INDEX

A

- `ACCEPT` rules
  - and `DROP` rule, 46
  - for SSH connections, 23
- `ACCEPT` target, 12
- access directive, for fwknop server, 242
- ACK scan, 64
- `ack` Snort rule option, 158, 159
- acknowledgment values, inclusion in iptables, 51
- active response
  - examples, 137–143
    - configuration settings, 138–139
    - FIN scan response, 141–142
    - maliciously spoofing scan, 142–143
    - Nmap version scan, 141
    - SYN scan response, 139–140
    - UDP scan response, 140–141
  - integrating with third-party tools, 143–147
    - command-line interface, 143–144
  - vs. intrusion detection, 131–133
  - psad vs. fwsnort, 198–199
  - trade-offs, 133–134
- Address Resolution Protocol (ARP), 22
- Advanced Encryption Standard (AES), 243
- AfterGlow, 257, 262–263
- Aleph One, 75
- `alert` action
  - in fwsnort, 157
  - in Snort, 156
- `ALERT_ALL` variable, in psad.conf file, 93
- `ALERTING_METHODS` variable, in psad.conf file, 95
- `--algo bm` argument, 70
- `--analysis-fields` argument, for psad, 266
- anomaly, problem defining, 216
- application layer, 69
  - abusing, 73–79
    - buffer overflow exploits, 74–76
    - gray matter hacking, 77–79
    - Snort signatures, 74
    - SQL injection attacks, 76–77
  - attack definitions, 72–73
  - encryption and application encodings, 79–80
  - responses, 80
  - string matching with iptables, 70–72
    - non-printable data match, 71–72
- *Applied Cryptography* (Schneier), 229
- ARP (Address Resolution Protocol), 22
- `asn1` keyword, in Snort, 171
- asymmetric encryption, SPA with, 246–249
- asymmetric-key cipher, 243
- Atkins, Todd, 145
- attacking IP addresses, psad display of top fifty, 126
- attacks
  - classes of, 133
  - concealing with fragments and targeted TTLs, 43
  - expectation of, 4
  - psad for responding to, 134–137
  - raw packet data for analysis, 3

attacks, *continued*
reducing surface, 213–214
Snort rules for detecting, 113–119
spoofing, 279–283
connection tracking, 280–283
visualizations, 263–277
Nachi worm, 272–273
of port scans, 264–267
of port sweeps, 267–270
SQL Slammer worm, 270–271
authentication, 232
tricking user into providing credentials, 77
AUTH_MODE variable, for fwknop, 234
authorization, 232
AUTO_BLOCK_REGEX variable, 136, 199
AUTO_BLOCK_TIMEOUT variable, 136, 138
AUTO_IDS_DANGER_LEVEL variable, 136, 199
automatically blocked IP addresses, psad display of, 127
auto-response messages, from psad, 111
AVG_IP_HEADER_LEN keyword, in /etc/fwsnort/fwsnort.conf file, 166
AVG_TCP_HEADER_LEN keyword, in /etc/fwsnort/fwsnort.conf file, 166

B

back reference, regular expression with, 145
backdoor, 78–79
backdoor server, in Dumador trojan, 186
"Bancos Trojan" signature, 154
bandwidth, saturation, 39
Base64-encode, 243
Bastille Linux project, 4, 81
Bastille-NIDS, 82
Beale, Jay, 82
Bernstein, Daniel, 66
BINDIR variable, 19
BlackICE, 132
blacklists, setup, 191
Bleeding Snort project, 174
"Bancos Trojan" signature, 154
detection of attempts to truncate SQL query section, 76
bleeding-all.rules file, 188
blocked IP addresses, automatically, psad display of, 127
blocking rules, changing, 144
botnet, 199
Bourne shell script
fwsnort.sh script, 179–182
for implementing iptables filtering policy, 20
Boyer-Moore string search algorithm, 70, 71, 160
buffer overflow exploits, 74–76
Bugtraq, 214
ID 9057, 194
byte_jump option, in Snort, 171
byte_test option, in Snort, 171

C

C applications, buffer overflow, 74–75
C++ applications, buffer overflow, 74–75
California legislation, consumer notification of data theft, 214
cd00r, 217
CGI applications, as SQL injection attack target, 76
chains, 10–11. *See also individual chain names*
FORWARD, 11
in default policy, 25–26
listing current ruleset, 19
LOG rule in, 50–51
messages logged within, 102
FWKNOP_INPUT, 245
FWSNORT_FORWARD, 180, 189
FWSNORT_FORWARD_ESTAB, 181, 195
FWSNORT_INPUT, 180
FWSNORT_OUTPUT, 180
INPUT, 11
in default policy, 22–24
listing current ruleset, 19
LOG rule in, 50–51
messages logged within, 102

OUTPUT, 11
in default policy, 24
listing current ruleset, 19
LOG rule in, 50–51
messages logged within, 102
POSTROUTING, 11, 26
PREROUTING, 11, 26
viewing list of, 143
character device, 17
Check Point, 143
CHECK_INTERVAL variable, in psad.conf file, 92
chown command, signature for overflow against, 75
client-side vulnerabilities, over TCP, 30
CMD_REGEX variable, in /etc/fwknop/access.conf file, 238–239
code reuse, in computer underground, 216
--comment match, 12
compiling kernel, 18
compromised systems, outbound connections from, 273–277
CONFIG_SYN_COOKIES, kernel compiled with, 66
connection resource exhaustion, as transport layer attack, 52
connection tracking, 280–283
connectionless protocol, 49–50
connection-oriented protocol, 49
content Snort option, 160
cookies, mishandling, 73
counthouruniq directive, 265
Crypt::CBC Perl module, 233
Crypt::Rijndael Perl module, 233
--CSV-fields argument, for psad, 261
--CSV-regex argument, for psad, 262

