
Index

A

- Access Control option, Microsoft Exchange, 214-216
- access databases
 - Postfix, 69-71
 - Sendmail, 65-66
- actions
 - McAfee SpamKiller configuration, 224-225
 - Procmail configuration, 24
- Active Spam Killer. *See* ASK274
- address blacklists, Lotus Notes, 240
- addresses
 - special purpose email addresses, 7
 - validation check, 4-5
- administrators, SpamAssassin
 - Bayesian parameters, 333-335
 - network checksum preferences, 338-339
 - rules and scoring, 344
 - settings, 57
- Advanced screen, POPFile configuration, 167
- aliases, DSPAM, 352
 - per-user, 352-353
 - system-wide, 352
- amavisd-new, installation, 37-40
- analysis, message headers, 297-302
- Analyze an Email screen, ASSP (Anti-Spam SMTP Proxy), 150
- ANONYMOUS method, SASL library, 81
- anti-spam
 - defenses, 12
 - mailbox servers, 13
 - MX (mail exchange servers), 12-13
 - quarantining, 13
 - sidelining, 13
 - methods
 - charging per email, 8
 - content filters, 5-6
 - Distributed Collaborative Filtering, 6-7
 - header checks, 4-5
 - reporting spam, 8
 - sender verification, 7
 - third-party solutions, 8-9
 - whitelists and blacklists, 4
- Anti-Spam SMTP Proxy (ASSP), 130, 144
 - installation, 146
 - mail client integration, 151

INDEX

- network setup screen, 147-148
 - screens, 149-150
 - training, 148-149
 - requirements, 145
 - Web site, 370
 - Apache
 - Camram installation, 263
 - Web site, 374
 - appliances, third-party anti-spam solutions, 9
 - architectures, anti-spam design, 10
 - email clients, 14
 - example configurations, 16-18
 - gathering data, 10
 - multi-tiered strategy, 12-13
 - policy development, 11-12
 - questioning people in organization, 10-11
 - rules, 14-15
 - area tested, SpamAssassin default ruleset, 305-306
 - ASK274 (Active Spam Killer), 259
 - configuration, 275-276
 - installation, 274-275
 - MTA integration, 277
 - Postfix integration, 276
 - Procmail integration, 277
 - qmail integration, 276
 - queue management, 277-278
 - Sendmail integration, 276
 - ASSP (Anti-Spam SMTP Proxy), 130, 144
 - installation, 146
 - mail client integration, 151
 - network setup screen, 147-148
 - screens, 149-150
 - training, 148-149
 - requirements, 145
 - attacks, joe job, 295
 - authentication, 79-81
 - SMTP AUTH/STARTTLS method
 - Cyrus SASL, 82-84
 - MTAs, 81
 - Postfix, 86-89
 - qmail, 90-92
 - Sendmail, 84-86
- B**
- Bayes Rule, 118-21
 - bayes+net value, SpamAssassin Default Scores
 - Assigned, 307
 - Bayes, Thomas, 118-121
 - Bayesian analysis, 6, 13, 29
 - ASSP (Anti-Spam SMTP Proxy), 144-151
 - bogofilter, 138-144
 - CRM114, 131-138
 - DSPAM. *See* DSPAM
 - POPFile. *See* POPFile
 - selection, 129-130
 - Bayesian classifier, 13
 - Bayesian filtering, 117-118
 - advanced statistics, 125-127
 - attack efficiency, 123-124
 - available packages, 124-125
 - Bayes Rule, 118-121
 - Mozilla Messenger, 168-170
 - token scheme, 125
 - training, 123
 - words, 121-123
 - Bayesian parameters, SpamAssassin, 331
 - administrator only, 333-335
 - user settable, 331-332
 - Bernstein, Dan, qmail Web site, 366
 - Blackhole Listing Service, 12
 - native MTAs, 61-62
 - Postfix, 71-75
 - Sendmail, 67-68
 - SpamAssassin, 29
 - blacklist.mfp file, 138
 - blacklists, 3-5
 - CRM114 installation, 137-138

- Lotus Domino, DNS, 232-233
 - Lotus Notes, 240
 - McAfee SpamKiller configuration, 225
 - Microsoft Outlook, 186
 - anti-spam settings, 188
 - configuration, 187-188
 - Microsoft Outlook Express, 183-184
 - Procmail configuration, 26-27
 - SpamAssassin, 29, 50, 329-331
 - commands, 311-312
 - BlameYokohama, CRM114, 131
 - Block List Service (BLS), 206
 - Blocked Senders screen, Microsoft Outlook, 188
 - BLS (Block List Service), 206
 - body analysis, SpamAssassin, 29
 - body value, SpamAssassin area tested ruleset, 305
 - bogofilter, 13, 138-139
 - Bayesian analyzer, 130
 - components, 139-140
 - configuration, 138-139
 - installation, 138
 - three-folder system mail classification example, 140-144
 - training, 140
 - Web site, 130, 370
 - bogofilter.cf file, 138
 - bogoutil program, 139
 - Buckets screen, POPFile configuration, 161-163
- C**
- c flags, Procmail configuration, 24
 - Camram, 259-260
 - configuration, 265
 - camram.local file, 266-267
 - configuration file, 265-266
 - cron jobs, 268
 - user set up, 269
 - inbound messages, 261
 - installation, 262-263
 - Apache, 263
 - Procmail integration, 264-265
 - Sendmail integration, 263-264
 - message classification, 269-270
 - preferences, 270
 - recovery, 273
 - Spamtrap, 272
 - outbound messages, 261
 - Web site, 372
 - camram.local file, Camram configuration, 266-267
 - CAUCE Web site, 374
 - certificates, SMTP AUTH/STARTTLS method
 - Domino. *See* Domino
 - Exchange. *See* Exchange
 - Postfix, 88
 - qmail, 91
 - Sendmail, 85
 - challenge/response system, sender verification, 7, 259
 - checksums, Distributed Collaborative Filtering, 6-7
 - Cipertrust Ironmail Web site, 9, 363
 - CLI (command line interface), 45
 - DSPAM utilities, 354
 - mail clients, 2
 - TMDA (Tagged Message Delivery Agent) configuration, 283
 - SpamAssassin, 45
 - running via Procmail, 46
 - running via qmail, 46
 - sa-learn, 46
 - client plugins, anti-spam support, 14
 - Cloudmark, 14

