

Index

• Symbols •

- > (arrow) direction operator, 181
- <> (arrows) directionless operator, 181
- \ (backslash)
 - line continuation character, 143
 - normalization of, 208
- : (colon) rule port number separator, 183
- \$ (dollar sign)
 - Linux command prompt, 42
 - variable prefix, 179
- () (parentheses)
 - rule body delimiters, 184
 - syslog-ng driver argument delimiters, 248
- % (percent sign) URL escape character, 207
- | (pipe) or operator, 129
- # (pound sign)
 - comment prefix, 90
 - Linux command prompt, 42
- " " (quotation marks, double) rule value delimiters, 184
- ' ' (quotation marks, single) ADODB path delimiters, 149
- ;(semicolon)
 - ADODB line suffix, 149
 - MySQL command suffix, 99
 - Oinkmaster path separator, 267
 - PHP line prefix, 147
 - rule body option separator, 184
 - rule line suffix, 184
- / (slash)
 - CIDR notation component, 183
 - Unix directory prefix, 97

• A •

- ACID (Analysis Console for Intrusion Detection). *See also* reporting
- Access database support, 79
- ADODB requirement, 134, 135

- AG link, 162
- backing up, 273
- Barnyard ACID output, 296, 309–311
- browser, opening in, 161
- CD-ROM with this book, included on, 332
- configuration file, 157–159
- database management system, 173
- downloading, 136
- functionality overview, 134
- Graph Alert data page, 169–172
- IIS setup, 159–161
- installing, 156–157
- introduced, 16
- JpGraph requirement, 134
- main page, 163–169
- Maintenance page, 172–174
- MySQL setup, 151–153
- path, 156–157, 160
- permission, 160
- PHP dependency, 133, 134, 147, 160–161, 172
- version, 136
- Web server requirement, 133
- acid_conf.php file, 157–159
- ACID_DB Barnyard plug-in, 296, 309–311
- action plan, 213–214. *See also* incident response plan
- Address Resolution Protocol (ARP)
 - spoofing, 211, 278
- ADODB (Active Data Objects Data Base)
 - ACID ADODB requirement, 134, 135
 - CD-ROM with this book, included on, 333
 - downloading, 137
 - installing, 147–149
- adodb.inc.php file, 148, 149
- AIX support, 30
- alert
 - analyzing using SnortFW, 324
 - benign, 219
 - brute force attack alert, 220
 - classification.config file, 66, 92

alert (*continued*)

CSV output, 119–122, 296, 306–307

database, 222

DMZ alert, 24

DOS alert, 220

e-mailing, 255

facility, 109, 130, 179

fast, 112–113, 296, 304

file size, 80

firewall, triggering, 224

full, 113–114

HTML output, 296, 305–306

ID number, 166

IP address information, 164, 166–167,
168–169, 173–174

IP packet information, 223

ISystemActivator bind attempt alert,
221, 222, 225, 254

level, 92

management utility overview, 319–322

Meta information, 222–223

mode, 112–114, 128

monitoring, assigning responsibility
for, 219

monitoring using Swatch, 254

NETBIOS DCERPC alert, 221, 222,
223–224, 254

network scan, benign, 219

packet payload information, 168, 223, 224

partitioning for, 80–81

pcap output, 296, 308–309

ping alert, 109, 219

port information, 15, 164, 165

preprocessor evasion alert, 203

preprocessor reassembly alert, 205

priority, 15, 115–116

privilege escalation alert, 220

real-time, 219, 251

reporting alert information, 164–172, 173,
220–221, 222–226, 322–323

response utility overview, 323–325

rule alert action, 179, 181–182

shellcode detection alert, 220

sig_generator statement, 109

sig_id statement, 109

signature, 15–16, 166, 168

sig_revision statement, 109

snort.conf file

disable_evasion_alerts

keyword, 203

snort.conf file noalerts keyword, 205

socket, sending to, 128

switch overview, 128–129

syslog output, 114–117, 119, 296, 307–308

TCP information, 223

TFTP Get alert, 221, 224

timestamp, 165, 166, 306

tracing, 274

UDP information, 223

unfiltered Internet traffic, 24

unified, 132, 302

unsock, 128

alert_CSV

Barnyard plug-in, 296, 306–307

module, 119–122

alert_fast

Barnyard plug-in, 296, 304

module, 90, 112–113

alert_full module, 113–114

alert_fwsm module, 260

Alert_HTML Barnyard plug-in, 296, 305–306

alert_syslog

Barnyard plug-in, 296, 307–308

module, 68, 114–119, 282

alert_unified module, 132, 302

American Registry of Internet Numbers
(ARIN), 170

Analysis Console for Intrusion Detection.

See ACID

anomaly detection, 10

Apache HTTP Server Project Web site, 138

Apache HTTPD Server (on the CD), 333

Apache Software Foundation Web site

(www.apache.org), 136

Apache Web server

configuration file, 144

downloading, 136, 138

installing, 138–139

PHP setup, 143–145

run level, 144

- starting automatically, 144–145
- URL white space normalization, 208
- version, 138
- apachectl file, 144
- APNIC (Asia Pacific Network Information Center), 170
- application layer data, dumping, 103, 125
- arachNIDS signature database, 192, 214
- archive
 - MySQL table, 154, 156
 - rule archive, downloading, 266, 270
- ARIN (American Registry of Internet Numbers), 170
- ARP (Address Resolution Protocol)
 - spoofing, 211, 278
- arrow (>) direction operator, 181
- arrows (<>) directionless operator, 181
- ASCII
 - logging, 108, 122–126, 128, 130
 - rule content matching, 185
- Asia Pacific Network Information Center (APNIC), 170
- ASR Data Web site, 227
- ATTACK-RESPONSES log entry, 251, 254
- auditing, 9, 214–215
- Automake utility, 259
- Autopsy software, 227