D

danger level, in psad email alert, 108
DANGER_LEVEL{*n*} variable, in psad.conf file, 91
data transmission rate, minimal, and port knocking, 224
DATA_COLLECT_MODE variable, in /etc/fwknop/access.conf file, 239
Data::Dumper Perl module, 127
DDoS (Distributed Denial of Service) attacks, 44, 83
Trin00 tool for, 184–185
Debian package, installing psad as, 84
--debug switch, in psad, 128–129
default iptables policy
FORWARD chain, 25–26
INPUT chain, 22–24
instantiating, 27
Network Address Translation, 26–27
OUTPUT chain, 24
saving, 27–29
script preamble, 20–21
testing, 29–31
default-drop packet filter, 214
making connection through, 217
defense in depth principle, 4, 82, 151, 216
Denial of Service (DoS) attack. *See* DoS (Denial of Service) attack
depth Snort option, 162
--destination (-d) match, 12
destination IP address
in psad email alert, 109
specifying in Snort, 157
destination NAT (DNAT) target, 26
directories, for psad install, 85
distance Snort option, 161, 162
Distributed Denial of Service (DDoS) attacks, 44, 83
Trin00 tool for, 184–185
d'Itri, Marco, 89, 109
DNAT (destination NAT) target, 26
DNS cache-poisoning attack, detecting, 188–190
documentation, in psad.conf file, 90
DoS (Denial of Service) attack
against knock server, 225
LAND attack as, 116
Naptha, 117
downloading
latest version of psad, 83
Metasploit framework, 205–206
from mirror servers, 14
DROP rule, and ACCEPT rules, 46
DROP target, 12
vs. REJECT target, 201–204

DShield Distributed IDS, 84
  psad display of statistics, 127
  reporting, 123–124
DSHIELD_ALERT_INTERVAL variable, 123
DSHIELD_USER_ID variable, 123
dsize Snort option, 165–166
Dumador trojan, detecting, 186–188
dynamic action, in Snort, 156

E

Echo Reply packets, iptables policy for accepting, 32
Elgamal cryptosystem, 246*n*
email alerts from psad, 108–110
  on attempted Metasploit update, 210–211
EMAIL_ADDRESSES variable
  for fwknop, 237, 245
  in psad.conf file, 91
EMAIL_ALERT_DANGER_LEVEL variable, in psad.conf file, 93
EMAIL_LIMIT variable, in psad.conf file, 95
ENABLE_AUTO_IDS variable, in psad.conf file, 94, 127, 135, 199
ENABLE_AUTO_IDS_REGEX variable, 136, 139
ENABLE_CMD_EXEC variable, in /etc/fwknop/access.conf file, 238
ENABLE_DSHIELD_ALERTS variable, in psad.conf file, 94
ENABLE_MD5_PERSISTENCE variable, for fwknop, 236
ENABLE_PCAP_PROMISC variable, for fwknop, 235
ENABLE_PERSISTANCE variable, in psad.conf file, 92, 109
ENABLE_SPA_PACKET_AGING variable, for fwknop, 236
ENABLE_TCP_SERVER variable, for fwknop, 237
enc_knock.pl script, 223
encryption, asymmetric, SPA with, 246–249
entry router, for virtual circuit, 254
ESTABLISHED state, 23
/etc/fwknop/access.conf file, 237–240
  CMD_REGEX variable, 238–239
  DATA_COLLECT_MODE variable, 239
  ENABLE_CMD_EXEC variable, 238
  example, 240–241
  FW_ACCESS_TIMEOUT variable, 239
  GPG_DECRYPT_ID variable, 240
  GPG_DECRYPT_PW variable, 240
  GPG_REMOTE_ID variable, 240
  KEY variable, 239
  OPEN_PORTS variable, 238
  PERMIT_CLIENT_PORTS variable, 238
  REQUIRE_USERNAME variable, 239
  SOURCE variable, 238
/etc/fwknop directory, 233
/etc/fwknop/fwknop.conf file, 234–237
  AUTH_MODE variable, 234
  EMAIL_ADDRESSES variable, 237
  ENABLE_MD5_PERSISTENCE variable, 236
  ENABLE_PCAP_PROMISC variable, 235
  ENABLE_SPA_PACKET_AGING variable, 236
  ENABLE_TCP_SERVER variable, 237
  FIREWALL_TYPE variable, 235
  GPG_DEFAULT_HOME_DIR variable, 237
  IPT_AUTO_CHAIN1 variable, 235
  MAX_SPA_PACKET_AGE variable, 236
  PCAP_FILTER variable, 234–235
  PCAP_INFT variable, 234
  PCAP_PKT_FILE variable, 235
  REQUIRE_SOURCE_ADDRESS variable, 236–237
  TCPSERV_PORT variable, 237
/etc/fwsnort/fwsnort.conf file, 177
  WHITELIST and BLACKLIST variables, 191
/etc/fwsnort/fwsnort.sh script, 200
/etc/hosts.deny file, 134
/etc/init.d/fwknop initialization script, 234
/etc/psad/auto_dl file, 96, 108
  psad and, 143
/etc/psad/ip_options file, 97
/etc/psad/pf.os file, 97–98
/etc/psad/psad.conf file, 90–96
  ALERT_ALL variable, 93
  ALERTING_METHODS variable, 95