INDEX

- command line interface. *See* CLI
- commands
 - SpamAssassin
 - sa-learn program, 318-320
 - spamassassin command, 309-312
 - spamc program, 316-318
 - spamd program, 312-316
 - Vipul's Razor, 96
 - razor-admin, 100-101
 - razor-agent.conf, 97-100
 - razor-check, 101-102
 - razor-report, 102
 - razor-revoke, 102
- commands (Outlook), Tools menu, Rules and Alerts, 188
- companies. *See* enterprises
- conditional probability, Bayes Rule, 118-121
- conditions, Procmail configuration, 24
- configuration file, Camram configuration, 265-266
- Configuration screen, POPFile configuration, 164
- configurations
 - ASK (Active Spam Killer), 275-276
 - bogofilter, 138-139
 - Camram, 265
 - camram.local file, 266-267
 - configuration file, 265-266
 - cron jobs, 268
 - user set up, 269
 - DCC (Distributed Checksum Clearinghouse)
 - basic mode setup, 109
 - dcc_conf, 109-110
 - default, 108
 - file maintenance, 111
 - ids, 110
 - map.txt, 110
 - startup script, 111
 - whitelists, 110
- IMF (Intelligent Message Filter), 200-201
 - activate filtering, 202
 - Gateway Blocking Configuration, 201
 - Store Junk E-mail Configuration, 201-202
- McAfee SpamKiller, 222-224
 - actions, 224-225
 - blacklists, 225
 - disabled rules, 225
 - Lotus Domino, 241-250
 - Microsoft Exchange, 222-225
 - whitelists, 225
- POPFile, 159-160
 - Advanced screen, 167
 - Buckets screen, 161-163
 - Configuration screen, 164
 - History screen, 160-161
 - Magnets screen, 163-164
 - Security screen, 165-166
- Postfix, 40-41
- Procmail, 23
 - action, 24
 - blacklisting and filtering, 26-27
 - conditions, 24
 - example, 25
 - option flags, 24
- SpamAssassin, 321-322
 - Bayesian-related parameters, 331-335
 - blacklists, 329-331
 - CLI (command line interface), 45-46
 - files, 48-57
 - language, 327-329
 - message tagging, 324-327
 - network checksum facilities, 335-339
 - privileged settings, 322

- scoring, 323-324, 339-344
 - tags, 344-345
 - version-related keywords, 323
 - whitelists, 329-331
 - TMDA (Tagged Message Delivery Agent), 279
 - CLI mail client, 283
 - files, 279
 - non-CLI mail client, 284-285
 - Postfix, 281-282
 - qmail, 280
 - Sendmail, 282-283
 - Vipul's Razor, 102-103
 - Configure Anti-Spam Settings screen, McAfee SpamKiller configuration, 243-245
 - Configure Update Schedule screen, McAfee SpamKiller configuration, 245
 - Connection Control option, Microsoft Exchange, 216-217
 - connection controls, Lotus Domino, 233
 - Connection Filtering pane, Microsoft Exchange, 205-206
 - BLS (Block List Service) defining, 206
 - Global Accept/Deny lists, 207
 - content filters, 5-6
 - contrib program, 140
 - CPAN Web site, 374
 - CRAM-MD5 method, SASL library, 81
 - crm file, 131
 - CRM114, 13, 123, 131
 - Bayesian analyzer, 130
 - installation, 131
 - blacklists, 137-138
 - building .css file, 135-136
 - checking .css file, 136
 - .css file setup, 134-135
 - mailfilter configuration, 132-134
 - predefined .css file, 135
 - source code, 132
 - training filter, 137
 - whitelists, 137-138
 - Web site, 130
 - cron jobs
 - Camram configuration, 268
 - DCC file maintenance, 111
 - DSPAM, 353
 - .css file, CRM114 installation
 - building, 135
 - building from spam archives, 135-136
 - checking with utilities, 136
 - predefined, 135
 - setup, 134-135
 - cssdiff command, 136
 - cssdiff file, 131
 - cssmerge file, 131
 - cssutil command, 136
 - cssutil file, 131
 - Cyrus SASL, 81
 - SMTP AUTH/STATTLS method, 82
 - configuring, 83-84
 - installation, 82
- ## D
- databases, DSPAM cron job, 353
 - db_dump program, 139
 - db_recover program, 139
 - db_verify program, 139
 - DCC (Distributed Checksum Clearinghouse), 105
 - advanced setup, 112-113
 - firewalls, 115
 - flooding, 114
 - gray lists, 114-115
 - local DCC server, 113
 - ports, 115

INDEX

- basics, 105, 106
- configuration
 - basic mode setup, 109
 - dcc_conf, 109-110
 - file default, 108
 - file maintenance, 111
 - ids, 110
 - map.txt, 110
 - startup script, 111
 - whitelists, 110
- installation, 106-108
- Procmail, 111-112
- SpamAssassin, 335
 - administrator, 338-339
 - user preferences, 335-338
- dcc_conf file, 108-110
- dcc_conf.in file, DCC configuration, 108
- dccproc command, 111-112
- DCF (Distributed Checksum Filtering), 6-7, 93-94
 - checks, 12
 - DCC (Distributed Checksum Clearinghouse), 105
 - advanced setup, 112-115
 - basics, 105-106
 - configuration, 108-111
 - installation, 106-108
 - Procmail, 111-112
 - SpamAssassin, 29
 - Vipul's Razor, 95
 - commands, 96-103
 - installation, 95-96
 - using, 103-104
 - Declude's blacklist listing Web site, 62, 365
 - Default Scores Assigned, SpamAssassin default ruleset, 306-307
 - Dekand, Lin, 370
 - description of tests, SpamAssassin default ruleset, 306
 - designs, anti-spam architecture, 10
 - email clients, 14
 - example configurations, 16-18
 - gathering data, 10
 - multi-tiered strategy, 12-13
 - policy development, 11-12
 - questioning people in organization, 10-11
 - rules, 14-15
 - devices, third-party anti-spam solutions, 9
 - DIGEST-MD5 method, SASL library, 81
 - disabled rules, McAfee SpamKiller
 - configuration, 225
 - Distributed Checksum Clearinghouse.
 - See DCC
 - Distributed Checksum Filtering. See DCF
 - DNS
 - blacklist filters, Lotus Domino, 232-233
 - check reversal, 63
 - checks, 5
 - lookups, enabling Microsoft Exchange, 213
 - DNS TXT record, SPF (Sender Policy Framework), 288
 - DNSstuff, 303
 - Domino, 230
 - anti-spam architecture rules, 15
 - inbound SMTP connections
 - connection controls, 233
 - DNS blacklist filters, 232-233
 - recipient controls, 234-235
 - relay controls, 231
 - relay enforcement, 232
 - sender controls, 234
 - McAfee SpamKiller, 240-241
 - configuration, 241-250
 - installation, 241
 - SMTP AUTH support, 251
 - STARTTLS support, 252-254

