

CONTENTS IN DETAIL

ACKNOWLEDGMENTS

xv

INTRODUCTION

xvii

Why This Book?	xviii
Concepts and Approach	xviii
How to Use This Book	xx
About the Sample Capture Files	xx
The Rural Technology Fund	xxi
Contacting Me	xxi

1

PACKET ANALYSIS AND NETWORK BASICS

1

Packet Analysis and Packet Sniffers	2
Evaluating a Packet Sniffer	2
How Packet Sniffers Work	3
How Computers Communicate	4
Protocols	4
The Seven-Layer OSI Model	5
Network Hardware	10
Traffic Classifications	15
Broadcast Traffic	15
Multicast Traffic	16
Unicast Traffic	16
Final Thoughts	16

2

TAPPING INTO THE WIRE

17

Living Promiscuously	18
Sniffing Around Hubs	19
Sniffing in a Switched Environment	20
Port Mirroring	21
Hubbing Out	23
Using a Tap	24
ARP Cache Poisoning	27
Sniffing in a Routed Environment	31
Sniffer Placement in Practice	33

3

INTRODUCTION TO WIRESHARK

37

A Brief History of Wireshark	37
The Benefits of Wireshark	38

Installing Wireshark	39
Installing on Windows Systems	39
Installing on Linux Systems	41
Installing on OS X Systems	43
Wireshark Fundamentals	44
Your First Packet Capture	44
Wireshark's Main Window	45
Wireshark Preferences	46
Packet Color Coding	48
Configuration Files	50
Configuration Profiles	50

4

WORKING WITH CAPTURED PACKETS 53

Working with Capture Files	53
Saving and Exporting Capture Files	54
Merging Capture Files	55
Working with Packets	56
Finding Packets	56
Marking Packets	57
Printing Packets	58
Setting Time Display Formats and References	58
Time Display Formats	59
Packet Time Referencing	60
Time Shifting	60
Setting Capture Options	61
Input Tab	61
Output Tab	62
Options Tab	63
Using Filters	65
Capture Filters	65
Display Filters	71
Saving Filters	74
Adding Display Filters to a Toolbar	75

5

ADVANCED WIRESHARK FEATURES 77

Endpoints and Network Conversations	78
Viewing Endpoint Statistics	78
Viewing Network Conversations	79
Identifying Top Talkers with Endpoints and Conversations	80
Protocol Hierarchy Statistics	83
Name Resolution	84
Enabling Name Resolution	84
Potential Drawbacks to Name Resolution	86
Using a Custom hosts File	86
Manually Initiated Name Resolution	88
Protocol Dissection	88
Changing the Dissector	88
Viewing Dissector Source Code	90

Following Streams	91
Following SSL Streams	92
Packet Lengths	93
Graphing	95
Viewing IO Graphs	95
Round-Trip Time Graphing	98
Flow Graphing	99
Expert Information	99

6

PACKET ANALYSIS ON THE COMMAND LINE 103

Installing TShark.	104
Installing tcpdump	105
Capturing and Saving Packets	106
Manipulating Output	109
Name Resolution	111
Applying Filters	113
Time Display Formats in TShark	114
Summary Statistics in TShark	115
Comparing TShark and tcpdump	118

7

NETWORK LAYER PROTOCOLS 119

Address Resolution Protocol (ARP)	120
ARP Packet Structure	121
Packet 1: ARP Request	122
Packet 2: ARP Response	123
Gratuitous ARP	124
Internet Protocol (IP)	125
Internet Protocol Version 4 (IPv4)	125
Internet Protocol Version 6 (IPv6)	133
Internet Control Message Protocol (ICMP)	144
ICMP Packet Structure	144
ICMP Types and Messages	144
Echo Requests and Responses	145
traceroute	147
ICMP Version 6 (ICMPv6)	150

8

TRANSPORT LAYER PROTOCOLS 151

Transmission Control Protocol (TCP)	151
TCP Packet Structure	152
TCP Ports	152
The TCP Three-Way Handshake	155
TCP Teardown	158
TCP Resets	159
User Datagram Protocol (UDP)	160
UDP Packet Structure	161