• B •

- Back Orifice utility, 211, 278
- back-door.rules file, 186
- background service, running Snort as, 102–103, 111
- backslash (\)
 - line continuation character, 143
 - normalization of, 208
- backup
 - ACID, 273
 - Barnyard, 270, 273, 302
 - incident recovery, using in, 237
 - logging configuration, 272
 - rule, 195, 270
 - snort.conf file, 176–177, 270
 - updating Snort, before, 272–273

- BalaBit Web site, 244
- bandwidth, 24
- Barnyard utility (on the CD)
 - ACID output, 296, 309–311
 - alert_CSV output, 296, 306–307
 - alert_fast output, 296, 304
 - alert_HTML output, 296, 305–306
 - alert_syslog output, 307–308
 - background, running in, 315
 - backing up, 270, 273, 302
 - binary output, 296, 301–302
 - command line switches, 311–315
 - compiling, 300
 - configure command, 298
 - downloading, 297
 - enable command, 298
 - Ethernet setup, 303
 - flat text output, 296
 - gen-msg.map file, 301, 313
 - input, reading, 295, 312
 - installing, 300–301
 - Log_Dump output, 304–305
 - MySQL setup, 298–300
 - parsing, 296
 - pcap output, 296, 308–309
 - pid file output, 315
 - plug-in, 296, 304–309
 - Postgres support, 299–300
 - sid-msg.map file, 301, 313
 - snort.conf file setup, 301–302
 - snort-conf variable, 311
 - spool filename, 312
 - starting, 311–315
 - timestamp switches, 306, 312
 - unified output, 301–302, 310, 312–314
 - version, returning, 315
 - waldo file, 313, 314
 - with command, 299
- Baseline Security Analyzer, 83
- base-16 format, 185
- base64 string, 130
- BIOS password, 54
- black-hat hacker, 8
- Blaster.E worm, 226, 230–231, 232, 236, 237
- bo preprocessor, 211, 278

boot
 hard drive, restricting to, 81
 starting Snort at, 74–75
 starting `syslog-ng` at, 246
 bridge, 8
 brute force attack, 220
 BugTraq Vulnerability mailing list, 192, 214

• C •

`cat` Linux command, 56
 CDC (Cult of the Dead Cow), 211
 CD-ROM with this book, 331–336
 Center for Internet Security, 83
 CERT Web site, 180
 Chaotic Web site, 324
`chkconfig` Linux command, 44
`chown` utility, 69
`chroot` utility, 286
 CIDR (Classless Inter-Domain Routing)
 notation, 14, 183
 Cipherdyne Web site, 324
`classification.config` file, 66, 92
`.cnf` files, 97
 colon (:) rule port number separator, 183
 Comma Separated Values (CSV) alert
 output, 119–122, 296
 command line
 Barnyard, 311–315
 Snort, 94, 111, 177
 commenting code, 90, 99, 194, 212
 Common Vulnerabilities and Exposures
 (CVE) database, 192, 214, 222
 Comprehensive Perl Archive Network
 (CPAN), 253
 configure
 Barnyard command, 298
 script, 58, 65
 console, outputting log entry to,
 124, 129, 255
 cost
 hardware, 34
 Linux, 33
 MySQL, 79
 Snort, 13

CPAN (Comprehensive Perl Archive
 Network), 253
 cracker, 8
`create_mysql` file, 153
 CSV (Comma Separated Values) alert
 output, 119–122, 296
 Cult of the Dead Cow (CDC), 211
 CVE (Common Vulnerabilities and
 Exposures) database, 192, 214, 222
 Cygwin utility, 264, 267

• D •

daemon. *See also* background service,
 running Snort as
 introduced, 48
 MySQL, 60–61
 Snort, running as, 111, 122
 SSH, 48–54
`syslog`, 69, 119
`syslog-ng`, 247
 Danyliw, Roman (ACID developer), 136
 data spitter, 108
 database server, 27
 DDOS (Distributed Denial of Service)
 attack, 8, 220
`.deb` files, 47
 decoder, 14, 15, 68
`deleted.rules` file, 270
 Demarc PureSecure utility (on the CD),
 325–326, 332
 De-Militarized Zone (DMZ), 22–24, 279–280
 Denial of Service (DOS) attack, 8, 220, 251
 detection engine, 14–15
 direction operator, 181
 directionless operator, 181
 Distributed Denial of Service (DDOS)
 attack, 8, 220
 DMZ (De-Militarized Zone), 22–24, 279–280
 DNS (Domain Name Server), 67, 194
`dns.rules` file, 194
 dollar sign (\$)

- Linux command prompt, 42
- variable prefix, 179

 DOS (Denial of Service) attack, 8, 220, 251

downloading
ACID, 136
ADODB, 137
Apache Web server, 136, 138
Barnyard, 297
MySQL, 56, 95
Perl, 264
PHP, 136
rule archive, 266, 270
Snort source code, 63
Snort update, 13
SnortSam, 258
stunnel, 284
Swatch, 252
syslog-ng, 244
downtime, 32

