

# CONTENTS IN DETAIL

<b>ABOUT THE AUTHOR</b>	<b>xvii</b>
-------------------------	-------------

<b>FOREWORD by Todd Heberlein</b>	<b>xix</b>
-----------------------------------	------------

<b>PREFACE</b>	<b>xxv</b>
----------------	------------

Audience . . . . .	.xxvi
Prerequisites . . . . .	.xxvii
A Note on Software and Protocols . . . . .	.xxvii
Scope . . . . .	.xxviii
Acknowledgments . . . . .	.xxix

## **PART I GETTING STARTED**

<b>1 NETWORK SECURITY MONITORING RATIONALE</b>	<b>3</b>
--	----------

An Introduction to NSM . . . . .	4
Does NSM Prevent Intrusions? . . . . .	5
What Is the Difference Between NSM and Continuous Monitoring? . . . . .	8
How Does NSM Compare with Other Approaches? . . . . .	9
Why Does NSM Work? . . . . .	10
How NSM Is Set Up . . . . .	11
When NSM Won't Work . . . . .	12
Is NSM Legal? . . . . .	13
How Can You Protect User Privacy During NSM Operations? . . . . .	14
A Sample NSM Test . . . . .	15
The Range of NSM Data . . . . .	16
Full Content Data . . . . .	16
Extracted Content Data . . . . .	19
Session Data . . . . .	21
Transaction Data . . . . .	22
Statistical Data . . . . .	24
Metadata . . . . .	26
Alert Data . . . . .	28
What's the Point of All This Data? . . . . .	30
NSM Drawbacks . . . . .	31
Where Can I Buy NSM? . . . . .	31
Where Can I Go for Support or More Information? . . . . .	32
Conclusion . . . . .	32

<b>2</b>	<b>COLLECTING NETWORK TRAFFIC: ACCESS, STORAGE, AND MANAGEMENT</b>	<b>33</b>
A Sample Network for a Pilot NSM System . . . . .		33
Traffic Flow in a Simple Network . . . . .		35
Possible Locations for NSM . . . . .		38
IP Addresses and Network Address Translation . . . . .		39
Net Blocks . . . . .		39
IP Address Assignments . . . . .		41
Address Translation . . . . .		42
Choosing the Best Place to Obtain Network Visibility . . . . .		45
Location for DMZ Network Traffic . . . . .		45
Locations for Viewing the Wireless and Internal Network Traffic . . . . .		45
Getting Physical Access to the Traffic . . . . .		47
Using Switches for Traffic Monitoring . . . . .		47
Using a Network Tap . . . . .		48
Capturing Traffic Directly on a Client or Server . . . . .		49
Choosing an NSM Platform . . . . .		49
Ten NSM Platform Management Recommendations . . . . .		51
Conclusion . . . . .		52

## **PART II SECURITY ONION DEPLOYMENT**

<b>3</b>	<b>STAND-ALONE NSM DEPLOYMENT AND INSTALLATION</b>	<b>55</b>
Stand-alone or Server Plus Sensors? . . . . .		56
Choosing How to Get SO Code onto Hardware . . . . .		59
Installing a Stand-alone System . . . . .		59
Installing SO to a Hard Drive . . . . .		60
Configuring SO Software . . . . .		64
Choosing the Management Interface . . . . .		66
Installing the NSM Software Components . . . . .		68
Checking Your Installation . . . . .		70
Conclusion . . . . .		74
<b>4</b>	<b>DISTRIBUTED DEPLOYMENT</b>	<b>75</b>
Installing an SO Server Using the SO .iso Image . . . . .		76
SO Server Considerations . . . . .		76
Building Your SO Server . . . . .		77
Configuring Your SO Server . . . . .		78
Installing an SO Sensor Using the SO .iso Image . . . . .		80
Configuring the SO Sensor . . . . .		81
Completing Setup . . . . .		83
Verifying that the Sensors Are Working . . . . .		84
Verifying that the Autossh Tunnel Is Working . . . . .		84

Building an SO Server Using PPAs . . . . .	85
Installing Ubuntu Server as the SO Server Operating System . . . . .	85
Choosing a Static IP Address . . . . .	87
Updating the Software . . . . .	88
Beginning MySQL and PPA Setup on the SO Server . . . . .	89
Configuring Your SO Server via PPA . . . . .	90
Building an SO Sensor Using PPAs . . . . .	92
Installing Ubuntu Server as the SO Sensor Operating System . . . . .	92
Configuring the System as a Sensor . . . . .	94
Running the Setup Wizard . . . . .	95
Conclusion . . . . .	98

## **5 SO PLATFORM HOUSEKEEPING 99**

Keeping SO Up-to-Date . . . . .	99
Updating via the GUI . . . . .	100
Updating via the Command Line . . . . .	101
Limiting Access to SO . . . . .	102
Connecting via a SOCKS Proxy . . . . .	103
Changing the Firewall Policy . . . . .	105
Managing SO Data Storage . . . . .	105
Managing Sensor Storage . . . . .	106
Checking Database Drive Usage . . . . .	107
Managing the Sguil Database . . . . .	108
Tracking Disk Usage . . . . .	108
Conclusion . . . . .	109