  - `AUTO_BLOCK_REGEX` variable, 136
  - `AUTO_BLOCK_TIMEOUT` variable, 136, 138
  - `AUTO_IDS_DANGER_LEVEL` variable, 136, 137
  - `CHECK_INTERVAL` variable, 92
  - `DANGER_LEVEL{n}` variable, 91
  - `DSHIELD_ALERT_INTERVAL` variable, 123
  - `DSHIELD_USER_ID` variable, 123
  - `EMAIL_ADDRESSES` variable, 91
  - `EMAIL_ALERT_DANGER_LEVEL` variable, 93
  - `EMAIL_LIMIT` variable, 95
  - `ENABLE_AUTO_IDS` variable, 94, 127, 135
  - `ENABLE_AUTO_IDS_REGEX` variable, 136, 139
  - `ENABLE_DSHIELD_ALERTS` variable, 94
  - `ENABLE_PERSISTANCE` variable, 92
  - `EXTERNAL_NET` variable, 91
  - `FW_MSG_SEARCH` variable, 95–96
  - `HOME_NET` variable, 91
  - `IGNORE_LOG_PREFIXES` variable, 95
  - `IGNORE_PORTS` variable, 94
  - `IGNORE_PROTOCOLS` variable, 95
  - `IMPORT_OLD_SCANS` variable, 94
  - `IPTABLES_BLOCK_METHOD` variable, 136
  - `IPT_AUTO_CHAIN{n}` variables, 137, 139
  - `MIN_DANGER_LEVEL` variable, 93
  - `PORT_RANGE_SCAN_THRESHOLD` variable, 92–93
  - `SCAN_TIMEOUT` variable, 92
  - `SHOW_ALL_SIGNATURES` variable, 93
  - `SNORT_SID_STR` variable, 93
  - `STATUS_IP_THRESHOLD` variable, 126
  - `STATUS_PORTS_THRESHOLD` variable, 127
  - `SYSLOG_DAEMON` variable, 92
  - `TCPWRAPPERS_BLOCK_METHOD` variable, 136
- /etc/psad/signatures file, 96, 114
- /etc/psad/snort_rule_dl file, 97
- Ethernet sniffer, 4
  - for extracting user and password information, 79
- exit router, for virtual circuit, 254
- exploit code, 75
- `EXTERNAL_NET` variable
  - for fwsnort, 177
  - in psad.conf file, 91

F

- false negatives, 134
- false positives, 3
  - hiding attacks in, 279
  - in intrusion detection systems, 134
- Filesystem Hierarchy Standard (FHS), 85
- `filter` table, 11
- filtering response, in network layer, 45
- FIN scans
  - detection with psad, 105–106
  - and Netfilter connection tracking, 105
  - response, 141–142
  - of TCP ports, 58
- FireWall KNock OPerator (fwknop). *See* fwknop (FireWall KNock OPerator)
- firewall logs, reasons for analyzing, 72
- Firewall Snort. *See* fwsnort (Firewall Snort)
- firewalls
  - and intrusion detection systems, 82
  - and intrusion prevention system,150
  - rules, and router ACLs, 67
  - technology trends, 1
- `FIREWALL_TYPE` variable, for fwknop, 235
- `flags` Snort option, 162–163
- flexresp detection plug-in, in Snort, 65
- flexresp2 detection plug-in, in Snort, 65
- flexresponse detection plug-in, `resp` option, 169
- flexresponse2 detection plug-in, `resp` option, 169
- flooding target, with ICMP Echo Response Packets, 43
- `flow` Snort option, 166–168
- `flowbits` option, in Snort, 171
- `--Flush` argument, 144
- forensics mode, in psad, 128, 266
- `FORWARD` chain, 11
  - in default policy, 25–26
  - listing current ruleset, 19
  - `LOG` rule in, 50–51
  - messages logged within, 102

frag3 preprocessor, 151
fragbits option, in Snort, 172
fragments, concealing attack with, 43
fragroute tool, 42
FsSniffer backdoor, 79
Full-disclosure, 214
--fw-block-ip argument, 144
--fw-list argument, 143
--fw-rm-block-ip argument, 144
FW_ACCESS_TIMEOUT variable, in /etc/fwknop/access.conf file, 239
fwcheck_psad script, 86
fwdata file, log messages from, 102
fwknop (FireWall KNock OPerator), 2, 231
- configuration, 234–241
  - /etc/fwknop/access.conf file, 237–240
  - /etc/fwknop/fwknop.conf file, 234–237
- deploying, 243–255
- GnuPG keys
  - exchange, 246–249
  - running with, 248–249
- installing, 232–234
- OpenSSH integration patch, 252–253
- rules and iptables policy rules, 246
- SPA packet format, 241–243

FWKNOP_INPUT chain, 245
fwknop_serv daemon, 254
FW_MSG_SEARCH variable, in psad.conf file, 95–96
fwsnort (Firewall Snort), 2, 119, 149
- active response vs. psad, 198–199
- attack detection with, 195–196
  - restricting psad responses, 199
- command-line options, 182–183
- configuration file, 177–179
- DROP vs. REJECT targets, 201–204
- example attacks, 184–190
  - DNS cache-poisoning attack, 188–190
  - Dumador Trojan, 186–188
  - Linux shellcode traffic detection, 185–186
  - Trin00 DDoS tool detection, 184–185
- installing, 173–175
- iptables signature policy in, 152
- output, 176
- reasons to run, 150–152
  - defense in depth principle, 151
  - inline responses, 152
  - intrusion detection and network layer defragmentation, 151–152
  - lightweight footprint, 152
- running, 175–183
- Snort rules interpretation, 155–172
- for stopping Metasploit updates, 208–211
- tying detection to psad operations, 194–198
- whitelists and blacklists setup, 191

FWSNORT_FORWARD chain, 180, 189
FWSNORT_FORWARD_ESTAB chain, 181, 195
FWSNORT_INPUT chain, 180
FWSNORT_OUTPUT chain, 180
fswnort.log file, 177
fwsnort.sh script, 177
- example, 285–290
- structure, 179–182
  - activating chains with jump rules, 182
  - signature inspection and log generation, 181–182
  - TCP connection states and chains, 180–182

Fyodor's Top 100 Network Security Tools list, 204

G

getlogin() function (Perl), 241
getpwuid() function (Perl), 241
GnuPG, 243
- key exchange for fwknop, 246–249
- signature, 232
  - verifying, 83

GnuPG::Interface Perl module, 233
Gnuplot, 257, 260–262
- graphing directives, 260–261
- plot of port scan, 264