• E •

echo Linux command, 58
e-mailing
alert, 255
log entry, 251
enable Barnyard command, 298
Encase software, 227
encryption
log output, 280
MD5 hash, 50, 58, 64, 85
PGP signature, 49, 58, 64
public key, 49
Engage Security Web site, 326
Ethernet
NIC, 39
OSI layer, 11
port, disabling upon attack, 227
tap, passive, 28
exploit.rules file, 213–214
expression, regular, 62–63, 192, 254, 255, 268
EXTERNAL_NET variable, 20, 67, 277

• F •

false negative, 9–10, 205
false positive, 9, 25, 212–215, 261

fault tolerance, 38
file
checking for odd, 234–236
integrity, verifying, 11, 85
modification time, using in tracing
attack, 237
monitoring using Swatch, 257
sharing, p2p, 279
FIN packet flag, 211
find Linux command, 234
firewall
alert, triggering firewall from, 224
IDS, using in conjunction with, 12
introduced, 12
iptables firewall, 258, 324
LAN, 278
rule, 324–325
SnortSam, using with, 258–259, 261–262
switch, placing between router and, 24
fragmentation, packet, 205
frag2 preprocessor, 205–206
FreeBSD support, 30
Freshmeat.net Web site, 322, 326, 329–330

• G •

GD library, 141–142
gen-msg.map file, 301, 313
GFI LANguard Security Event Log
Monitor, 230
GNU Automake utility, 259
GNU Privacy Guard Web site, 49
GNU Project Web site (www.gnu.org), 259
GNU Zip software, 137
GnuPG utility, 85
Google USENET newsgroup, 225
GPG (Gnu Privacy Guard) signature, 245
gpgv Linux command, 245
grant MySQL command, 152
graphing, 163, 169–172, 322–323
grep utility, 127
group setup, 64
Guardian utility (on the CD), 324–325, 334
Guidance Software Web site, 227

• H •

- hacker, 8
 - hard drive
 - boot, restricting to, 81
 - parity, 38
 - partitioning, 80–81
 - RAID, 38
 - reformatting after incident, 237
 - SCSI, 38
 - system requirement, 37–38
 - hardware requirement, 34–39, 77–78, 79–80
 - headless server, 27
 - Hexadecimal format, 168, 185
 - HIDS (host-based IDS), 10–11, 12, 21
 - home network logging, 128. *See also* LAN (Local Area Network)
 - HOME_NET variable, 20, 25, 67, 88–89, 277
 - host
 - multi-processor, 26, 36
 - single-processor, 26
 - host-based IDS (HIDS), 10–11, 12, 21
 - HP Tru64 support, 30
 - HTML (HyperText Markup Language) alert output, 296
 - HTTP (HyperText Transport Protocol), 11, 206–208
 - httpd.conf file, 144
 - http_decode preprocessor, 206
 - http_inspect preprocessor, 206–208
 - hub, 21–22
 - Hyper-Threading, 36
-
- I
 - IANA (Internet Assigned Numbers Authority), 223
 - IBM AIX support, 30
 - IDS (Intrusion Detection System), 9–12
 - IDSCenter utility (on the CD), 326, 331
 - ifconfig Linux command, 75
 - IIS (Internet Information Services)
 - ACID setup, 159–161
 - \ (backslash) normalization, 208
 - installing, 140
 - PHP setup, 145
 - securing, 83
 - version, 136
 - IIS Lockdown Tool, 83
 - incident response plan, 217–218, 238–239. *See also* action plan
 - index.php file, 144
 - info.rules file, 187
 - Insecure.org Web site, 212
 - inspection, stateful, 201
 - INSTALL Windows command, 103
 - installing ACID, 156–157
 - installing ADODB, 147–149
 - installing Apache Web server, 138–139
 - installing Barnyard, 300–301
 - installing IIS, 140
 - installing MySQL, 58–59, 95–97
 - installing PHP, 141, 145
 - installing Snort
 - binary package, 85–86
 - compiling, 65–66
 - component selection, 86
 - configuration file location, specifying, 64
 - group setup, 64
 - ld.so.conf file setup, 63
 - libpcap requirement, 61–62, 65
 - logging setup, 64, 85
 - MySQL support setup, 65
 - Oracle setup, 85
 - PCRE requirement, 62–63
 - service, as, 103
 - SQL Server setup, 85
 - tarball, opening, 65
 - testing installation, 73–74, 93–94, 273–274
 - upgrade, 272–274
 - user account setup, 64
 - WinPcap requirement, 84
 - International PGP Home Page Web site, 49
 - Internet Assigned Numbers Authority (IANA), 223
 - Internet Information Services. *See* IIS
 - Internet Ports Database, 223
 - Internet traffic, monitoring unfiltered, 24
 - Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX) support, 15
 - Intrusion Detection System (IDS), 9–12

IP (Internet Protocol) address
 alert IP address information, reporting,
 164, 166–167, 168–169, 173–174
 CIDR notation, 14, 183
 conversion mask, 128
 monitoring, 88, 182
 NAT, 22
 OSI layer, 11
 port information, 15
 registry, 170
 tracing, 169
 whitelist, 261–262
iptables firewall, 258, 324
IPX/SPX (Internetwork Packet Exchange
 /Sequenced Packet Exchange)
 support, 15

• J •

Jabber chat room, outputting
 log entry to, 250
JpGraph graph library (on the CD),
 134, 135, 137, 151, 159

• K •

kernel, 31
keystroke logger attack, 21
Kiwi Syslog Daemon, 119
Knoppix Linux Live CD, 228

