Files 110
- Requesting the Ransom 111
- Maintaining C2 111
- Final Thoughts 112

**Command and Control Part V: Creating a Covert C2 Solution** 112

- Introducing the Onion Router 112
- The Torrc File 113
- Configuring a C2 Agent to Use the Tor Network 115
- Bridges 115

**New Strategies in Stealth and Deployment** 116

- VBA Redux: Alternative Command-Line Attack Vectors 116
- PowerShell 117
- FTP 117
- Windows Scripting Host (WSH) 118
- BITSadmin 118
- Simple Payload Obfuscation 119
- Alternative Strategies in Antivirus Evasion 121

**The Attack** 125

- Gun Design Engineer Answers Your Questions 126
Identifying the Players 127
Smart(er) VBA Document Deployment 128
Email and Saved Passwords 131
Keyloggers and Cookies 132
Bringing It All Together 133
Summary 134
Exercises 135

Chapter 6  Criminal Intelligence 137

Payload Delivery Part VI: Deploying with HTA 138
  Malware Detection 140
Privilege Escalation in Microsoft Windows 141
  Escalating Privileges with Local Exploits 143
  Exploiting Automated OS Installations 147
  Exploiting the Task Scheduler 147
  Exploiting Vulnerable Services 149
  Hijacking DLLs 151
  Mining the Windows Registry 154
Command and Control Part VI: The Creeper Box 155
  Creeper Box Specification 155
  Introducing the Raspberry Pi and Its Components 156
  GPIO 157
  Choosing an OS 157
  Configuring Full-Disk Encryption 158
  A Word on Stealth 163
Configuring Out-of-Band Command and Control 164
  Using 3G/4G 164
  Creating a Transparent Bridge 168
  Using a Pi as a Wireless AP to Provision Access by Remote Keyloggers 169
The Attack 171
  Spoofing Caller ID and SMS Messages 172
Summary 174
Exercises 174

Chapter 7  War Games 175

Background and Mission Briefing 176
Payload Delivery Part VII: USB Shotgun Attack 178
  USB Media 178
  A Little Social Engineering 179
Command and Control Part VII: Advanced Autonomous Data Exfiltration 180
  What We Mean When We Talk About “Autonomy” 180
  Means of Egress 181
The Attack 185
  Constructing a Payload to Attack a Classified Network 187
  Stealthy 3G/4G Software Install 188
### Contents

- Attacking the Target and Deploying the Payload 189
- Efficient “Burst-Rate” Data Exfiltration 190
- Summary 191
- Exercises 191

#### Chapter 8  Hack Journalists 193

- Briefing 193
- Advanced Concepts in Social Engineering 194
  - Cold Reading 194
- C2 Part VIII: Experimental Concepts in Command and Control 199
  - Scenario 1: C2 Server Guided Agent Management 199
  - Scenario 2: Semi-Autonomous C2 Agent Management 202
- Payload Delivery Part VIII: Miscellaneous Rich Web Content 205
  - Java Web Start 205
  - Adobe AIR 206
  - A Word on HTML5 207
- The Attack 207
- Summary 211
- Exercises 211

#### Chapter 9  Northern Exposure 213

- Overview 214
- Operating Systems 214
  - Red Star Desktop 3.0 215
  - Red Star Server 3.0 219
- North Korean Public IP Space 221
- The North Korean Telephone System 224
- Approved Mobile Devices 228
- The “Walled Garden”: The Kwangmyong Intranet 230
- Audio and Video Eavesdropping 231
- Summary 233
- Exercises 234

### Index 235