## **PART III TOOLS**

### **6 COMMAND LINE PACKET ANALYSIS TOOLS 113**

SO Tool Categories . . . . .	114
SO Data Presentation Tools . . . . .	114
SO Data Collection Tools . . . . .	115
SO Data Delivery Tools . . . . .	115
Running Tcpdump . . . . .	116
Displaying, Writing, and Reading Traffic with Tcpdump . . . . .	117
Using Filters with Tcpdump . . . . .	118
Extracting Details from Tcpdump Output . . . . .	121
Examining Full Content Data with Tcpdump . . . . .	122
Using Dumpcap and Tshark . . . . .	122
Running Tshark . . . . .	123
Running Dumpcap . . . . .	123
Running Tshark on Dumpcap's Traffic . . . . .	125
Using Display Filters with Tshark . . . . .	125
Tshark Display Filters in Action . . . . .	127

Running Argus and the Ra Client . . . . .	128
Stopping and Starting Argus . . . . .	129
The Argus File Format . . . . .	129
Examining Argus Data . . . . .	130
Conclusion . . . . .	133

## **7 GRAPHICAL PACKET ANALYSIS TOOLS 135**

Using Wireshark . . . . .	136
Running Wireshark . . . . .	136
Viewing a Packet Capture in Wireshark . . . . .	137
Modifying the Default Wireshark Layout . . . . .	137
Some Useful Wireshark Features . . . . .	140
Using Xplico . . . . .	147
Running Xplico . . . . .	147
Creating Xplico Cases and Sessions . . . . .	148
Processing Network Traffic . . . . .	149
Understanding the Decoded Traffic . . . . .	150
Getting Metadata and Summarizing Traffic . . . . .	153
Examining Content with NetworkMiner . . . . .	153
Running NetworkMiner . . . . .	154
Collecting and Organizing Traffic Details . . . . .	155
Rendering Content . . . . .	156
Conclusion . . . . .	157

## **8 NSM CONSOLES 159**

An NSM-centric Look at Network Traffic . . . . .	160
Using Sguil . . . . .	161
Running Sguil . . . . .	161
Sguil's Six Key Functions . . . . .	164
Using Squert . . . . .	173
Using Snorby . . . . .	174
Using ELSA . . . . .	178
Conclusion . . . . .	181

# **PART IV NSM IN ACTION**

## **9 NSM OPERATIONS 185**

The Enterprise Security Cycle . . . . .	186
The Planning Phase . . . . .	187
The Resistance Phase . . . . .	187
The Detection and Response Phases . . . . .	187

Collection, Analysis, Escalation, and Resolution . . . . .	188
Collection . . . . .	189
Analysis . . . . .	193
Escalation . . . . .	195
Resolution . . . . .	198
Remediation . . . . .	201
Using NSM to Improve Security . . . . .	202
Building a CIRT . . . . .	203
Conclusion . . . . .	205

## **10**

### **SERVER-SIDE COMPROMISE 207**

Server-side Compromise Defined . . . . .	208
Server-side Compromise in Action . . . . .	209
Starting with Sguil . . . . .	210
Querying Sguil for Session Data . . . . .	211
Returning to Alert Data . . . . .	214
Reviewing Full Content Data with Tshark . . . . .	216
Understanding the Backdoor . . . . .	218
What Did the Intruder Do? . . . . .	219
What Else Did the Intruder Do? . . . . .	222
Exploring the Session Data . . . . .	224
Searching Bro DNS Logs . . . . .	225
Searching Bro SSH Logs . . . . .	226
Searching Bro FTP Logs . . . . .	228
Decoding the Theft of Sensitive Data . . . . .	229
Extracting the Stolen Archive . . . . .	230
Stepping Back . . . . .	231
Summarizing Stage 1 . . . . .	231
Summarizing Stage 2 . . . . .	232
Next Steps . . . . .	232
Conclusion . . . . .	233

## **11**

### **CLIENT-SIDE COMPROMISE 235**

Client-side Compromise Defined . . . . .	236
Client-side Compromise in Action . . . . .	237
Getting the Incident Report from a User . . . . .	238
Starting Analysis with ELSA . . . . .	239
Looking for Missing Traffic . . . . .	243
Analyzing the Bro dns.log File . . . . .	245
Checking Destination Ports . . . . .	246
Examining the Command-and-Control Channel . . . . .	250
Initial Access . . . . .	251
Improving the Shell . . . . .	255
Summarizing Stage 1 . . . . .	256
Pivoting to a Second Victim . . . . .	257
Installing a Covert Tunnel . . . . .	257

Enumerating the Victim . . . . .	259
Summarizing Stage 2 . . . . .	260
Conclusion . . . . .	261

