Table of Contents

Preface 1

Section 1: Obtaining the Evidence

Chapter 1: Introducing Network Forensics 7
- Technical requirements 8
- Network forensics investigation methodology 9
- Source of network evidence 11
  - Tapping the wire and the air 11
  - CAM table on a network switch 13
  - Routing tables on routers 13
  - Dynamic Host Configuration Protocol logs 14
  - DNS servers logs 15
  - Domain controller/authentication servers/ system logs 15
  - IDS/IPS logs 16
  - Firewall logs 16
  - Proxy server logs 16
- Wireshark essentials 17
  - Identifying conversations and endpoints 19
  - Identifying the IP endpoints 21
  - Basic filters 23
- Exercise 1 – a noob's keylogger 29
- Exercise 2 – two too many 40
- Summary 42
- Questions and exercises 42
- Further reading 42

Chapter 2: Technical Concepts and Acquiring Evidence 43
- Technical requirements 43
- The inter-networking refresher 44
- Log-based evidence 46
  - Application server logs 47
  - Database logs 52
  - Firewall logs 54
  - Proxy logs 58
  - IDS logs 68
- Case study – hack attempts 74
- Summary 77
- Questions and exercises 78
- Further reading 78

Section 2: The Key Concepts

Chapter 3: Deep Packet Inspection 81
Technical requirements 82
Protocol encapsulation 82
The Internet Protocol header 83
The Transmission Control Protocol header 85
The HTTP packet 86
Analyzing packets on TCP 88
Analyzing packets on UDP 94
Analyzing packets on ICMP 103
Case study – ICMP Flood or something else 106
Summary 117
Questions and exercises 117
Further reading 117

Chapter 4: Statistical Flow Analysis 119
Technical requirements 119
The flow record and flow-record processing systems (FRPS) 120
Understanding flow-record processing systems 120
Exploring Netflow 120
Uniflow and bitflow 121
Sensor deployment types 122
Analyzing the flow 124
Converting PCAP to the IPFIX format 125
Viewing the IPFIX data 125
Flow analysis using SiLK 126
Viewing flow records as text 128
Summary 140
Questions 141
Further reading 141

Chapter 5: Combatting Tunneling and Encryption 143
Technical requirements 144
Decrypting TLS using browsers 144
Decoding a malicious DNS tunnel 150
Using Scapy to extract packet data 152
Decrypting 802.11 packets 155
Decrypting using Aircrack-ng 157
Decoding keyboard captures 162
Summary 166
Questions and exercises 166
Further reading 166

Section 3: Conducting Network Forensics

Chapter 6: Investigating Good, Known, and Ugly Malware 169
Technical requirements 170
Dissecting malware on the network 170
Finding network patterns 175
Intercepting malware for fun and profit 181
PyLocky ransomware decryption using PCAP data 182
Decrypting hidden tear ransomware 183
Behavior patterns and analysis 187
A real-world case study – investigating a banking Trojan on the network 198
Summary 212
Questions and exercises 212
Further reading 213

Chapter 7: Investigating C2 Servers 215
Technical requirements 215
Decoding the Metasploit shell 216
Working with PowerShell obfuscation 219
Decoding and decompressing with Python 220
Case study – decrypting the Metasploit Reverse HTTPS Shellcode 228
Analyzing Empire C2 233
Case study – CERT.SE's major fraud and hacking criminal case, B 8322-16 236
Summary 242
Questions and exercises 242
Further reading 243

Chapter 8: Investigating and Analyzing Logs 245
Technical requirements 246
Network intrusions and footprints 246
Investigating SSH logs 248
Investigating web proxy logs 253
Investigating firewall logs 256
A case study – defaced servers 260
Summary 270
Questions and exercises 270
Further reading 270

Chapter 9: WLAN Forensics 271
Technical requirements 272
The 802.11 standard 272
Wireless evidence types 273
Using airodump-ng to tap the air 275

Packet types and subtypes 279
Locating wireless devices 282
Identifying rogue access points 287
Obvious changes in the MAC address 287
The tagged perimeters 288
The time delta analysis 289
Identifying attacks 293
Rogue AP attacks 293
Peer-to-peer attacks 293
Eavesdropping 294
Cracking encryption 294
Authentication attacks 294
Denial of service 295
Investigating deauthentication packets 295
Case study – identifying the attacker 298
Summary 304
Questions 304
Further reading 305
Chapter 10: Automated Evidence Aggregation and Analysis 307
Technical requirements 307
Automation using Python and Scapy 308
Automation through pyshark – Python's tshark 316
Merging and splitting PCAP data 319
Splitting PCAP data on parameters 326
Splitting PCAP data in streams 327
Large-scale data capturing, collection, and indexing 329
Summary 334
Questions and exercises 334
Further reading 334
Other Books You May Enjoy 337
Assessments 341
Index 343