• L •

LACNIC (Latin American and Caribbean
 Addresses Registry), 170
LAN (Local Area Network)
 firewall, 278
 monitoring, 25, 230, 277–279
 preprocessor, 278
 rule setup, 279
 sensor setup, 277–279
LANGuard Security Event Log Monitor, 230
Latin American and Caribbean Addresses
 Registry (LACNIC), 170
ldconfig Linux command, 58, 59

ld.so.conf file, 58, 63
libol library, 244–245
libpcap library (on the CD),
 26, 61–62, 65, 131
libpng library (on the CD), 141, 142
Linux
 advantages/disadvantages, 30, 34
 cat command, 56
 chkconfig command, 44
 chown utility, 69
 chroot utility, 286
 configure script, 58, 65
 cost, 33
 echo command, 58
 encryption, 49–50
 find command, 234
 gpgv command, 245
 grep utility, 127
 Hyper-Threading support, 36
 ifconfig command, 75
 initialization script, 43–44, 45,
 52–53, 74–75
 kernel, 31
 ldconfig command, 58, 59
 log, 228–229
 make command, 58, 143
 make install command, 58, 143
 memory requirement, 37
 mysqladmin program, 59
 netstat command, 42–43, 82, 236
 network status, checking, 42–43
 PAM, 52
 patching, 32
 PGP signature, 49, 58, 64
 port setup, 53
 process control, 43–46
 ps command, 231–232
 rule setup, 66, 67, 71
 runlevel command, 44
 script command, 52
 SSH daemon, 48–54
 sshd_config file, 53–54
 su command, 230
 sudo command, 230
 support, commercial, 33
 swap space, 36

Linux (*continued*)

- TCP/IP stack, 31
- touch command, 69
- update-rc.d command, 45–46
- Windows versus, 31–32
- Linux Live CD, 228
- Linux Security Web site, 225
- LinuxSecurity.com Web Site, 329
- Local Area Network. *See* LAN
- local.rules file, 118, 268
- log facility, 109–111, 129–130, 179
- Logcheck utility, 230
- Log_Dump Barnyard plug-in, 296, 304–305
- logging. *See also* alert; MySQL (on the CD)
 - analyzing log using Snortalog, 323
 - application-layer data, dumping,
 - 103, 125, 128
 - ASCII output, 108, 122–126, 128, 130
 - ATTACK-RESPONSES log entry, 251, 254
 - backing up logging configuration, 272
 - Barnyard Log_Dump output, 304–305
 - binary output, 126–127, 128, 130, 296, 301–302
 - compromise of system, reviewing log
 - after, 229–230
 - console output, 124, 129, 255
 - databases, to multiple, 281–282
 - default, 122–126
 - e-mailing log entry, 251
 - encryption, 280
 - existence of log file, checking, 69
 - fast, 131
 - filtering, 251
 - flat text output, 127, 129, 296
 - full, 131
 - HIDS, 11
 - home network, 128
 - installing Snort, setup during, 64, 85
 - IP address conversion mask, 128
 - Jabber chat room output, 250
 - link-layer data, 128
 - Linux log, 228–229
 - location of log file, 64, 111, 128
 - messages file, excluding log entry
 - from, 70
 - monitoring log using LANguard Security Event Log Monitor, 230
 - monitoring log using
 - Logcheck/Logsentry, 230
 - monitoring log using Logwatch, 230
 - monitoring log using Swatch, 252–257
 - monitoring log using syslog-ng, 244–252
 - NIDS, 10
 - Oracle output, 85
 - overhead, 34, 281
 - partitioning for, 80–81
 - password change, reviewing log for, 230
 - Perl script output, 250
 - ping, 126, 219
 - Postgres output, 129, 299–300
 - privilege escalation, reviewing log for, 230
 - reboot, reviewing log for, 230
 - remote, 116–117, 119, 230–231,
 - 248–249, 291
 - securing log file, 230–231, 283, 291
 - sensor setup, 276, 278–279
 - server, using centralized, 239, 249
 - service starting/stopping, reviewing
 - log for, 230
 - size of log file, 127
 - snap length, 129
 - snort.conf file output
 - database module, 70, 129–130, 282
 - snort.log file, 69, 111, 117
 - SnortSam, 261
 - sorting log file, 127
 - SQL Server output, 85
 - switch overview, 128–129
 - syslog output, 68–70, 114–119, 129,
 - 282, 307–308
 - tcpdump binary file output, 126–127, 128
 - timestamp, 127, 129, 312
 - tracing attack, using system log
 - file in, 237
 - unified, 131–132, 296, 301–302, 310,
 - 312–314
 - Unix log, 228–229
 - user change, reviewing log for, 229
 - verbosity, 93, 95, 111
 - waldo file, 313, 314

Windows Event Viewer, 229, 230–231
 year, including in log file, 129
 Logsentry utility, 230
 log_tcpdump module, 126–127
 Logwatch utility, 230

• M •

MAC (Media Access Control) address, 21
 MacOS X support, 30
 mailing list
 BugTraq Vulnerability, 192, 214
 snort-announce, 328
 Snort.org Web site, 63
 snort-sigs, 328
 snort-users, 328
 USENET newsgroup, 225
 make install Linux command, 58, 143
 make Linux command, 58, 143
 makefile.linux file, 142
 man-in-the-middle attack, 202
 McAfee Web site, 192, 225
 MD5 hash, 50, 58, 64, 85
 MD5Summer utility, 85
 Media Access Control (MAC) address, 21
 memory requirement, 36–37
 messages file, 70
 Microsoft Security Web site, 225
 MIDAS server, 325
 modular nature of Snort, 25
 MSDE (Microsoft Data Engine), 219
 mslaugh.exe file, 224, 225, 226, 232–233,
 236. *See also* Blaster.E worm
 MS-SQL worm, 15, 196, 220–221
 my.ini file, 97, 98–99, 101
 My-snort.org Web site, 329
 MySQL (on the CD)
 ACID setup, 151–153
 Admin console, 96, 98
 Admin traffic light, 97
 archive table, 154, 156
 background service, running as, 102–104
 Barnyard setup, 298–300
 binary distribution, 55, 56
 client, 71