--gnuplot argument, for psad, 260, 261

--gnuplot-file-prefix argument, for psad, 262
--gnuplot-graph-style argument, for psad, 262
GPG_DECRYPT_ID variable, in /etc/fwknop/access.conf file, 240
GPG_DECRYPT_PW variable, in /etc/fwknop/access.conf file, 240
GPG_DEFAULT_HOME_DIR variable, for fwknop, 237
GPG_REMOTE_ID variable, in /etc/fwknop/access.conf file, 240
graphs
  external source addresses vs. destination ports vs. packet counts, 268
  external sources vs. number of unique local destinations, 267
  link graph
    from AfterGlow, 262, 269–270
    of Nachi worm packets, 274
    of outbound connections from honeynet, 276, 277
  MySQL 3306 port sweep, 269
  number of packets to ports per minute, 258
  number of SYN packets to ports per hour, 259
  point graph of outbound connections from honeynet, 275
  Slammer worm packet counts
    by the hour, 271
    by the minute, 272
  source IP addresses vs. number of unique ports, 264
  time vs. unique ports, 266
  value of, 259
  for visualizing security data, 257
gray matter hacking, 77–79
grep command, to view Netfilter configuration, 16
gzip encoding, web browser support for, 80

H

hacking, gray matter, 77–79
half-open (TCP SYN) scans, 56–57
  detection with psad, 103–105
header abuses
  as network layer attacks, 39
  as transport layer attacks, 53
--hex-string argument, 72
HOME_NET variable
  for fwsnort, 177
  in psad.conf file, 91
Honeynet Project, 257–258, 263
  system on open Internet, 273–277
host discovery, 39
hping utility, 31, 32, 41
  to spoof Snort content fields, 167
HTTP, and short-lived SPA sessions, 228–229
HTTP Cross-Site Cooking, 73

I

ICMP (Internet Control Message Protocol)
  list of all message types, 163
  packets in port knocking sequence, 219
  Port Unreachable message, 31, 60, 67, 107
  testing iptables policy over, 32
ICMP Echo Response Packets
  flooding target with, 43
  length of, 165
icmp_id Snort rule option, 158
icmp_seq Snort rule option, 158
icode Snort option, 163
id Snort rule option, 158
iDefense, 214
IDS (intrusion detection system)
  and firewalls, 2, 82, 150
  and RST generation, 65
  searching data for sequences of malicious bytes, 70
  signature-based, implications, 215–216
  target-based, and network layer defragmentation, 151–152

IGMP (Internet Group Management Protocol)
  attacks, 44
  DoS, 39
IGNORE_LOG_PREFIXES variable, in psad.conf file, 95
IGNORE_PORTS variable, in psad.conf file, 94
IGNORE_PROTOCOLS variable, in psad.conf file, 95
IMPORT_OLD_SCANS variable, in psad.conf file, 94
--in-interface (-i) match, 12
IN= string, 88
--include-type option, for fwsnort, 183
informational syslog message, from psad, 110–111
initial sequence numbers, randomization of, 61
initialization scripts, for psad, 85
inline device, 82
INPUT chain, 11
  in default policy, 22–24
  listing current ruleset, 19
  LOG rule in, 50–51
  messages logged within, 102
installing
  fwknop, 232–234
  fwsnort, 173–175
  iptables, 12–14
  iptables Userland Binaries, 19–20
  kernel, 18
  psad, 83–85
instantiating, default iptables policy, 27
Internet Control Message Protocol (ICMP). *See* ICMP (Internet Control Message Protocol)
Internet Group Management Protocol (IGMP). *See* IGMP (Internet Group Management Protocol)
Internet, open, Honeynet Project system on, 273–277
Internet Security Systems, 132
INT_NET variable, defining in iptables.sh script, 22
intrusion detection system (IDS). *See* IDS (intrusion detection system)
intrusion prevention system (IPS). *See* IPS (intrusion prevention system)
INVALID state, 23
IP
  address
    psad mapping to integers for Gnuplot graph, 265
    psad to automatically block, 136
    time for blocking rules against, 140
  communications, dropping all packets, 22
  fragmentation, 41–42
  header
    length of, 165
    logging, 36–38
  spoofing, 40–41, 47
    with Perl, 41
ipEye port scanner, 115
  detecting, 115
ip_options file, for psad, 97
ipopts Snort option, 164–165
ip_proto Snort option, 166
IPS (intrusion prevention system), 3, 82, 150
  and firewalls, 150
  and lightweight system usage footprint, 152
  Snort as, 168
  and worms, 61
IPT_AUTO_CHAIN{*n*} variables, 137, 139
--ipt-drop option, for fwsnort, 182, 195
--ipt-flush option, for fwsnort, 183
--ipt-list option, for fwsnort, 183
--ipt-reject argument, for fwsnort, 208
--ipt-reject option, for fwsnort, 183, 195
iptables, 2, 9–10
  attack visualizations, 263–277
  blocking rules, syslog message showing creation and destruction, 111

building rules file in human-readable format, 27
decoding TCP options from logs, 122–123
default policy, 20–32
FORWARD chain, 25–26
INPUT chain, 22–24
instantiating, 27
Network Address Translation, 26–27
OUTPUT chain, 24
policy requirements, 20–21
saving, 27–29
script preamble, 20–21
testing, 29–31
for detecting attacks, 2–4
emulation in Snort, 156
features, 10
installing, 12–14
installing Userland Binaries, 19–20
log messages, 10
from SYN scan, 55
log prefix, 196
packet filtering with, 10–12
persistent blocking rules when session is shut down, 209
policy configuration in psad, 86–88
and regular expressions, 161
Snort rule options unsupported by, 171–172
string match expression, 70
for supplementing intrusion detection infrastructures, 3
translating Snort rules into rules for, 2
visualizing logs, 257
AfterGlow, 262–263
Gnuplot, 260–262
seeing the unusual, 258–260
iptables-restore command, 27–29
iptables-save command, 27–29
IPTABLES variable, defining in iptables.sh script, 22
IPTABLES_BLOCK_METHOD variable, 136
IPTables::ChainMgr Perl module, 233
IPTables::Parse Perl module, 88, 173, 174, 233
iptables.sh script, 20
preamble, 22
IPT_AUTO_CHAIN1 variable, for fwknop, 235
ipt.save file, 28
IRC client, for backdoor, 78
isdataat option, in Snort, 172
itype Snort option, 163

