

CONTENTS IN DETAIL

ACKNOWLEDGMENTS	xv
------------------------	-----------

FOREWORD by Richard Bejtlich	xvii
-------------------------------------	-------------

INTRODUCTION	1
---------------------	----------

Why Detect Attacks with iptables?	2
What About Dedicated Network Intrusion Detection Systems?	3
Defense in Depth	4
Prerequisites	4
Technical References	5
About the Website	5
Chapter Summaries	6

1	
CARE AND FEEDING OF IPTABLES	9

iptables	9
Packet Filtering with iptables	10
Tables	11
Chains	11
Matches	12
Targets	12
Installing iptables	12
Kernel Configuration	14
Essential Netfilter Compilation Options	15
Finishing the Kernel Configuration	16
Loadable Kernel Modules vs. Built-in Compilation and Security	16
Security and Minimal Compilation	17
Kernel Compilation and Installation	18
Installing the iptables Userland Binaries	19
Default iptables Policy	20
Policy Requirements	20
iptables.sh Script Preamble	22
The INPUT Chain	22
The OUTPUT Chain	24
The FORWARD Chain	25
Network Address Translation	26
Activating the Policy	27
iptables-save and iptables-restore	27
Testing the Policy: TCP	29
Testing the Policy: UDP	31
Testing the Policy: ICMP	32
Concluding Thoughts	33

2	NETWORK LAYER ATTACKS AND DEFENSE	35
Logging Network Layer Headers with iptables		35
Logging the IP Header		36
Network Layer Attack Definitions		38
Abusing the Network Layer		39
Nmap ICMP Ping		39
IP Spoofing		40
IP Fragmentation		41
Low TTL Values		42
The Smurf Attack		43
DDoS Attacks		44
Linux Kernel IGMP Attack		44
Network Layer Responses		45
Network Layer Filtering Response		45
Network Layer Thresholding Response		45
Combining Responses Across Layers		46
3	TRANSPORT LAYER ATTACKS AND DEFENSE	49
Logging Transport Layer Headers with iptables		50
Logging the TCP Header		50
Logging the UDP Header		52
Transport Layer Attack Definitions		52
Abusing the Transport Layer		53
Port Scans		53
Port Sweeps		61
TCP Sequence Prediction Attacks		61
SYN Floods		62
Transport Layer Responses		62
TCP Responses		62
UDP Responses		66
Firewall Rules and Router ACLs		67
4	APPLICATION LAYER ATTACKS AND DEFENSE	69
Application Layer String Matching with iptables		70
Observing the String Match Extension in Action		70
Matching Non-Printable Application Layer Data		71
Application Layer Attack Definitions		72
Abusing the Application Layer		73
Snort Signatures		74
Buffer Overflow Exploits		74
SQL Injection Attacks		76
Gray Matter Hacking		77
Encryption and Application Encodings		79
Application Layer Responses		80

5 INTRODUCING PSAD: THE PORT SCAN ATTACK DETECTOR 81

History	81
Why Analyze Firewall Logs?	82
psad Features	83
psad Installation	83
psad Administration	85
Starting and Stopping psad	85
Daemon Process Uniqueness	86
iptables Policy Configuration	86
syslog Configuration	88
whois Client	89
psad Configuration	90
/etc/psad/psad.conf	90
/etc/psad/auto_dl	96
/etc/psad/signatures	96
/etc/psad/snort_rule_dl	97
/etc/psad/ip_options	97
/etc/psad/pf.os	97
Concluding Thoughts	98

6 PSAD OPERATIONS: DETECTING SUSPICIOUS TRAFFIC 99

Port Scan Detection with psad	100
TCP connect() Scan	101
TCP SYN or Half-Open Scan	103
TCP FIN, XMAS, and NULL Scans	105
UDP Scan	106
Alerts and Reporting with psad	108
psad Email Alerts	108
psad syslog Reporting	110
Concluding Thoughts	112

7 ADVANCED PSAD TOPICS: FROM SIGNATURE MATCHING TO OS FINGERPRINTING 113

Attack Detection with Snort Rules	113
Detecting the ipEye Port Scanner	115
Detecting the LAND Attack	116
Detecting TCP Port 0 Traffic	116
Detecting Zero TTL Traffic	117
Detecting the Naptha Denial of Service Attack	117
Detecting Source Routing Attempts	118
Detecting Windows Messenger Pop-up Spam	118
psad Signature Updates	119
OS Fingerprinting	120
Active OS Fingerprinting with Nmap	120
Passive OS Fingerprinting with pOf	121