command syntax, 99
 compiling, 57–59
 cost, 79
 daemon, 60–61
 database setup, 153–156
 downloading, 56, 95
 grant command, 152
 installing, 58–59, 95–97
 key_buffer setup, 98
 ld.so.conf file, 58
 login, 96–97
 MD5 hash, 58
 my.ini file, 97, 98–99, 101
 naming database, 91
 outputting to, 79, 90–92, 99–101, 279
 PASS variable, 97
 password, 59, 91, 97, 102, 152
 path, 151–152
 permission, 71, 101, 152–153
 PGP signature, 58
 port setup, 98
 root account, Linux environment, 57, 59
 root account, Windows environment,
 97, 99, 100, 102
 set password command, 102
 show databases command, 100
 Snort installation, setup during, 65
 snort table, 153–154, 156
 snort.conf file setup, 70–71
 SQLPath variable, 97
 starting/stopping, 60–61
 stunnel mysqls service, 288, 289, 290
 support, native, 79
 testing installation, 101
 user account, 56, 70, 101, 151–153
 USER variable, 97
 MySQL Web site, 56
 mysqladmin program, 59
 mysqld-nt.exe file, 101

• N •

NAT (Network Address Translation), 22
 negative, false, 9–10, 205
 Nessus utility, 192, 214–215

- network
 - cataloging, 212
 - disconnecting upon attack, 226–227
 - protocol, disabling unneeded, 82
 - protocol, rule support, 182
 - p2p, 279
 - scan, benign, 219
 - scanning for rogue computer, 212
 - service, checking for odd, 236–237
 - status, checking, 42–43
 - summary, 213
 - topology map, 212
 - trusted/untrusted, 39
 - wireless, 20
- Network Address Translation (NAT), 22
- network-based IDS (NIDS), 10, 19–25
- NIC (network interface card)
 - Ethernet NIC, 39
 - multiple NIC environment, 26–27, 38–39, 75
 - NIDS NIC, 10
 - OSI layer, 11
 - packet sniffing, dedicated, 39
 - promiscuous mode, 10, 11, 20
 - sensor NIC, 38–39
 - system requirement, 38–39
 - un-addressed, 27
- NIDS (network-based IDS), 10, 19–25
- Nikto utility, 261
- nmap utility, 109, 212
- Novell support, 15
- N-tier architecture, 27
- NULL packet flag, 211



- octet, 220
- Oinkmaster (on the CD), 263–271
- Open Systems Interconnection (OSI) Reference Model, 11
- OpenBSD support, 30
- OpenSSH utility (on the CD), 48, 49, 51–54
- OpenSSL library (on the CD), 51–52, 287
- OpenSSL Project Web site, 51
- Oracle log output, 85

- OS (operating system). *See also specific operating system*
 - access control, 81–82
 - choosing, 29–34, 78
 - kernel, 31
 - rebooting compromised system, 227
 - shutting down upon attack, 227
 - support, 13, 29–30
- OSI (Open Systems Interconnection) Reference Model, 11
- output
 - facility, 108
 - plug-in, 112
 - snort.conf file module, 27, 112, 260
- output database module, 70, 129–130, 282
- Output_pcap Barnyard plug-in, 296, 308–309



- packet
 - analysis, 14–15, 39
 - capture library, 14
 - decoder, 14, 15, 68
 - dropping, 17, 35, 79, 113
 - flag, 211
 - fragmentation, 205
 - Hexadecimal display, 168
 - IP information, 223
 - malformed, 201
 - payload, reporting, 168, 223, 224
 - reassembly by preprocessor, 204–205
 - scope, 201
 - stealth, 201
- PAM (Pluggable Authentication Module), 52
- parentheses ()
 - rule body delimiters, 184
 - syslog-ng driver argument delimiters, 248
- parity, 38
- partitioning hard drive, 80–81
- PASS variable, 97