J

jump rules, to activate fwsnort chains, 182

K

kernel compilation
with CONFIG_SYN_COOKIES, 66
and installing, 18
kernel configuration, 14–17
Netfilter compilation options, 15–16
Core Netfilter configuration, 15
IP: Netfilter configuration, 15–16
saving file, 16
Kernel Rebuild Guide, 13
kernel source code, 13
KERNEL_DIR variable, 19
Kernel-HOWTO, 13
kernel.org webserver, load increase on, 14
key exchange, for asymmetric ciphers, 246
KEY variable, in /etc/fwknop/access.conf file, 239
keylogger, in Dumador trojan, 186
kill() system call, to check for currently running process, 87
klogd (kernel logging daemon), 88
kmsgsd daemon, 84, 85
purpose, 86
Knuth-Morris-Pratt string-searching algorithm, 71
Krzywinski, Martin, 217

L

LAND attack, 116
legitimate traffic, 136
LEN field
  SYN scan vs. connect() scan, 104
  for UDP in iptables log message, 52
length match, for iptables, 165
LIBDIR variable, 19
libpcap, 218
link graph
  from AfterGlow, 262, 269–270
  of Nachi worm packets, 274
  of outbound connections from honeynet, 276, 277
Linux kernel
  configuration and compilation, 13
  IGMP attacks, 44
/linux/net/ipv4/netfilter/ipt-REJECT.c file, 204
Linux shellcode traffic detection, 185–186
Loadable Kernel Module (LKM), Netfilter subsystems as, 16–17
log action
  in fwsnort, 156
  in Snort, 156
log messages, 30
LOG target, 12, 35, 50, 158
--log-tcp-options argument, 50–51, 122
logging
  headers with iptables, 35–38
    ICMP, 38
    IP header, 36–38
    IP options, 37–38
  SYN packet, 104
  TCP headers, 50–51
  UDP headers, 52
  UDP packets, 42
logging prefixes, psad display of, 127
Loose Source Route (lssr) option, testing for, 165
Lowe, Kwan, 13
lynx command, 200

M

MAC address, filtering IP packets based on extension, 22
MadHat, 231
make config command, 14
make menuconfig command, 14
make xconfig command, 14
mangle table, 11
Marty, Raffael, 262
matches, in iptables rule, 12
--max-rtt-timeout option, 101
Maximum Segment Size (MSS) value, 57
MAX_SPA_PACKET_AGE variable, for fwknop, 236
MD5 sum, verifying, 83
Metasploit Project, 204–211
  2.6 updates, 206
  busting updates with fwsnort and psad, 208–211
  downloading and updating framework, 205–206
  signature development, 206–207
Microsoft
  JPEG vulnerability, 30
  operating systems, 215
MIN_DANGER_LEVEL variable, in psad.conf file, 93
mirror servers, downloading from, 14
mode, for SPA packet for fwknop server, 242
MS03-026 vulnerability, 272
msfupdate script, 206
MSS (Maximum Segment Size) value, 57
multicast addresses, packets for, TTL value, 42

N

Nachi worm, 272–273
  link graph, 274
named pipe, 85*n*
Naptha denial of service attack, 117
NAT (Network Address Translation)
  addresses, and piggy-backing, 228
  in default iptables policy, 26–27
  vs. IP spoofing, 40

nat table, 11
National Institutes of Standards and Technology (NIST), 221
Ncurses interface, 14
Netcat, running TCP server on, 170
Netfilter, 9–10
  compilation options, 13
    viewing, 16
  subsystems, security vulnerabilities, 17
Net::IPv4Addr Perl module, 173, 174, 233
Net::Pcap Perl module, 233
Net::RawIP Perl module, 219, 233, 251
network, default diagram, *21*
Network Address Translation (NAT). *See* NAT (Network Address Translation)
Network Anomaly Detection Systems, 216
network layer
  abusing, 39–44
    DDoS attacks, 44
    IP fragmentation, 41–42
    IP spoofing, 40–41
    Linux kernel IGMP attacks, 44
    Nmap ICMP ping, 39–40
    Smurf attack, 43
  attack definitions, 38–39
  defragmentation, intrusion detection and, 151–152
  logging headers with iptables, 35–38
  responses, 45–47
    combining response across layers, 46–47
    filtering response, 45
    thresholding response, 45–46
Network Packet Filtering Framework, 14
network stack exploits, as network layer attacks, 39
NF_DROP macro, 204
NIST (National Institutes of Standards and Technology), 221
Nmap
  active fingerprinting with, 120
  command attempt signature, 153–154
  ICMP ping, 39–40
  for port scans, 100–101
    decoy option, 54
  and round trip times, 101
  scanner, 54
  for testing iptables policy, 31
  use of raw socket, 56
  version scan, 141
--no-addresses option, for fwsnort, 183
--no-ipt-sync option, for fwsnort, 183
--no-rdns option, 109
non-printable data match, in iptables search, 71–72
NSA SELinux distribution, 5
NULL scans
  detection with psad, 105–106
  of TCP ports, 58

O

obscurity, security and, 229–230
offset Snort option, 161–162
Onion Router (Tor), 254
OpenBSD TCP stack, 61
OPEN_PORTS variable, in /etc/fwknop/access.conf file, 238
OpenSSH
  integration patch, for fwknop, 252–253
  project, 215
OPSEC API, 143
OPT field, SYN scan vs. connect() scan, 105
OS fingerprinting, 120–123
  active fingerprinting with Nmap, 120
  combining with port knocking, 231
  passive fingerprinting with p0f, 121–123
OSI Reference Model, 4
--out-interface (-o) match, 12
OUT= string, 88
outbound connections, from compromised systems, 273–277