**12**  
**EXTENDING SO** **263**

Using Bro to Track Executables . . . . .	264
Hashing Downloaded Executables with Bro . . . . .	264
Submitting a Hash to VirusTotal. . . . .	264
Using Bro to Extract Binaries from Traffic. . . . .	266
Configuring Bro to Extract Binaries from Traffic. . . . .	266
Collecting Traffic to Test Bro . . . . .	267
Testing Bro to Extract Binaries from HTTP Traffic . . . . .	269
Examining the Binary Extracted from HTTP . . . . .	270
Testing Bro to Extract Binaries from FTP Traffic . . . . .	272
Examining the Binary Extracted from FTP . . . . .	273
Submitting a Hash and Binary to VirusTotal . . . . .	273
Restarting Bro . . . . .	275
Using APT1 Intelligence . . . . .	277
Using the APT1 Module . . . . .	278
Installing the APT1 Module . . . . .	280
Generating Traffic to Test the APT1 Module . . . . .	280
Testing the APT1 Module . . . . .	281
Reporting Downloads of Malicious Binaries. . . . .	283
Using the Team Cymru Malware Hash Registry. . . . .	283
The MHR and SO: Active by Default . . . . .	285
The MHR and SO vs. a Malicious Download . . . . .	286
Identifying the Binary. . . . .	287
Conclusion . . . . .	288

**13**  
**PROXIES AND CHECKSUMS** **289**

Proxies . . . . .	289
Proxies and Visibility . . . . .	290
Dealing with Proxies in Production Networks . . . . .	294
Checksums . . . . .	294
A Good Checksum . . . . .	295
A Bad Checksum . . . . .	295
Identifying Bad and Good Checksums with Tshark . . . . .	296
How Bad Checksums Happen . . . . .	298
Bro and Bad Checksums . . . . .	298
Setting Bro to Ignore Bad Checksums. . . . .	300
Conclusion . . . . .	302

**CONCLUSION** **303**

Cloud Computing . . . . .	304
Cloud Computing Challenges . . . . .	304
Cloud Computing Benefits . . . . .	306

Workflow, Metrics, and Collaboration . . . . .	307
Workflow and Metrics . . . . .	307
Collaboration . . . . .	308
Conclusion . . . . .	309

## APPENDIX

### SO SCRIPTS AND CONFIGURATION 311

SO Control Scripts . . . . .	311
/usr/sbin/nsm . . . . .	313
/usr/sbin/nsm_all_del . . . . .	313
/usr/sbin/nsm_all_del_quick . . . . .	314
/usr/sbin/nsm_sensor . . . . .	315
/usr/sbin/nsm_sensor_add . . . . .	316
/usr/sbin/nsm_sensor_backup-config . . . . .	316
/usr/sbin/nsm_sensor_backup-data . . . . .	316
/usr/sbin/nsm_sensor_clean . . . . .	316
/usr/sbin/nsm_sensor_clear . . . . .	316
/usr/sbin/nsm_sensor_del . . . . .	316
/usr/sbin/nsm_sensor_edit . . . . .	317
/usr/sbin/nsm_sensor_ps-daily-restart . . . . .	317
/usr/sbin/nsm_sensor_ps-restart . . . . .	317
/usr/sbin/nsm_sensor_ps-start . . . . .	319
/usr/sbin/nsm_sensor_ps-status . . . . .	319
/usr/sbin/nsm_sensor_ps-stop . . . . .	320
/usr/sbin/nsm_server . . . . .	320
/usr/sbin/nsm_server_add . . . . .	320
/usr/sbin/nsm_server_backup-config . . . . .	320
/usr/sbin/nsm_server_backup-data . . . . .	320
/usr/sbin/nsm_server_clear . . . . .	321
/usr/sbin/nsm_server_del . . . . .	321
/usr/sbin/nsm_server_edit . . . . .	321
/usr/sbin/nsm_server_ps-restart . . . . .	321
/usr/sbin/nsm_server_ps-start . . . . .	321
/usr/sbin/nsm_server_ps-status . . . . .	321
/usr/sbin/nsm_server_ps-stop . . . . .	321
/usr/sbin/nsm_server_sensor-add . . . . .	322
/usr/sbin/nsm_server_sensor-del . . . . .	322
/usr/sbin/nsm_server_user-add . . . . .	322
SO Configuration Files . . . . .	322
/etc/nsm/ . . . . .	322
/etc/nsm/administration.conf . . . . .	323
/etc/nsm/ossec/ . . . . .	323
/etc/nsm/pulledpork/ . . . . .	323
/etc/nsm/rules/ . . . . .	323
/etc/nsm/securityonion/ . . . . .	324
/etc/nsm/securityonion.conf . . . . .	324
/etc/nsm/sensortab . . . . .	325
/etc/nsm/servertab . . . . .	326
/etc/nsm/templates/ . . . . .	326
/etc/nsm/\$HOSTNAME-\$INTERFACE/ . . . . .	326
/etc/cron.d/ . . . . .	330

Bro .....	330
CapMe .....	331
ELSA .....	331
Squert .....	331
Snorby .....	331
Syslog-ng .....	331
/etc/network/interfaces .....	331
Updating SO .....	332
Updating the SO Distribution .....	332
Updating MySQL .....	333

## **INDEX**

**335**