- password
 - BIOS password, 54
 - log, reviewing for password change, 230
 - MySQL, 59, 91, 97, 102, 152
 - policy, 82
- PATH variable, 57
- pattern matching, 184–187, 206, 244.
 - See also* regular expression
- pcap library, 199, 296
- PCRE (Perl-Compatible Regular Expressions), 62–63
- peer-to-peer (p2p) network, 279
- PEM files, 287
- percent sign (%) URL escape character, 207
- Perl
 - CPAN, 253
 - downloading, 264
 - log entry, outputting to, 250
 - PCRE, 62–63
 - wget interpreter, 264
- Perl Monks Web site, 254
- perl.com Web site, 264
- Perl-Compatible Regular Expressions (PCRE), 62–63
- permission. *See also* privilege
 - ACID, 160
 - MySQL, 71, 101, 152–153
- PGP (Pretty Good Privacy) signature, 49, 58, 64, 245
- PHP scripting language (on the CD)
 - ACID dependency, 133, 134, 147, 160–161, 172
 - Apache setup, 143–145
 - downloading, 136
 - GD library, 141–142
 - IIS setup, 145
 - index.php file, 144
 - installing, 141, 145
 - location, 142, 145
- PHP Web site, 136
- PHPEveryWhere Web site (php.weblogs.com), 137
- php.exe file, 145
- php4ts.dll file, 147
- php.ini file, 146–147
- php.ini-dist file, 146
- PHPlot graph library (on the CD), 134, 135, 137, 150, 159
- physical security, 54, 81
- Pig Sentry script (on the CD), 321, 334
- ping
 - alert, 109, 219
 - logging, 126, 219
- pipe (|) or operator, 129
- .pkg files, 47
- planning
 - action plan, 213–214
 - incident response plan, 217–218, 238–239
 - sensor deployment, 276
- Pluggable Authentication Module (PAM), 52
- plug-in. *See also specific plug-in*
 - Barnyard, for, 296, 304–309
 - Nessus, for, 214
 - output plug-in, 112
 - preprocessor plug-in, 14, 201
 - support, 15
- port
 - alert port information, 15, 164, 165
 - Ethernet port, disabling upon attack, 227
 - IANA, 223
 - Internet Ports Database, 223
 - Linux port setup, 53
 - listening status, checking, 43, 236–237
 - monitoring port, 22, 23
 - MySQL setup, 98
 - OpenSSH daemon port, 53
 - preprocessing, restricting to specific, 205
 - RPC, 208–209
 - rule, applying to port number range, 183
 - scan detection, 109, 201, 203, 209–211
 - SPAN port, 22
 - stunnel setup, 290
- portmapper, 209
- positive, false, 9, 25, 212–215, 261
- Postgres log output, 129, 299–300
- post-processing, 296
- pound sign (#)
 - comment prefix, 99, 212
 - Linux command prompt, 42

- power plug, pulling upon attack, 227, 228
 - preprocessing
 - ARP spoofing detection, 211
 - ball sorting analogy, 200
 - bo preprocessor, 211, 278
 - decoder level, 201
 - evasion alert, 203
 - frag2 preprocessor, 205–206
 - http_decode preprocessor, 206
 - http_inspect preprocessor, 206–208
 - inspection, restricting stateful, 204
 - introduced, 14
 - LAN environment, 278
 - packet reassembly, 204–205
 - plug-in, 14, 201
 - port, restricting to specific, 205
 - portscanning detection, 203, 209–211
 - purpose, 200
 - rpc_decode preprocessor, 208–209
 - session reassembly, 204–205
 - session tracking, 200, 202, 204
 - snort.conf file preprocessor line, 203, 207, 210, 211
 - speed, effect on, 201–202
 - statistics, 204
 - stream4 preprocessor, 202–205, 279
 - TCP packet flow state analysis, 203
 - telnet_decode preprocessor, 208
 - testing preprocessor, 274
 - timeout, 204
 - traffic normalization, 122, 206–209
 - TTL, 203
 - Pretty Good Privacy (PGP) signature, 49, 58, 64, 245
 - privilege. *See also* permission
 - escalation, 220, 230
 - Oinkmaster, 265
 - process
 - killing, 43
 - reviewing for sign of attack, 231–233
 - processor
 - multi-processor system, 26, 36
 - single-processor system, 26
 - system requirement, 35–36
 - ps Linux command, 231–232
 - p2p (peer-to-peer) network, 279
 - PureSecure Professional utility (on the CD), 325–326, 332
- *Q* •
- quotation marks, double (" ") rule value delimiters, 184
 - quotation marks, single (' ') ADODB path delimiters, 149
- *R* •
- RAID (Redundant Array of Independent Disks), 38
 - RARLabs Web site, 137
 - RDBMS (Relational Database Management System), 78
 - reboot
 - compromise of system, upon, 227
 - log, reviewing for, 230
 - recovering from incident, 237–238
 - Redundant Array of Independent Disks (RAID), 38
 - reference.config file, 66, 93
 - reformatting hard drive after incident, 237
 - Regional Internet Registry (RIR), 170
 - regular expression, 62–63, 192, 254, 255, 268
 - Relational Database Management System (RDBMS), 78
 - Remote Procedure Call (RPC), 208–209
 - repeater. *See* hub
 - reporting
 - alert information, 164–172, 173, 220–221, 222–226, 322–323
 - destination information, 168
 - graphing, 163, 169–172, 322–323
 - IP address information, 164, 166–167, 168–169, 173–174
 - packet payload information, 168, 223, 224
 - port information, 164, 165
 - protocol information, 164, 166
 - sensor information, 164