OUTPUT chain, 11
in default policy, 24
listing current ruleset, 19
LOG rule in, 50–51
messages logged within, 102

P

p0f project
OS database from, psad use of, 97
passive fingerprinting with, 121–123
packet
filtering, with iptables, 10–12
MD5 sum, and fwknop client, 242
payload, for Snort rule, 165
PAM ICQ module, 132
pass action, 156
password
Ethernet sniffer for extracting, 79
theft by Bancos Trojan, 154
Paxson, Vern, 43
PCAP_FILTER variable, for fwknop, 234–235
PCAP_INFT variable, for fwknop, 234
PCAP_PKT_FILE variable, for fwknop, 235
pcre option, in Snort, 172
Perl
IP spoofing with, 41
for main psad daemon, 84
psad requirements for modules, 84
regular expressions, applying to arbitrary logfiles, 145
Perl Compatible Regular Expressions, 172
PERMIT_CLIENT_PORTS variable, in /etc/fwknop/access.conf file, 238
pf.os file, for psad, 97–98
PGPNet connection attempt signature, 154–155
phishing attacks, 73, 77
Phrack, 17
PID file, 87
piggy-backing, and NAT addresses, 228
ping command
to measure round-trip time, 101
timestamp option, 37
plot directive (Gnuplot), 261
port knocking, 217–225
architectural limitations, 223–225
knock sequence busting with spoofed packets, 225
knock sequences and port scans, 224–225
minimal data transmission rate, 224
sequence replay problem, 223–224
combining with OS fingerprinting, 231
encrypted sequences, 221–223
shared sequences, 218–221
SPA for addressing limitations, 227–228
thwarting Nmap and target identification phase, 218
Port Scan Attack Detector. *See* psad (Port Scan Attack Detector)
port scans
detection with psad, 100–107
FIN, XMAS, and NULL scans, 105–106
TCP connect() scan, 101–103
TCP SYN (half-open) scans, 103–105
UDP scans, 106–107
knock sequences and, 224–225
matching to vulnerable services, 53–54
psad detection of, 83
of TCP ports, 54–59
connect() scans, 54–55
FIN, XMAS, and NULL scans, 58
TCP ACK scans, 58
TCP idle scans, 59–60
TCP SYN (half-open) scans, 56–57
UDP scans, 60
visualizations, 264–267
port sweeps, 61
visualizations, 267–270
portkey, 217
PORT_RANGE_SCAN_THRESHOLD variable, in psad.conf file, 92–93
PortSentry, 82

POSTROUTING chain in nat table, 11, 26
PREROUTING chain in nat table, 11, 26
privacy, 69
private key, 243
process ID, of psad daemons, 86
process status information, psad report on, 126
programming bugs, and application layer attacks, 73
--protocol (-p) match, 12
psad (Port Scan Attack Detector), 2, 81
  active response
    configuration settings, 138–139
    vs. fwsnort, 198–199
    integrating with third-party tools, 143–147
  alerts and reporting with, 108–111, 196–197
    email alerts, 108–110
    syslog reporting, 110–111
  attack detection with Snort rules
    ipEye port scanner, 115
    LAND attack, 116
    Naptha denial of service attack, 117
    source routing attempts, 118
    TCP port 0 traffic, 116
    Windows Messenger pop-up spam, 118–119
    zero TTL traffic, 117
  combining with Gnuplot, 261–262
  configuration, 90–98
    /etc/psad/auto_dl, 96
    /etc/psad/ip_options, 97
    /etc/psad/pf.os, 97–98
    /etc/psad/psad.conf, 90–96
    /etc/psad/signatures, 96
    /etc/psad/snort_rule_dl, 97
    variables, 135–137
  daemon process uniqueness, 86
  --debug switch, 128–129
  emulating p0f with, 122
  features, 83
  forensics mode, 128, 266
  --fw-list argument, 143
  --gnuplot mode, 260
  history, 81–82
  installing, 83–85
  intrusion detection vs. active response, 131–133
  iptables policy configuration, 86–88
  number of packets monitored by, 102
  OS fingerprinting, 120–123
    active fingerprinting with Nmap, 120
    passive fingerprinting with p0f, 121–123
  port scan detection with, 100–107
    FIN, XMAS, and NULL scans, 105–106
    TCP connect() scan, 101–103
    TCP SYN (half-open) scans, 103–105
    UDP scans, 106–107
  responding to attacks, 134–137
  --sig-update argument, 119
  signature updates, 119–120
  starting and stopping, 85–86
  --Status, 140
  for stopping Metasploit updates, 208–211
  support for email submission of scan data to DShield, 123
  syslog configuration, 88–89
  tying fwsnort detection to, 194–198
  verbose/debug mode, 128–129
  viewing status output, 124–127
  whois client, 89–90
psad.conf file. *See* /etc/psad/psad.conf file
psad_derived_sids keyword, for Snort rules, 114
psad_dl keyword, for Snort rules, 114
psad_dsize keyword, for Snort rules, 114
psad_id keyword, for Snort rules, 114
psad_ip_len keyword, for Snort rules, 115
psadwatchd daemon, 84, 85, 86
public key, 243
  transfer mechanism, 248