- rules, 235-237
 - starting, 230
 - Web site, 371
- DSPAM, 347-348
- installation, 349-350
 - alias setup, 352-353
 - Apache setup, 351-352
 - command line utilities, 354
 - database purge cron job, 353
 - dspam_clean cron job, 353
 - GUI (Graphical User Interface), 355-356, 359-361
 - notifications, 353-354
 - post tasks, 350-351
 - troubleshooting, 362
 - integration planning, 349
 - sidelining versus tagging, 348-349
 - dspam_clean cron job, DSPAM, 353
- E**
- e flags, Procmail configuration, 24
 - email
 - basic terminology, 2
 - headers
 - analyzing, 297-302
 - Microsoft Outlook, 297
 - Microsoft Outlook Express, 297
 - Mozilla Messenger, 296-297
 - tools, 302-304
 - email clients
 - anti-spam architecture, 14
 - content filters, 6
 - filters, 153-154
 - Microsoft Outlook, 185-194
 - Microsoft Outlook Express, 179-184
 - Mozilla Messenger, 168-178
 - POPFile, 155-168
 - Lotus Notes, 238
 - address blacklists, 240
 - subject line filtering, 238-239
 - E-mail Rules tab, Microsoft Outlook, 188
 - EmailRelay Web site, 372
 - enterprises, anti-spam architectures, 10
 - email clients, 14
 - example configurations, 16-18
 - gathering data, 10
 - multi-tiered strategy, 12-13
 - policy development, 11-12
 - questioning people in organization, 10-11
 - rules, 14-15
 - /etc/passwd, Cyrus SASL authentication method, 82
 - Exchange, 197-199
 - anti-spam architecture rules, 15
 - IMF (Intelligent Message Filter), 199
 - configuration, 200-202
 - installation, 199-200
 - maintenance, 203-205
 - incoming message filtering, 205
 - activating, 211-212
 - connection filtering, 205-207
 - logs, 212-213
 - recipient filtering, 210
 - sender filtering, 208-210
 - main screen, 198
 - McAfee SpamKiller, 218-219
 - anti-spam configuration, 222-225
 - installation, 220
 - running, 220-222
 - settings, 225-226
 - outbound messages, 213-214
 - Access Control option, 214-216
 - Connection Control option, 216-217

INDEX

Relay Restrictions option, 218
 Secure Communications option, 216
 System Manager window, 199

F

f flags, Procmail configurations, 24
 false negatives, 3
 false positives, 3
 file configurations, SpamAssassin, 48-57
 filter by header
 Microsoft Outlook, 191-193
 Mozilla Messenger, 175-177
 filter by subject
 Lotus Notes, 238-239
 Microsoft Outlook, 188-190
 Mozilla Messenger, 174
 filtering, Procmail configuration, 26-27
 filters
 Bayesian, 117-118
 advanced statistics, 125-127
 analyzer selection, 129-130
 ASSP (Anti-Spam SMTP Proxy), 144-151
 attack efficiency, 123-124
 available packages, 124-125
 Bayes Rule, 118-121
 bogofilter, 138-144
 CRM114, 131-138
 DSPAM. *See* DSPAM
 token scheme, 125
 training, 123
 word analysis, 121-122
 word selection, 122-123
 content, 5-6
 DCF (Distributed Collaborative Filtering),
 checks, 6-7, 12, 93-94
 DCC (Distributed Checksum Clearing-
 house), 105-115

Vipul's Razor, 95-104
 email clients, 153-154
 Microsoft Outlook, 185-194
 Microsoft Outlook Express, 179-184
 Mozilla Messenger, 168-178
 POPFile, 155-168
 IMF (Intelligent Message Filter), 199
 configuration, 200-202
 installation, 199-200
 maintenance, 203-205
 incoming messages, Microsoft Exchange,
 205-213
 outbound messages, Microsoft Exchange,
 213-218
 static
 native MTAs, 60
 Postfix, 68-71
 Sendmail, access database, 65-66
 firewalls, DCC (Distributed Checksum
 Clearinghouse), 115
 Fishers method, Bayesian filtering, 127
 flags, Procmail configuration, 24
 flod file, DCC configuration, 108
 flooding, DCC (Distributed Checksum
 Clearinghouse), 114
 .forward files, Procmail invoking, 21
 From addresses, validation check, 4-5
 full value, SpamAssassin area tested
 ruleset, 305
 Fullmer, Jon, Web site, 369

G

Gateway Blocking Configuration, IMF
 (Intelligent Message Filter), 201
 Global Accept/Deny lists, Microsoft
 Exchange, 207
 global keywords, SpamAssassin configuration
 language, 51