9

COMMON UPPER-LAYER PROTOCOLS

163

Dynamic Host Configuration Protocol (DHCP)	163
DHCP Packet Structure	164
The DHCP Initialization Process	165
DHCP In-Lease Renewal	170
DHCP Options and Message Types	170
DHCP Version 6 (DHCPv6)	171
Domain Name System (DNS)	173
DNS Packet Structure	173
A Simple DNS Query	174
DNS Question Types	176
DNS Recursion	177
DNS Zone Transfers	181
Hypertext Transfer Protocol (HTTP)	183
Browsing with HTTP	183
Posting Data with HTTP	186
Simple Mail Transfer Protocol (SMTP)	187
Sending and Receiving Email	188
Tracking an Email Message	189
Sending Attachments via SMTP	196
Final Thoughts	198

10

BASIC REAL-WORLD SCENARIOS

199

Missing Web Content	200
Tapping into the Wire	200
Analysis	201
Lessons Learned	204
Unresponsive Weather Service	205
Tapping into the Wire	206
Analysis	206
Lessons Learned	209
No Internet Access	210
Gateway Configuration Problems	210
Unwanted Redirection	213
Upstream Problems	216
Inconsistent Printer	219
Tapping into the Wire	219
Analysis	219
Lessons Learned	222
No Branch Office Connectivity	222
Tapping into the Wire	223
Analysis	223
Lessons Learned	226
Software Data Corruption	226
Tapping into the Wire	226
Analysis	227
Lessons Learned	230
Final Thoughts	230

11		
FIGHTING A SLOW NETWORK		231
TCP Error-Recovery Features	232	
TCP Retransmissions	232	
TCP Duplicate Acknowledgments and Fast Retransmissions	235	
TCP Flow Control	240	
Adjusting the Window Size	241	
Halting Data Flow with a Zero Window Notification	242	
The TCP Sliding Window in Practice	243	
Learning from TCP Error-Control and Flow-Control Packets	247	
Locating the Source of High Latency	248	
Normal Communications	248	
Slow Communications: Wire Latency	248	
Slow Communications: Client Latency	249	
Slow Communications: Server Latency	250	
Latency Locating Framework	251	
Network Baselineing	251	
Site Baseline	252	
Host Baseline	253	
Application Baseline	254	
Additional Notes on Baselines	255	
Final Thoughts	255	

12		
PACKET ANALYSIS FOR SECURITY		257
Reconnaissance	258	
SYN Scan	258	
Operating System Fingerprinting	263	
Traffic Manipulation	266	
ARP Cache Poisoning	267	
Session Hijacking	271	
Malware	275	
Operation Aurora	275	
Remote-Access Trojan	281	
Exploit Kit and Ransomware	288	
Final Thoughts	294	

13		
WIRELESS PACKET ANALYSIS		295
Physical Considerations	296	
Sniffing One Channel at a Time	296	
Wireless Signal Interference	297	
Detecting and Analyzing Signal Interference	297	
Wireless Card Modes	298	
Sniffing Wirelessly in Windows	300	
Configuring AirPcap	300	
Capturing Traffic with AirPcap	302	
Sniffing Wirelessly in Linux	303	
802.11 Packet Structure	304	

Adding Wireless-Specific Columns to the Packet List Pane	305
Wireless-Specific Filters.	307
Filtering Traffic for a Specific BSS ID	307
Filtering Specific Wireless Packet Types	307
Filtering a Specific Frequency	308
Saving a Wireless Profile	309
Wireless Security	309
Successful WEP Authentication	309
Failed WEP Authentication	311
Successful WPA Authentication	312
Failed WPA Authentication	314
Final Thoughts	315

A

FURTHER READING 317

Packet Analysis Tools	317
CloudShark	317
WireEdit	318
Cain & Abel	319
Scapy	319
TraceWrangler	319
Tcpreplay	319
NetworkMiner	319
CapTipper	320
ngrep	321
libpcap	321
Npcap	321
hping	321
Python	321
Packet Analysis Resources	321
Wireshark's Home Page	322
Practical Packet Analysis Online Course	322
SANS's Security Intrusion Detection In-Depth Course	322
Chris Sanders's Blog	322
Brad Duncan's Malware Traffic Analysis	322
IANA's Website	323
W. Richard Stevens's TCP/IP Illustrated Series	323
The TCP/IP Guide	323

B

NAVIGATING PACKETS 325

Packet Representation	326
Using Packet Diagrams	328
Navigating a Mystery Packet	330
Final Thoughts	332

INDEX 333