R

rand() function (Perl), 241
raw sockets, 56
  Nmap use of, 56
raw table, 11
RealSecure, 132
reconnaissance against network, 42
Record Route option, detecting, 165
redundancy, 2
regular expressions
  applying to arbitrary logfiles, 145
  with back reference, 145
  and iptables, 161
REJECT target, 12, 64, 169, 170
  vs. DROP target, 201–204
--reject-with icmp-port-unreachable argument, 67
RELATED state, 23
remote operating system fingerprinting, 97
  p0f for, 121
  passively, 83
replace Snort option, 168–169
replay attack, 223
  detecting and stopping, 249–251
  SPA solution for, 227
REQUIRE_SOURCE_ADDRESS variable, for fwknop, 236–237
REQUIRE_USERNAME variable, in /etc/fwknop/access.conf file, 239
Reset (RST) packet, 62
  and intrusion detection systems, 65
  vs. RST/ACK packet, 63–65
Reset/Acknowledgment (RST/ACK) packet, 62–63
  vs. RST packet, 63–65
resource exhaustion, and application layer attacks, 73
resp Snort option, 169
--restrict-intf option, for fwsnort, 183
RETURN target, 12
RFC (Request for Comments)
  791 on IP, 36
  792 on ICMP, 38
  793 on TCP, 50, 63
Rijndael cipher, 217, 221, 243
rmmod command, 16
rootkits, 17
route blackholing, 45
router ACLs, 67
rpc option, in Snort, 172
RPM for Linux distribution, installing psad as, 84
RST (Reset) packet, 62
  and intrusion detection systems, 65
  vs. RST/ACK packet, 63–65
RST/ACK (Reset/Acknowledgment) packet, 62–63
  vs. RST packet, 63–65
Ruby, 205
rules in iptables policy, 10
running process, current, kill() system call to check, 87

S

sameip
  packet header test, 116
  Snort rule option, 158
    for LAND attack detection, 159
saving
  default iptables policy, 27–29
  kernel configuration file, 16
scan match messages, from psad, 111
Scan34 Honeynet challenge, 258, 263
scanned port, states for, 54
scanned TCP and UDP ports, psad display of, 127
SCAN_TIMEOUT variable, in psad.conf file, 92
Schneier, Bruce, *Applied Cryptography*, 229
scripts, 146–147
Sdbot trojan, 78
secure computing, challenge of, 1
security
  for compiling as LKM vs. compiling directly into kernel, 16
  Metasploit Project and, 204
  and minimal compilation, 17–18
  obscurity and, 229–230
seq Snort rule option, 158, 159
server authentication method, for fwknop server, 242

- `set terminal` directive (Gnuplot), 261
- `set title` directive (Gnuplot), 261
- `set xdata time` directive (Gnuplot), 261
- `set xrange` directive (Gnuplot), 261
- shared port-knocking sequences, 218–221
- `SHOW_ALL_SIGNATURES` variable, in psad.conf file, 93
- signature
  - format, in p0f, 121–122
  - match messages, from psad, 111
  - matches, psad display of top fifty, 126
  - translation, examples, 153–155
  - updates, in psad, 119–120
- signature-based intrusion detection, implications, 215–216
- Single Packet Authorization (SPA), 217, 226–229
  - addressing limitations of port knocking, 227–228
  - architectural limitations, 228–229
  - with asymmetric encryption, 246–249
  - ciphertext data length associated with message, 247
  - for fwknop, 231
  - network, 227
  - over Tor, 254–255
  - packet format for fwknop, 241–243
  - spoofing packet source address, 251–252
- Slammer worm, 61
  - visualizations to detect, 270–271
- Smurf attack, 43
- SNAT (source NAT) target, 26
- Snort, 4
  - actions and alerts, 157
  - flexresp and flexresp2 detection plug-ins, 65
  - rule interpretation by fwsnort, 155–172
    - translating Snort rules header, 155–157
  - rule options in iptables
    - explicit matching and filtering support, 160
    - unsupported, 171–172
  - rule translation
    - into iptables rules, 2
    - options, iptables packet logging, 157–159
  - rules for attack detection, 113–119
    - fwsnort for translating into iptables rules, 149
    - ipEye port scanner, 115
    - LAND attack, 116
    - Naptha denial of service attack, 117
    - source routing attempts, 118
    - TCP port 0 traffic, 116
    - Windows Messenger pop-up spam, 118–119
    - zero TTL traffic, 117
  - signature ruleset, 44
  - stateless attacks against, 167
- `--snort-conf` option, for fwsnort, 183
- Snort HTTP preprocessor, 80
- Snort rule IDs
  - ID 275, 117
  - ID 524, 116
  - ID 527, 116
  - ID 622, for ipEye scanner detection, 115
  - ID 1321, 117
  - ID 2281, 194, 198
- `--snort-sid` option, for fwsnort, 183
- Snort signatures, 74
  - ruleset availability, 174
  - shellcode.rules file in, 185
- snort2iptables shell script, 149*n*
- snort_rule_dl file, for psad, 97
- `SNORT_SID_STR` variable, in psad.conf file, 93, 196
- snortspoof.pl script (Perl), 280–282
- Snot tool, 167
- Song, Dug, 42
- source code, for projects, 5
- source IP address
  - in psad email alert, 109
  - specifying in Snort, 157
  - spoofing, 41
- source NAT (SNAT) target, 26

- source routing attempts, 118
- `--source` (`-s`) match, 12
- `SOURCE` variable, in /etc/fwknop/access.conf file, 238
- SPA (Single Packet Authorization). *See* Single Packet Authorization (SPA)
- spam, 118–119
- spoofed attack, monitoring by IDS, 214
- spoofed packets, 40
  - knock sequence busting with, 225
  - TCP ACK, 167
- SQL injection attacks, 76–77
- SQL Slammer worm, 61
  - visualizations to detect, 270–271
- SSL, Metasploit update use of, 207
- Stacheldraht DDoS agent, 44
- stack-based buffer overflows, 74
- starting psad, 85–86
- `--state ESTABLISHED` argument, 71
- `--state` match, 12
- stateful firewall
  - determining if port is filtered by, 58
  - iptables as, 167
- stateless attacks, against Snort, 167
- `STATUS_IP_THRESHOLD` variable, 126
- `STATUS_PORTS_THRESHOLD` variable, 127
- Stearns, William, 149*n*
- Stick tool, 167
- stopping psad, 85–86
- stream preprocessor, 167
  - stream4, 280
  - stream5, 283
- Strict Source Route option, detecting, 165
- `--string` match, 12
- string match expression, in iptables, 70
- Subversion source control system, 205
- SucKIT rootkit, 17
- Swatch utility, 145
- symmetric-key cipher, 243
- SYN/ACK packet in TCP handshake, 55
  - unsolicited, 56
- SYN cookies, 66
- SYN packet in TCP handshake, 55
- SYN scan response, 139–140
- *SysAdmin* magazine, 217
- syslog
  - configuration in psad, 88–89
  - fwknop server messages to, 249
  - hostname in psad email alert, 109
  - reporting in psad, 110–111
  - writing log data to, 35
- syslog-ng daemon, 88–89
- syslogd daemon, 88
- `SYSLOG_DAEMON` variable, in psad.conf file, 92