- learning, 52
 - miscellaneous, 53
 - network tests, 52
 - scoring, 50
 - tagging, 51
 - whitelist and blacklist, 50
 - GNU Web site, 373
 - Graham, Paul
 - Bayesian filtering, 117
 - Web site, 369
 - grey lists, DCC (Distributed Checksum Clearinghouse), 105, 114-115
 - grey_flod file, DCC configuration, 108
 - grey_whitelist file, DCC configuration, 108
 - GSSAPI method, SASL library, 81
- ## H
- Hashcash Web site, 372
 - header-based filters
 - Microsoft Outlook, 191-193
 - Mozilla Messenger, 175-177
 - headers
 - analyzing, 29, 297-302
 - checks, anti-spam methods, 4-5
 - Microsoft Outlook, 297
 - Microsoft Outlook Express, 297
 - Mozilla Messenger, 296-297
 - tools, 302
 - DNSstuff, 303
 - SamSpade, 302
 - SpamCop, 303-304
 - value, SpamAssassin area tested ruleset, 306
 - heuristics, 13
 - History screen, POPFile configuration, 160-161
- ## I
- IDENT (identification protocol),
 - SpamAssassin commands, 315
 - ids file, 108-110
 - IETF Web site, 363
 - IMF (Intelligent Message Filter), 197-199
 - configuration, 200-201
 - installation, 199-200
 - maintenance
 - performance monitor data, 204-205
 - UceArchive folder, 203-204
 - incoming messages, 2-3
 - Camram, 261
 - Microsoft Exchange filtering, 205
 - activating, 211-212
 - connection filtering, 205-207
 - logs, 212-213
 - recipient filtering, 210
 - sender filtering, 208-210
 - SMTP connections, Lotus Domino, 231-235
 - installation
 - amavisd-new, 37-40
 - ASK (Active Spam Killer), 274-275
 - ASSP (Anti-Spam SMTP Proxy), 146
 - mail client integration, 151
 - network setup screen, 147-148
 - screens, 149-150
 - training, 148-149
 - bogofilter, 138
 - Camram, 262-263
 - Apache, 263
 - Procmail integration, 264-265
 - Sendmail integration, 263-264
 - CRM114, 131
 - blacklists, 137-138
 - building .css file, 135
 - building .css file from spam archives, 135-136

INDEX

- checking .css file, 136
- .css file setup, 134-135
- mailfilter configuration, 132-134
- predefined .css file, 135
- source code, 132
- training filter, 137
- whitelists, 137-138

DCC (Distributed Checksum Clearinghouse), 106-108

DSPAM, 349-350

- alias setup, 352-353
- Apache setup, 351-352
- command line utilities, 354
- database purge cron job, 353
- dspam_clean cron job, 353
- GUI (Graphical User Interface), 355-356, 359-361
- notifications, 353-354
- post tasks, 350-351
- troubleshooting, 362

IMF (Intelligent Message Filter), 199-200

McAfee SpamKiller, 220, 241

milter, 34

MIMEDefang, 34-36

POPFile, 155-158

Procmail, 20

Python, 260

qmail, SMTP AUTH/STARTTLS method, 90-91

SpamAssassin, 32-33

- Postfix, 36-41
- qmail, 41-44
- Sendmail, 33-36

TMDA (Tagged Message Delivery Agent), 279

Vipul's Razor, 95-96

Intelligent Message Filter. *See* IMF

Internet Mail Consortium Web site, 374

J

- joe job attacks, 295
- Junk E-Mail Filter, Microsoft Outlook, 185-188

K

- K9, 185
- kerberos, Cyrus SASL authentication method, 82
- KERBEROS_V4 method, SASL library, 81
- keywords, SpamAssassin configuration
 - language, 51
 - learning, 52
 - miscellaneous, 53
 - network tests, 52
 - scoring, 50
 - tagging, 51
 - whitelist and blacklist, 50

L

- languages, SpamAssassin, 51, 327-329
- large enterprises, anti-spam example architecture, 17-18
- learning keywords, SpamAssassin, 52
- local value, SpamAssassin Default Scores Assigned, 306
- locale, SpamAssassin default ruleset, 306
- LOGIN method, SASL library, 81
- logs, Microsoft Exchange filters, 212-213
- Lotus Domino, 230
 - anti-spam architecture rules, 15
 - inbound SMTP connections
 - connection controls, 233
 - DNS blacklist filters, 232-233
 - recipient controls, 234-235
 - relay controls, 231
 - relay enforcement, 232
 - sender controls, 234

- McAfee SpamKiller, 240-241
 - configuration, 241-250
 - installation, 241
 - SMTP AUTH support, 251
 - STARTTLS support, 252-254
 - rules, 235-237
 - starting, 230
 - Web site, 371
- Lotus Notes, 238
- address blacklists, 240
 - subject line filtering, 238-239
 - Web site, 371
- ## M
- Mackey, Jeff, 62
- Magnets screen, POPFile configuration, 163-164
- mail
- clients2 integration, ASSP (Anti-Spam SMTP Proxy), 151
 - delivery agents (MDAs), 2
 - mail.local default, 19
 - Procmail, 19-27
 - exchange services (MX), anti-spam architecture, 12-13
- MAIL FROM field, 60
- mail transfer agents. *See* MTAs
- mail.local, MDA default, 19
- Mail-Abuse Web site, 365
- mailbox servers, anti-spam architecture, 13
- maildrop, SpamAssassin integration with qmail, 42
- mailfilter file, CRM114 installation, 132-134
- maintenance, IMF (Intelligent Message Filter)
 - performance monitor data, 204-205
 - UceArchive folder, 203-204
- make-dcc_conf file, DCC configuration, 108
- manual whitelisting/blacklisting, SpamAssassin, 29
- map.txt file, 108-110
- McAfee Security Web site, 371
- McAfee SpamKiller
 - Lotus Domino, 240-241
 - configuration, 241-250
 - installation, 241
 - SMTP AUTH support, 251
 - STARTTLS support, 252-254
- Microsoft Exchange, 218-219
 - anti-spam configuration, 222-225
 - installation, 220
 - running, 220-222
 - settings, 225-226
- MDAs (mail delivery agents), 2
 - mail.local default, 19
 - Procmail, 19-20
 - configuration, 23-27
 - installation, 20
 - invoking, 21-23
- medium enterprises, anti-spam example architectures, 17-18
- message filters
 - Lotus Notes, 238-239
 - Microsoft Outlook, 188-193
 - Mozilla Messenger, 171
 - actions on flagged messages, 174
 - header-based filters, 175-177
 - message selection, 173
 - perform actions, 177
 - running filters, 178
 - subject-based filters, 174
- messages
 - classification, Camram, 269-270
 - preferences, 270
 - recovery, 273
 - Spamtrap, 272
- headers
 - analyzing, 297-302