DShield Reporting	123
DShield Reporting Format	124
Sample DShield Report	124
Viewing psad Status Output	124
Forensics Mode	128
Verbose/Debug Mode	128
Concluding Thoughts	130

8 ACTIVE RESPONSE WITH PSAD 131

Intrusion Prevention vs. Active Response	131
Active Response Trade-offs	133
Classes of Attacks	133
False Positives	134
Responding to Attacks with psad	134
Features	135
Configuration Variables	135
Active Response Examples	137
Active Response Configuration Settings	138
SYN Scan Response	139
UDP Scan Response	140
Nmap Version Scan	141
FIN Scan Response	141
Maliciously Spoofing a Scan	142
Integrating psad Active Response with Third-Party Tools	143
Command-Line Interface	143
Integrating with Swatch	145
Integrating with Custom Scripts	146
Concluding Thoughts	147

9 TRANSLATING SNORT RULES INTO IPTABLES RULES 149

Why Run fwsnort?	150
Defense in Depth	151
Target-Based Intrusion Detection and Network Layer Defragmentation	151
Lightweight Footprint	152
Inline Responses	152
Signature Translation Examples	153
Nmap command attempt Signature	153
Bleeding Snort “Bancos Trojan” Signature	154
PGPNet connection attempt Signature	154
The fwsnort Interpretation of Snort Rules	155
Translating the Snort Rule Header	155
Translating Snort Rule Options: iptables Packet Logging	157
Snort Options and iptables Packet Filtering	160
Unsupported Snort Rule Options	171
Concluding Thoughts	172

10	DEPLOYING FWSNORT	173
Installing fwsnort		173
Running fwsnort		175
Configuration File for fwsnort		177
Structure of fwsnort.sh		179
Command-Line Options for fwsnort		182
Observing fwsnort in Action		184
Detecting the Trin00 DDoS Tool		184
Detecting Linux Shellcode Traffic		185
Detecting and Reacting to the Dumador Trojan		186
Detecting and Reacting to a DNS Cache-Poisoning Attack		188
Setting Up Whitelists and Blacklists		191
Concluding Thoughts		192
11	COMBINING PSAD AND FWSNORT	193
Tying fwsnort Detection to psad Operations		194
WEB-PHP Setup.php access Attack		194
Revisiting Active Response		198
psad vs. fwsnort		198
Restricting psad Responses to Attacks Detected by fwsnort		199
Combining fwsnort and psad Responses		199
DROP vs. REJECT Targets		201
Thwarting Metasploit Updates		204
Metasploit Update Feature		204
Signature Development		206
Busting Metasploit Updates with fwsnort and psad		208
Concluding Thoughts		212
12	PORT KNOCKING VS. SINGLE PACKET AUTHORIZATION	213
Reducing the Attack Surface		213
The Zero-Day Attack Problem		214
Zero-Day Attack Discovery		215
Implications for Signature-Based Intrusion Detection		215
Defense in Depth		216
Port Knocking		217
Thwarting Nmap and the Target Identification Phase		218
Shared Port-Knocking Sequences		218
Encrypted Port-Knocking Sequences		221
Architectural Limitations of Port Knocking		223
Single Packet Authorization		226
Addressing Limitations of Port Knocking		227
Architectural Limitations of SPA		228
Security Through Obscurity?		229
Concluding Thoughts		230

13		
INTRODUCING FWKNOP		231
fwknop Installation		232
fwknop Configuration		234
/etc/fwknop/fwknop.conf		234
/etc/fwknop/access.conf		237
Example /etc/fwknop/access.conf File		240
fwknop SPA Packet Format		241
Deploying fwknop		243
SPA via Symmetric Encryption		244
SPA via Asymmetric Encryption		246
Detecting and Stopping a Replay Attack		249
Spoofing the SPA Packet Source Address		251
fwknop OpenSSH Integration Patch		252
SPA over Tor		254
Concluding Thoughts		255
14		
VISUALIZING IPTABLES LOGS		257
Seeing the Unusual		258
Gnuplot		260
Gnuplot Graphing Directives		260
Combining psad and Gnuplot		261
AfterGlow		262
iptables Attack Visualizations		263
Port Scans		264
Port Sweeps		267
Slammer Worm		270
Nachi Worm		272
Outbound Connections from Compromised Systems		273
Concluding Thoughts		277
A		
ATTACK SPOOFING		279
Connection Tracking		280
Spoofing exploit.rules Traffic		282
Spoofed UDP Attacks		283
B		
A COMPLETE FWSNORT SCRIPT		285
INDEX		291