T

- tables in iptables, 11
- target-based intrusion detection, and network layer defragmentation, 151–152
- targets for iptables, 12
- TCP (Transmission Control Protocol), 49
  - ACK scans of ports, 58
  - building iptables rule applied to traffic, 157
  - `connect()` scan
    - detection with psad, 101–103
    - vs. SYN scan, 103
  - connection states, and fwsnort chains, 180–182
  - decoding options from iptables logs, 122–123
  - detecting attacks in connections, 133
  - flags, 197
  - header length, 165
  - idle scans, 59–60
  - logging headers, 50–51
  - port 0 traffic, 116
  - ports, psad display of scanned, 127
  - RST (Reset) packet, 62
    - and intrusion detection systems, 65
    - vs. RST/ACK packet, 63–65

sequence
inclusion in iptables, 51
prediction attacks, 61–62
SYN (half-open) scans, 56–57
detection with psad, 103–105
testing iptables policy, 29–31
three-way handshake, 55
for Tor transport, 254
translated Snort rule applied to traffic, 185
tcpdump, 4, 207
to capture SPA packet to file, 249
TCP/IP suite, as attack target, 100
tcpreplay, 249
`TCPSERV_PORT` variable, for fwknop, 237
tcpwrappers, 134
`TCPWRAPPERS_BLOCK_METHOD` variable, 136
technical references, 5
terminal interface, 14
testing, default iptables policy, 29–31
three-way handshake, 55, 167
thresholding response, in network layer, 45–46
timer, rules expiring based on, 143
timestamp, for fwknop server, 241
Time-to-Live (TTL). *See* TTL (Time-to-Live)
Tor anonymizing network, 198
SPA over, 254–255
TOS (Type Of Service) bits, Snort to inspect, 164
`tos` Snort option, 164
traceroute program, 42
traffic analysis, 254
Transmission Control Protocol (TCP). *See* TCP (Transmission Control Protocol)
transport layer, 49
abusing, 53–62
port scans, 53–60
port sweeps, 61
SYN floods, 62
TCP sequence prediction attacks, 61–62
attack definitions, 52–53
logging headers with iptables, 50–52
responses, 62–67
TCP, 62–66
for terminating connection, 62
UDP, 66–67
transport stack exploits, 53
Trin00 tool, 184–185
trust, exploiting, 77
trust relationships, and application layer attacks, 73
TTL (Time-to-Live)
concealing attack with targeted, 43
low values, 42
`TTL` field, SYN scan vs. `connect()` scan, 104
`ttl` Snort option, 163–164
Tumbler, 217
tumbler project, 232
Type-Length-Value (TLV) encoding, 122
Type Of Service (TOS) bits, Snort to inspect, 164

U

UDP (User Datagram Protocol), 49–50
checksum-crafting script, 220
header length, 165
ICMP for response, 66–67
iptables filtering against ports, 31–32
logging headers, 52
packet logging by iptables, 42
port scans, 60
psad display of scanned ports, 127
scans
detection with psad, 106–107
response, 140–141
spoofed attack, 283
ulog project, 157*n*
Unix filesystem directory structure, directory purpose, 85
`Unix::Syslog` Perl module, 233
unsolicited SYN/ACK packet, 56
`uricontent` Snort option, 160–161
URL-encoded data, decoding in real time, 80

US Advanced Encryption Standard, 221
User Datagram Protocol (UDP). *See* UDP (User Datagram Protocol)
user information, Ethernet sniffer for extracting, 79
username, for fwknop command execution, 241
/usr/bin/fwknop program, 233
/usr/bin/fwknop_serv, 233
/usr/lib/fwknop directory, 233
/usr/lib/fwsnort directory, 174
/usr/sbin/fwknopd daemon, 233
/usr/sbin/knopmd daemon, 233
/usr/sbin/knoptm daemon, 233
/usr/sbin/knopwatchd daemon, 233–234

V

/var/lib/psad/psadfifo named pipe, 103
/var/log/auth.log file, monitoring for authentication failure, 146
/var/log/messages file, 101
/var/log/psad directory, 124
/var/log/psad/scan_hash.pid file, 127
/var/run/psad/auto_ipt.sock Unix domain socket, 146
variables, in psad.conf file, 90. *See also individual variable names*
verbose/debug mode, in psad, 128–129
virtual circuit, 254
Vuln-dev mailing lists, 214
vulnerabilities in software, increase in discovery, 214

W

Ward, Brian, 13
Watkins, Peter, 81, 82
Watson, Paul A., 61
`WEB-PHP Setup.php access` attack, 194–198, 199–201
webserver, CGI applications as SQL injection attack target, 76
website for book, 5
whitelists, 133
  setup, 191
whois client
  database information in psad email alert, 109–110
  in psad, 89–90
Wikipedia, 194
wildcards, in Snort header, and variable resolution, 156
`WINDOW` field, SYN scan vs. `connect()` scan, 104
`window` Snort rule option, 158, 159
Windows Messenger pop-up spam, 118–119
Wireshark, 4, 220
`within` Snort option, 162
Witty worm of 2004, 132
worms, 61

X

X Windows interface, 14
XMAS scans
  detection with psad, 105–106
  of TCP ports, 58
Xprobe, 120

Z

Zalewski, Michal, 121
Zenoss, 152
zero TTL traffic, 117
zero-day attack problem, 214–216
zombie, 44
zombie host, 59