INDEX

- DSPAM, 348-349
- Microsoft Outlook, 297
- Microsoft Outlook Express, 297
- Mozilla Messenger, 296-297
- tools, 302-304
- inbound
 - Camram, 261
 - Microsoft Exchange filters, 205-213
 - SMTP connections, 231-235
 - versus outbound, 2-3
- misclassifications, 3
- non-spam, SpamAssassin operation, 48
- outbound
 - Camram, 261
 - Microsoft Exchange filters, 213-218
 - versus inbound, 2-3
- scoring, SpamAssassin, 44
- spam, SpamAssassin operation, 47-48
- tagging, SpamAssassin, 324-327
- methods, defeating spam
 - charging per email, 8
 - content filters, 5-6
 - Distributed Collaborative Filtering, 6-7
 - header checks, 4-5
 - reporting spam, 8
 - sender verification, 7
 - third-party solutions, 8-9
 - whitelists and blacklists, 3-4
- mewdecode program, 133
- Microsoft Exchange, 197-199
 - anti-spam architecture rules, 15
 - IMF (Intelligent Message Filter), 199
 - configuration, 200-202
 - installation, 199-200
 - maintenance, 203-205
 - incoming message filtering, 205
 - activating, 211-212
 - connection filtering, 205-207
 - logs, 212- 213
 - recipient filtering, 210
 - sender filtering, 208-210
- main screen, 198
- McAfee SpamKiller, 218-219
 - anti-spam configuration, 222-225
 - installation, 220
 - running, 220-222
 - settings, 225-226
- outbound messages, 213-214
 - Access Control option, 214-216
 - Connection Control option, 216-217
 - Relay Restrictions option, 218
 - Secure Communications option, 216
- System Manager window, 199
- Microsoft Outlook, 153
 - anti-spam support, 14
 - filters, 185
 - activation, 194
 - filter by header, 191-193
 - filter by subject, 188-190
 - Junk E-Mail Filter, 185-188
 - viewing message headers, 297
- Microsoft Outlook Express, 153
 - filters
 - blacklists, 183-184
 - process, 179-183
 - viewing message headers, 297
- Microsoft SmartScreen Technology, Junk E-Mail filter, 185-188
- Microsoft Web site, 200, 370
- Milter
 - DCC (Distributed Checksum Clearinghouse), 106
 - installation, 34
 - Web site, 365

- mime_decoder variable, 133
 - MIMEDefang installation, 34-36
 - mimedefang-filter file, 36
 - mimencode program, 133
 - Mirapoint, 9, 363
 - miscellaneous keywords, SpamAssassin, 53
 - misclassified messages, 3
 - mobile users, authentication, 79-92
 - Mozilla Messenger, 153
 - embedded anti-spam support, 14
 - filters, 168
 - Bayesian, 168-170
 - messages, 171-178
 - viewing message headers, 296-297
 - Web site, 370
 - MTAs (mail transfer agents), 2, 59-63, 93
 - ASK (Active Spam Killer) integration, 277
 - blackhole listing services, 61-62
 - DNS check reversal, 63
 - Microsoft Exchange, 197
 - Postfix, 68-78
 - Procmail invocation, 22
 - Postfix, 22-23
 - qmail, 23
 - Sendmail, 22
 - qmail, 78
 - Sendmail, 64-76
 - SMTP AUTH/STATTLS method, 81
 - SMTP command elimination, 63
 - SpamAssassin integration, 31-32
 - static filters, 60
 - strict protocol adherence, 63
 - whitelists and blacklists, 3-5
 - multi-tiered anti-spam strategies, 12-13
 - Mutt Web site, 374
 - MX (mail exchange servers), anti-spam architecture, 12-13
 - MySQL-related parameters, SpamAssassin, 334-335
- N**
- Network Associates Web site, 363
 - network testing, SpamAssassin, 52, 335-339
 - New Mail Rule panel, Microsoft Outlook Express filters, 179
 - non-CLI mail client, TMDA (Tagged Message Delivery Agent) configuration, 284-285
 - non-spam messages, SpamAssassin operation verification, 48
 - Notes, 238
 - address blacklists, 240
 - subject line filtering, 238-239
 - Web site, 371
 - notifications, DSPAM, 353-354
- O**
- organizations, anti-spam architectures, 10
 - email clients, 14
 - example configurations, 16-18
 - gathering data, 10
 - multi-tiered strategy, 12-13
 - policy development, 11-12
 - questioning people in organization, 10-11
 - rules, 14-15
 - OTP method, SASL library, 81
 - outbound messages, 2-3
 - Camram, 261
 - Microsoft Exchange filtering, 213-214
 - Access Control option, 214-216
 - Connection Control option, 216-217
 - Relay Restrictions option, 218
 - Secure Communications option, 216
 - Outclass, 185
 - Outlook, 153
 - anti-spam support, 14
 - filters, 185
 - activation, 194

