Contents

Introduction xiii

Chapter 1 Introducing Wireshark 1
What Is Wireshark? 2
A Best Time to Use Wireshark? 2
Avoiding Being Overwhelmed 3
The Wireshark User Interface 3
Packet List Pane 5
Packet Details Pane 6
Packet Bytes Pane 8
Filters 9
Capture Filters 9
Display Filters 13
Summary 17
Exercises 18

Chapter 2 Setting Up the Lab 19
Kali Linux 20
Virtualization 22
Basic Terminology and Concepts 23
Benefits of Virtualization 23
VirtualBox 24
Installing VirtualBox 24
Installing the VirtualBox Extension Pack 31
Creating a Kali Linux Virtual Machine 33
Installing Kali Linux 40
The W4SP Lab 46
Requirements 46
A Few Words about Docker 47
What Is GitHub? 48
## Contents

<table>
<thead>
<tr>
<th>Chapter</th>
<th>The Fundamentals</th>
<th>Capturing Packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Networking</strong></td>
<td><strong>Sniffing</strong></td>
</tr>
<tr>
<td></td>
<td><strong>OSI Layers</strong></td>
<td><strong>Promiscuous Mode</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Networking between Virtual Machines</strong></td>
<td><strong>Starting the First Capture</strong></td>
</tr>
<tr>
<td>Security</td>
<td><strong>The Security Triad</strong></td>
<td><strong>TShark</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Intrusion Detection and Prevention Systems</strong></td>
<td><strong>Dealing with the Network</strong></td>
</tr>
<tr>
<td></td>
<td><strong>False Positives and False Negatives</strong></td>
<td><strong>Local Machine</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Malware</strong></td>
<td><strong>Sniffing Localhost</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Spoofing and Poisoning</strong></td>
<td><strong>Sniffing on Virtual Machine Interfaces</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Packet and Protocol Analysis</strong></td>
<td><strong>Sniffing with Hubs</strong></td>
</tr>
<tr>
<td></td>
<td><strong>A Protocol Analysis Story</strong></td>
<td><strong>SPAN Ports</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Ports and Protocols</strong></td>
<td><strong>Network Taps</strong></td>
</tr>
<tr>
<td>Summary</td>
<td></td>
<td><strong>Transparent Linux Bridges</strong></td>
</tr>
<tr>
<td>Exercises</td>
<td></td>
<td><strong>Wireless Networks</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Loading and Saving Capture Files</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>File Formats</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Ring Buffers and Multiple Files</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Recent Capture Files</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Dissectors</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>W4SP Lab: Managing Nonstandard HTTP Traffic</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Filtering SMB Filenames</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Packet Colorization</strong></td>
</tr>
</tbody>
</table>

Creating the Lab User 49
Installing the W4SP Lab on the Kali Virtual Machine 50
Setting Up the W4SP Lab 53
The Lab Network 54
Summary 55
Exercises 56

Chapter 3 The Fundamentals 57
Networking 58
OSI Layers 58
Networking between Virtual Machines 61
Security 63
The Security Triad 63
Intrusion Detection and Prevention Systems 63
False Positives and False Negatives 64
Malware 64
Spoofing and Poisoning 66
Packet and Protocol Analysis 66
A Protocol Analysis Story 67
Ports and Protocols 71
Summary 73
Exercises 74

Chapter 4 Capturing Packets 75
Sniffing 76
Promiscuous Mode 76
Starting the First Capture 78
TShark 82
Dealing with the Network 86
Local Machine 87
Sniffing Localhost 88
Sniffing on Virtual Machine Interfaces 92
Sniffing with Hubs 96
SPAN Ports 98
Network Taps 101
Transparent Linux Bridges 103
Wireless Networks 105
Loading and Saving Capture Files 108
File Formats 108
Ring Buffers and Multiple Files 111
Recent Capture Files 116
Dissectors 118
W4SP Lab: Managing Nonstandard HTTP Traffic 118
Filtering SMB Filenames 120
Packet Colorization 123
Chapter 5 \textbf{Diagnosing Attacks} \hfill 129

- Attack Type: Man-in-the-Middle
  - Why MitM Attacks Are Effective
  - How MitM Attacks Get Done: ARP
  - W4SP Lab: Performing an ARP MitM Attack
  - W4SP Lab: Performing a DNS MitM Attack
  - How to Prevent MitM Attacks
- Attack Type: Denial of Service
  - Why DoS Attacks Are Effective
  - How DoS Attacks Get Done
  - How to Prevent DoS Attacks
- Attack Type: Advanced Persistent Threat
  - Why APT Attacks Are Effective
  - How APT Attacks Get Done
  - Example APT Traffic in Wireshark
  - How to Prevent APT Attacks

Chapter 6 \textbf{Offensive Wireshark} \hfill 163

- Attack Methodology
- Reconnaissance Using Wireshark
- Evading IPS/IDS
  - Session Splicing and Fragmentation
  - Playing to the Host, Not the IDS
  - Covering Tracks and Placing Backdoors
- Exploitation
  - Setting Up the W4SP Lab with Metasploitable
  - Launching Metasploit Console
  - VSFTP Exploit
  - Debugging with Wireshark
  - Shell in Wireshark
  - TCP Stream Showing a Bind Shell
  - TCP Stream Showing a Reverse Shell
  - Starting ELK
- Remote Capture over SSH

Chapter 7 \textbf{Decrypting TLS, Capturing USB, Keyloggers, and Network Graphing} \hfill 193

- Decrypting SSL/TLS
  - Decrypting SSL/TLS Using Private Keys
Decryption of SSL/TLS Using Session Keys 199
USB and Wireshark 202
    Capturing USB Traffic on Linux 203
    Capturing USB Traffic on Windows 206
    TShark Keylogger 208
Graphing the Network 212
    Lua with Graphviz Library 213
Summary 218
Exercises 219

Chapter 8 Scripting with Lua 221
Why Lua? 222
Scripting Basics 223
    Variables 225
    Functions and Blocks 226
    Loops 228
    Conditionals 230
Setup 230
    Checking for Lua Support 231
    Lua Initialization 232
    Windows Setup 233
    Linux Setup 233
Tools 234
    Hello World with TShark 236
    Counting Packets Script 237
    ARP Cache Script 241
Creating Dissectors for Wireshark 244
    Dissector Types 245
    Why a Dissector Is Needed 245
    Experiment 253
Extending Wireshark 255
    Packet Direction Script 255
    Marking Suspicious Script 257
    Snooping SMB File Transfers 260
Summary 262

Index 265