- signature-based intrusion detection
 - compared, 175–176
 - source information, 168
- resource justification, 9
- RIPE (Reséaux IP Européens), 170
- RIR (Regional Internet Registry), 170
- Roesch, Marty (Snort creator), 13
- router, 24
- RPC (Remote Procedure Call), 208–209
- rpc_decode preprocessor, 208–209
- .rpm files, 47
- RRD-Snort utility, 322–323
- rservices.rules file, 213
- rule
 - activate action, 182
 - alert action, 179, 181–182
 - any keyword, 183
 - arachNIDS keyword, 192
 - archive, downloading, 266, 270
 - attempted-admin rule, 220, 221
 - attempted-dos rule, 220
 - attempted-recon rule, 219
 - attempted-user rule, 220
 - backdoor.rules rule, 279
 - backing up, 195, 270
 - bad-traffic rule, 279
 - body, 184–193
 - bugtraq keyword, 192
 - category overview, 178
 - chat.rules rule, 279
 - classtype keyword, 189–190
 - commenting out, 194, 212
 - content matching, 184–187, 206
 - creating, 195–197, 238
 - cve keyword, 192
 - deleted.rules file, 270
 - depth keyword, 186
 - destination argument, 179, 182–183
 - Destination Unreachable rule, 166
 - direction operator, 181
 - directionless operator, 181
 - DNS rule, 194
 - dynamic action, 182
 - editing, 176–177, 193–195
 - exploit rule, 279
 - firewall rule, 324–325
 - flow keyword, 180, 181, 192, 202
 - header, 181–183
 - icmp rule, 279
 - LAN environment, 279
 - Linux environment, 66, 67, 71
 - local.rules file, 118, 268
 - location, 66, 67
 - log action, 181
 - match information, 180
 - McAfee keyword, 192
 - mesg keyword, 191
 - Nessus keyword, 192
 - netbios.rules rule, 279
 - network protocol support, 182
 - nocase keyword, 187, 188
 - offset keyword, 187
 - pass action, 182
 - path, 89, 177, 266
 - port number range, applying to, 183
 - priority keyword, 188–189
 - production rule, 270
 - p2p.rules rule, 279
 - referencing external resource,
 - 180, 191–192, 222
 - removing unnecessary, 194, 212, 213
 - rev keyword, 191
 - shellcode-detect rule, 220
 - SID rule, 188, 269
 - snort.conf file rule section, 177
 - SnortSam setup, 261
 - source argument, 179, 182–183
 - string parser, 193
 - successful-admin rule, 220
 - suspicious-login rule, 220
 - syntax, 184
 - tcp keyword, 179
 - text matching, 183, 185, 187
 - updating, 13, 215, 265–266, 267–271,
 - 324–325
 - uricontent keyword, 180, 187–188
 - URL, referencing, 180, 191–192
 - variable, declaring, 179
 - Web site, referencing, 180, 191–192
 - WEB-MISC rule, 261

rule (*continued*)

wildcard, using, 183

Windows environment, 89, 93

RULE_PATH variable, 89, 177

runlevel Linux command, 44

• S •

SAM (Snort Alert Monitor), 320–321, 322

SamSpade Web site, 169

SANS Institute, 14, 83, 239, 328

scalability, 25, 27

script Linux command, 52

script-kiddie, 8

SCSI (Small Computer System Interface)

hard drive, 38

security auditing tool, 214–215

SecurityFocus Web site, 192, 214, 225, 329

semicolon (;)

ADODB line suffix, 149

MySQL command suffix, 99

Oinkmaster path separator, 267

PHP line prefix, 147

rule body option separator, 184

rule line suffix, 184

sensor

deploying multiple sensors, 27–28,
275–276

DMZ, deploying in, 279–280

hiding using passive Ethernet tap, 28

LAN setup, 277–279

location, 22–23, 25–28, 88, 277

logging setup, 276, 278–279

naming convention, 276

NIC, 38–39

numbering convention, 276

planning, 276

security, physical, 54, 81

testing, 274

SERVERS variable, 278

service

disabling unneeded, 43–46, 82, 212

MySQL, running as background service,
102–104

network service, checking for odd,
236–237

Snort, running as background service,
102–103

starting/stopping, reviewing log for, 230

SERVICE Windows command, 103

session

introduced, 200

preprocessing session reassembly,
204–205

preprocessing session tracking,
200, 202, 204

set password MySQL command, 102

shellcode.rules file, 213

show databases MySQL command, 100

shutting down upon attack, 227

SID (Snort IDentification), 180, 188, 269

sid-msg.map file, 301, 313

signature

alert signature, 15–16, 166

analysis, 199

arachNIDS signature database, 192, 214

GPG, 245

PGP, 49, 58, 64, 245

rule-based intrusion detection compared,
175–176

Slammer worm. *See* MS-SQL worm

slash (/)