INDEX

- filter by header, 191-193
 - filter by subject, 188-190
 - Junk E-Mail Filter, 185-188
 - viewing message headers, 297
- Outlook Express, 153
 - filters
 - blacklists, 183-184
 - process, 179-183
 - viewing message headers, 297
- P**
- PAM (pluggable authentication method),
 - Cyrus SASL authentication method, 82
- Pantel, Patrick, 370
- parameters, Bayesian, SpamAssassin, 331-335
- performance monitor, IMF (Intelligent Message Filter), 204-205
- Perl modules, 42, 95
- PLAIN method, SASL library, 81
- pluggable authentication method (PAM),
 - Cyrus SASL, 82
- plugins, IMF (Intelligent Message Filter),
 - 197-199
 - configuration, 200-202
 - installation, 199-200
 - maintenance, 203-205
- policies, anti-spam architecture development,
 - 11-12
- POP/IMAP-before-SMTP method, remote
 - user authentication, 79-80
- POPFile, 13-14, 153
 - filters, 155
 - configuration, 159-167
 - installation, 155-158
 - operation, 168
- POPFile Classification Bucket Creation
 - screen, 157
- POPFile Client Configuration screen, 158
- POPFile Installation Options page, 156
- POPFile Setup Wizard, 158
- ports, DCC (Distributed Checksum Clearinghouse), 115
- Postfix
 - ASK (Active Spam Killer) integration, 276
 - native MTAs
 - blackhole listing, 74-75
 - blackhole listing services, 71-72
 - configuration, 77-78
 - configuration files, 68
 - email address blocking, 74
 - IP address blocking, 73-74
 - static filter setup, 68-71
 - Procmail invocation, 22-23
 - SMTP AUTH/STARTTLS method, 86
 - certificates, 88
 - installation and configuration, 86-88
 - starting and testing, 88-89
 - SpamAssassin, 36-37
 - amavisd-new installation, 37-40
 - configuring, 40-41
 - TMDA (Tagged Message Delivery Agent)
 - configuration, 281-282
 - Web site, 68, 366
- Postini, 8-9, 364
- preferences, Camram message
 - classification, 270
- priolist.mfp file, 137
- privileges, SpamAssassin
 - configuration files, 54-57
 - rules and scoring, 340-344
- Procmail, 19-20
 - ASK (Active Spam Killer) integration, 277
 - Camram integration, 264-265
 - configuration, 23
 - action, 24
 - blacklisting and filtering, 26-27

- conditions, 24
 - example, 25
 - option flags, 24
 - DCC (Distributed Checksum Clearinghouse), 106, 111-112
 - installation, 20
 - invoking, 21-23
 - running SpamAssassin, 46
 - Web site, 364
 - procmailer man page, Procmail option flags, 24
 - protocols, strict adherence, 63
 - Python
 - installation, 260
 - Web site, 372
 - Pyzor, SpamAssassin, 335
 - administrator, 338- 339
 - user preferences, 335-338
- Q**
- qmail
 - ASK (Active Spam Killer) integration, 276
 - native MTAs, configuration, 78
 - Procmail invocation, 23
 - running SpamAssassin, 46
 - SMTP AUTH/STARTTLS method, 90
 - certificates, 91
 - functionality, 81
 - installation, 90-91
 - testing, 92
 - SpamAssassin, 41-44
 - TMDA (Tagged Message Delivery Agent) configuration, 280
 - Web site, 367
 - .qmail files, Procmail invoking, 21
 - .qmail-default files, 21
 - qmail-queue patch, SpamAssassin integration with qmail, 42
 - Qmail-Scanner, SpamAssassin integration with qmail, 42-43
 - quarantining, 3, 13
- R**
- rawbody value, SpamAssassin area tested ruleset, 306
 - Razor. *See* Vipul's Razor
 - razor-admin command, Vipul's Razor, 100-101
 - razor-agent.conf configuration file, Vipul's Razor, 97-100
 - razor-check command, Vipul's Razor, 101-102
 - razor-report command, Vipul's Razor, 102
 - razor-revoke command, Vipul's Razor, 102
 - rblsmtpd command, qmail blocking, 72
 - Recipient Filtering screen, Microsoft Exchange, 210
 - recipients
 - filtering, Microsoft Exchange, 210
 - Lotus Domino, controls, 234-235
 - recovery, Camram message classification, 273
 - registering, Vipul's Razor, 104
 - rejection messages, SPF (Sender Policy Framework), 292-293
 - relay controls, Lotus Domino, 231
 - relay enforcement, Lotus Domino, 232
 - Relay Restrictions option, Microsoft Exchange, 218
 - remote users, authentication, 79-92
 - reporting
 - spam, 8, 295-296
 - SpamAssassin, commands, 312
 - Vipul's Razor, 104
 - resources, 363-374
 - rewrites.mfp file, 133
 - Robinson, Gary, 125, 370
 - rules
 - anti-spam architecture, 14-15

INDEX

- Lotus Domino, 235-237
 - SpamAssassin, 305
 - administrators, 344
 - area tested, 305-306
 - Default Scores Assigned, 306-307
 - description of test, 306
 - locale, 306
 - privileged, 340-344
 - samples, 307-308
 - scoring, 44
 - test name, 306
 - user preferences, 339
 - Rules and Alerts command (Tools menu - Outlook), 188
- S**
- Safe Recipients tab, Microsoft Outlook, 188
 - Safe Senders screen, Microsoft Outlook, 188
 - sa-learn program, 45-46, 318-320
 - sample-spam.txt file, 48
 - SamSpade, 302-303, 373
 - SASL (Simple Authentication and Security Layer), 80-81
 - sasldb, Cyrus SASL authentication method, 82
 - saspasswd command, 82
 - scoring, 13
 - keywords, SpamAssassin, 50
 - messages, SpamAssassin, 44
 - SpamAssassin, 323-324
 - administrators, 344
 - privileged, 340-344
 - user preferences, 339
 - screens, ASSP (Anti-Spam SMTP Proxy), 149-150
 - Secure Communications option, Microsoft Exchange, 216
 - secure SMTP, remote user authentication, 79-80
 - Security Sage Web site, 368
 - Security screen, POPFile configuration, 165-166
 - See the maillog Tail screen, ASSP (Anti-Spam SMTP Proxy), 150
 - Select Server screen, McAfee SpamKiller configuration, 250
 - sender compute model, sender verification, 7
 - Sender Filtering tab, Microsoft Exchange, 208-210
 - Sender Policy Framework (SPF), 5, 287
 - basics, 287-288
 - enforcing records, 291
 - rejection message, 292-293
 - Sendmail spf-milter installation, 291-292
 - publishing records, 288
 - Web site, 372
 - senders
 - filtering, Microsoft Exchange filters, 208-210
 - Lotus Domino, controls, 234
 - verification, 7, 257-260
 - ASK (Active Spam Killer), 274-278
 - Camram, 260-273
 - challenge/response system,, 7 259
 - installing Python, 260
 - sender compute setup, 7, 258-259
 - special purpose email addresses, 7
 - TMDA (Tagged Message Delivery Agent), 278-285
 - Sendmail
 - ASK (Active Spam Killer) integration, 276
 - Camram integration, 263-264
 - DCC (Distributed Checksum Clearinghouse), 107
 - native spam controls
 - access database, 65-66
 - blackhole listing services, 67-68

- configuration, 76
- configuration files, 64
- Procmail invocation, 22
- SMTP AUTH/STARTTLS method, 84
 - certificates, 85
 - installation and configuration, 84-85
 - starting and testing, 85-86
- SpamAssassin, 33-36
- SpamAssassinMIMEdefang installation, 34-36
- TMDA (Tagged Message Delivery Agent)
 - configuration, 282-283
- Web site, 64, 368-369
- services, third-party anti-spam solutions, 8-9
- settings, McAfee SpamKiller, 225-226
- Seymour, Jim, Web site, 366
- sidelining, 3
 - anti-spam architectures, 13
 - DSPAM versus tagging, 348-349
- signatures, DCF, 93-94
 - DCC (Distributed Checksum Clearinghouse), 105-115
 - Vipul's Razor, 95-104
- Sill, Dave, Life with qmail Web site, 366
- Simple Authentication and Security Layer (SASL), 80-81
- Slamming Spam Web site, 363
- small enterprises, anti-spam example
 - architectures, 16-17
- SMTP, command elimination, 63
- SMTP connections, Lotus Domino, 231-235
- SMTP AUTH method
 - Cyrus SASL, 82
 - configuring, 83-84
 - installation, 82
 - McAfee SpamKiller, Lotus Domino, 251
 - MTAs, 81
 - Postfix, 86
 - certificates, 88
 - installation and configuration, 86-88
 - starting and testing, 88-89
- qmail, 90
 - certificates, 91
 - installation, 90-91
 - testing, 92
- remote user authentication, 79-80
- Sendmail, 84
 - certificates, 85
 - installation and configuration, 84-85
 - starting and testing, 85-86
- SMTPS, remote user authentication, 79-80
- SORBS blacklisting service, 61
- spam reporting, 295-296
- Spam Bouncer Web site, 364
- SpamAssassin, 13, 29-31
 - administrator settings, 57
 - commands
 - sa-learn program, 318-320
 - spamassassin command, 309-312
 - spamc program, 316-318
 - spamd program, 312-316
 - configuration, 44-46
 - configuration files, 321-322
 - Bayesian-related parameters, 331-335
 - blacklists, 329-331
 - keywords, 50-53
 - language, 327-329
 - location, 48-49
 - message tagging, 324-327
 - network checksum facilities, 335-339
 - precedence, 49
 - privilege parameters, 54-57
 - privileged settings, 322
 - scoring, 323-324
 - scoring rules, 339-344
 - tags, 344, 345

INDEX

- version-related keywords, 323
- whitelists, 329-331
- default ruleset, 305
 - area tested, 305-306
 - Default Scores Assigned, 306-307
 - description of test, 306
 - locale, 306
 - samples, 307-308
 - test name, 306
- installation, 32-33
 - Postfix, 36-41
 - qmail, 41-44
 - Sendmail, 33-36
- MTA integration, 31-32
- operation verification, 47-48
- scoring messages, 44
- Web site, 305, 321, 364
- spamassassin command, 44-45, 309
 - blacklists, 311-312
 - configuration file, 310-311
 - general, 310
 - reporting, 312
 - whitelists, 311-312
- spamc program, 45, 316-318
- SpamCop
 - blacklisting service, 61
 - header analysis, 303-304
 - Web site, 8, 303, 365
- spamd program, 45, 312
 - access control, 315
 - configuration file, 313
 - general, 312-313
 - IDENT (identification protocol), 315
 - MySQL, 314
 - SpamAssassin privilege settings, 322
 - SSL connections, 314
 - syslog facility, 314
 - user processing, 315-316
 - virtual users, 313-314
- Spamhaus
 - blacklisting service, 61
 - Web site, 366
- Spamihilator Web site, 185, 371
- SpamKiller, 9
 - Lotus Domino, 240-241
 - configuration, 241-250
 - installation, 241
 - SMTP AUTH support, 251
 - STARTTLS support, 252-254
 - Microsoft Exchange, 218-219
 - anti-spam configuration, 222-225
 - installation, 220
 - running, 220-222
 - settings, 225-226
- SpamLinks Web site, 62, 366, 374
- Spamtrap, Camram message classification, 272
- special purpose email addresses, 7
- SPF (Sender Policy Framework), 5, 287
 - basics, 287-288
 - enforcing records, 291
 - rejection message, 292-293
 - Sendmail spf-milter installation, 291-292
 - publishing records, 288
 - Web site, 372
- spf-milter, installation, 291-292
- Start From a Blank Rule option, Microsoft Outlook, 191
- STARTTLS method
 - Cyrus SASL, 82
 - configuring, 83-84
 - installation, 82
 - McAfee SpamKiller, Lotus Domino, 252-254
- MTAs, 81
- Postfix, 86
 - certificates, 88