CIDR notation component, 183

Unix directory prefix, 97

Slashdot Web site, 32

SleuthKit software, 227

Small Computer System Interface (SCSI)
hard drive, 38

SMART software, 227

SMS (Systems Management Server), 83

Sniffer mode, 93–94

S99Snort script, 74–75

Snort Alert Monitor (SAM), 320–321, 322

Snort IDentification (SID), 180, 188, 269

Snortalog utility (on the CD), 323, 334

snort-announce mailing list, 328

snort.conf file

alert keyword, 129–130

alert_csv module, 119–122

alert_fast module, 90, 112–113

alert_full module, 113–114

alert_fwsm module, 260

- alert_syslog module, 68, 114–119, 282
- alert_unified module, 132, 302
- apache_whitespace keyword, 208
- backing up, 176–177, 270
- Barnyard setup, 301–302
- both keyword, 205
- clientonly keyword, 205
- command line, overriding from, 111, 177
- commenting, 90
- config detection line, 68
- decoder setup, 68
- detect_scans keyword, 203
- detect_state_problems keyword, 203
- disable_evasion_alerts keyword, 203
- double_encode keyword, 207
- editing, 66, 176–177
- EXTERNAL_NET variable, 20, 67, 277
- HOME_NET variable, 20, 25, 67, 88–89, 277
- iis_backslash keyword, 208
- iis_unicode keyword, 207
- iis_unicode_map keyword, 207
- keepstats keyword, 204
- log keyword, 129
- log_flushed_streams keyword, 204
- MySQL setup, 70–71
- noalerts keyword, 205
- noinspect keyword, 204
- output database module,
 - 70, 129–130, 282
- output module, 27, 112, 260
- ports keyword, 205
- preprocessor line, 203, 207, 210, 211
- rule location, specifying, 67
- rule section, 177
- RULE_PATH variable, 89, 177
- serveronly keyword, 205
- SERVERS variable, 278
- Snortpath line, 86, 103
- timeout keyword, 204
- ttl_limit keyword, 203
- updating using Oinkmaster, 263, 268
- snort-conf variable, 311
- snort.exe file, 101
- SnortFW utility, 324
- snort.log file, 69, 111, 117
- Snort.org Web site
 - Barnyard download, 297
 - binary distribution download, 30, 85
 - mailing list, 63
 - Oinkmaster download, 264
 - overview, 327
 - passive Ethernet tap tutorial, 28
 - Snortalog download, 323
 - source code download, 63
 - update download, 13
- SnortSam utility (on the CD), 258–262
 - snort-sigs mailing list, 328
- SnortSnarf utility (on the CD), 319–320, 333
 - snort-users mailing list, 328
- Software Update Services (SUS), 83
- Solaris support, 30
- Sophos Web site, 225
- source code distribution, 29, 46–48, 63–65
- SourceForge.net Web site, 136
- SPAN port, 22
- spitter, data, 108
- SQL Server, logging to, 85
- SQLPath variable, 97
- SSH daemon, 48–54
- sshd_config file, 53–54
- state preservation, 201
- statefulness, 201
- stealth packet, 201
- stream4 preprocessor, 202–205, 279
- stunnel utility, 283–286, 288–293
- su Linux command, 230
- subnet, monitoring, 25, 26–27, 88, 277–279.
 - See also* LAN (Local Area Network)
- sudo Linux command, 230
- Sun Solaris support, 30
- SUS (Software Update Services), 83
- swap space, 36
- Swatch utility (on the CD), 230, 252–257
- switch, 21–22, 23, 24
- Symantec Web site, 225
- SYN packet flag, 211
- syslog facility, 68–70, 114–119, 129, 282, 307–308
- syslog-ng utility, 118–119, 244–252
- syslog2ng script, 246

system requirement, 34–39, 77–78, 79–80
Systems Management Server (SMS), 83

• T •

T flag, 177
tar software, 137, 264
tarball, 51, 65
Task Manager (Windows), 232–233
tcpdump utility, 13, 20, 107, 126–127, 128
tcpdump/libpcap Web site, 13
TCP/IP (Transmission Control Protocol/Internet Protocol)
 alert TCP information, 223
 header, outputting to screen, 93
 Linux TCP/IP stack, 31
 OSI layer, 11
 preprocessing, TCP packet flow state analysis in, 203
telnet_decode preprocessor, 208
Time To Live (TTL), 203
timestamp
 alert, 165, 166, 306
 Barnyard timestamp switches, 306, 312
 log, 127, 129, 312
touch Linux command, 69
tracing alert, 274
tracing attack
 file modification time, using in, 237
 IP address of attacker, 169
 system log file, using in, 237
Transmission Control Protocol/Internet Protocol. *See* TCP/IP
Trend Micro Web site, 225
Tru64 support, 30
TTL (Time To Live), 203

• U •

UDP (Universal Datagram Protocol)
 alert UDP information, 223
 OSI layer, 11
 syslog-ng source, taking UDP packet as, 247
Unicode character encoding, 207

Uniform Resource Identifier. *See* URI
Uniform Resource Locator. *See* URL
Universal Coordinated Time (UTC), 129
Unix log, 228–229
update-rc.d Linux command, 45–46
updating rule, 13, 215, 265–266, 267–271, 324–325
updating Snort
 downloading update, 13
 snort.conf file, 263, 268
 version, upgrading, 13, 272–274
URI (Uniform Resource Identifier)
 encoding, 207
 rule, restricting to, 180, 187–188
URL (Uniform Resource Locator)
 encoding, 206, 207
 normalization by preprocessor, 206, 207–208
 rule, referencing in, 180, 191–192
 white space normalization, 208
USENET newsgroup, 225
user account
 MySQL, 56, 70, 101, 151–153
 Snort, 64, 265
user change, reviewing log for, 229
USER variable, 97
UTC (Universal Coordinated Time), 129
UTF-8 character encoding, 207

• V •

Vorpal Media Web site, 330

• W •

waldo file, 313, 314
Web server, 133, 135. *See also* Apache Web server; IIS (Internet Information Services)
Web site, referencing in rule, 180, 191–192
webiis.rules file, 179
web-misc.rules file, 186
wget Perl interpreter, 264
Whitehats Web site, 192, 214, 225, 328
wildcard, using in rule, 183

Windows

- access control, 81–82
- advantages/disadvantages, 30, 33
- alert output setup, 90, 92
- component installation, limiting to
 - necessary, 82
- Event Viewer, 229, 230–231
- Hyper-Threading support, 36
- INSTALL command, 103
- Linux versus, 31–32
- monitoring setup, 87–89
- netstat command, 236
- network protocol, disabling unneeded, 82
- overhead considerations, 79–80
- packet dropping considerations, 79
- patching, 32, 83
- rule setup, 89, 93
- SERVICE command, 103
- syslog daemon, 119
- system requirement, 77–78, 79–80
- Task Manager, 232–233
- technical support considerations, 33
- updating, 83

- version, choosing appropriate, 78
- version support, 33

- winmysqladmin console, 98, 101

- WinPcap utility (on the CD), 84, 94

- WinRAR software, 137

- WINSNORT.com Web site, 329

- WinZip utility, 137, 336

- wireless network, 20

- with Barnyard command, 299

worm

- Blaster.E, 226, 230–231, 232, 236, 237

- introduced, 8

- MS-SQL, 15, 196, 220–221

- recovering from, 238

- removing, 238

• X •

- XMAS packet flag, 211

• Z •

- zlib utility (on the CD), 141–142