- installation and configuration, 86-88
 - starting and testing, 88-89
 - qmail, 90
 - certificates, 91
 - installation, 90-91
 - testing, 92
 - remote user authentication, 79-80
 - Sendmail, 84
 - certificates, 85
 - installation and configuration, 84-85
 - starting and testing, 85-86
 - static filters
 - native MTAs, 60
 - Postfix, 68-71
 - Sendmail, access database, 65-66
 - static lists, 12
 - Static Whitelist/Blacklist, 12
 - Statistics screen, ASSP (Anti-Spam SMTP Proxy), 149
 - Stop Spam Web site, 373
 - Store Junk E-mail Configuration, IMF (Intelligent Message Filter), 201-202
 - Stunnel Web site, 368
 - subject-based filters
 - Lotus Notes, 238-239
 - Microsoft Outlook, 188-190
 - Mozilla Messenger, 174
 - Symantec Brightmail, 8-9
 - System Manager window, Microsoft Exchange, 199
- T**
- Tagged Message Delivery Agent. *See* TMDA
 - tagging
 - DSPAM versus sidelining, 348-349
 - messages, 324-327
 - SpamAssassin, 51
 - tags, SpamAssassin, 344-345
 - tcpserver command
 - qmail blocking, 72
 - rules file, 73
 - techniques, defeating spam
 - charging per email, 8
 - content filters, 5-6
 - Distributed Collaborative Filtering, 6-7
 - header checks, 4-5
 - reporting spam, 8
 - sender verification, 7
 - third-party solutions, 8-9
 - whitelists and blacklists, 3-4
 - test name, SpamAssassin default ruleset, 306
 - testing
 - SMTP AUTH/STARTTLS method
 - Postfix, 88-89
 - qmail, 92
 - Sendmail, 85-86
 - SpamAssassin installation, 47-48
 - third-party anti-spam solutions
 - appliances, 9
 - services, 8-9
 - TMDA (Tagged Message Delivery Agent), 259, 278
 - configuration, 279
 - CLI mail client, 283
 - files, 279
 - non-CLI mail client, 284-285
 - Postfix, 281-282
 - qmail, 280
 - Sendmail, 282-283
 - installation, 279
 - Web site, 372
 - tokens, Bayesian filtering, 125
 - tools, header analysis, 302
 - DNSstuff, 303
 - SamSpade, 302
 - SpamCop, 303-304

INDEX

Tools menu commands (Outlook), Rules and Alerts, 188

training

Bayesian filtering, 123

filters

ASSP (Anti-Spam SMTP Proxy),
148-149

bogofilter, 140

CRM114 installation, 137

DSPAM. *See* DSPAM

POPFile. *See* POPFile

troubleshooting, DSPAM, 362

U

UceArchive folder, IMF (Intelligent Message Filter), 203-204

unlearn command, training filters, 137

unprivileged keywords, SpamAssassin configuration

language, 51

learning, 52

miscellaneous, 53

network tests, 52

scoring, 50

tagging, 51

whitelist and blacklist, 50

Update/Verify the Whitelist or Redlist screen, ASSP (Anti-Spam SMTP Proxy), 150

uri value, SpamAssassin area tested ruleset, 306

users

Camram configuration, 269

remote, authentication, 79-92

SpamAssassin

Bayesian parameters, 331-332

network checksum preferences, 335-338

rules and scoring, 339

V

verification

senders, 7, 257-260

ASK (Active Spam Killer), 274-278

Camram, 260-273

challenge/response system, 7, 259

installing Python, 260

sender compute model, 7, 258-259

special purpose email addresses, 7

TMDA (Tagged Message Delivery Agent), 278-285

SpamAssassin operation, 47

non-spam message test, 48

spam message test, 47-48

View Anti-spam Rules List screen, McAfee SpamKiller configuration, 248-249

View Quarantined Mail screen, McAfee SpamKiller configuration, 247-248

View Repository Database screen, McAfee SpamKiller configuration, 249-250

View Scanning History screen, McAfee SpamKiller configuration, 246

View Scanning Information screen, McAfee SpamKiller configuration, 243

Vipul's Razor, 95

commands, 96

razor-admin, 100-101

razor-agent.conf, 97-100

razor-check, 101-102

razor-report, 102

razor-revoke, 102

default configuration files, 102-103

installation, 95-96

signature, 14

SpamAssassin, 335

administrator, 338-339

user preferences, 335-338

using, 103-104

Web site, 369
whitelists, 103
VR. *See* Vipul's Razor

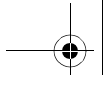
W

w flags, Procmail configuration, 24

Web sites

Active Spam Killer, 372
Anti-Spam Server Proxy, 370
Apache, 374
Bernstein, Dan, 366
bogofilter, 130, 370
Camram, 372
CAUCE, 374
Cipetrust Ironmail, 363
CPAN, 374
CRM114, 130
Declude's blocklist listing, 62, 365
DNSstuff, 303
EmailRelay, 372
Fullmer, Jon, 369
GNU, 373
Graham, Paul, 369
Hashcash, 372
IETF, 363
Internet Mail Consortium, 374
Life with qmail, 366
Lotus, 371
Mackey, Jeff, 62
Mail-Abuse, 365
McAfee Security, 371
Microsoft, 200, 370
Milter, 365
Mirapoint, 363
Mozilla, 370
Mutt, 374
Network Associates, 363
Postfix, 68, 366

Postini, 364
Procmail, 364
Python, 372
qmail, 367
SamSpade, 303, 373
Security Sage, 368
Sendmail, 64, 368-369
Seymour, Jim, 366
Slamming Spam, 363
SORBS, 61
Spam Bouncer, 364
SpamAssassin, 305, 321, 364
SpamCop, 8, 61, 303, 365
Spamhaus, 61, 366
Spamihilator, 185, 371
SpamLinks, 62, 374
SPF, 372
Stop Spam, 373
Stunnel, 368
TMDA, 372
Vipul's Razor, 369
web-based tools, DNSstuff, 303
whiteclnt file, 108-110
whitecommon file, 108-110
whitelist.mfp file, 138
whitelists, 3-5
 CRM114 installation, 137-138
 DCC (Distributed Checksum
 Clearinghouse), 110
 file, 108-110
 McAfee SpamKiller configuration, 225
 Microsoft Outlook, 186
 anti-spam settings, 188
 configuration, 187-188
 SpamAssassin, 29, 50, 311-312, 329-331
 Vipul's Razor, 103
with bayes value, SpamAssassin Default Scores
 Assigned, 306



INDEX

words, Bayesian filtering
analysis, 121-122
selection, 122-123

X-Y-Z

Yerazunis, Bill, Bayesian filtering, 121

