



## Symbols & Numerics

---

/usr/nr/etc/hosts file entries, 714–715

- 1000 Bad Option List signatures, 248
- 1000 Series signatures. *See* IP signatures
- 10000 Series policy-violation signatures, 378, 388
- 1001 IP Options-Record Packet Route signatures, 248
- 1002 IP Options-Timestamp signatures, 248
- 1003 IP Options-Provide s, c, h, tcc signatures, 249
- 1004 IP Options-Loose Source Route signatures, 249
- 1005 IP Options-SATNET ID signatures, 250
- 1006 IP Options-Strict Source Route, 250
- 1100 IP Fragment Attack signatures, 252
- 1101 Unknown IP Protocol signatures, 256
- 1102 Impossible IP Packet signatures, 257
- 1103 IP Fragments Overlap signatures, 252
- 1104 IP Localhost Source Spoof signatures, 257
- 1200 IP Fragmentation Buffer List signatures, 252
- 1201 IP Fragment Overlap signatures, 253
- 1202 IP Fragment Overrun-Datagram Too Long signatures, 253
- 1203 IP Fragment Overwrite-Data Is Overwritten signatures, 254
- 1204 IP Fragment Missing Initial Fragment signatures, 254
- 1205 IP Fragment Too Many Datagrams, 254
- 1206 IP Fragment Too Small signatures, 255
- 1207 IP Fragment Too Many Frags signatures, 255
- 1208 IP Fragment Incomplete Datagram signatures, 255
- 1220 Jolt2 Fragment Reassembly DoS Attack signatures, 256
- 2000 ICMP Echo Reply signatures, 258
- 2000 Series ICMP signatures. *See* ICMP signatures
- 2001 ICMP Host Unreachable signatures, 262
- 2002 ICMP Source Quench signatures, 263
- 2003 ICMP Redirect signatures, 263
- 2004 ICMP Echo Request signatures, 259
- 2005 ICMP Time Exceeded for a Datagram signatures, 264
- 2006 ICMP Parameter Problem on a Datagram signatures, 264
- 2007 ICMP Timestamp Request signatures, 259
- 2008 ICMP Timestamp Reply signatures, 260
- 2009 ICMP Information Request signatures, 260
- 2010 ICMP Information Reply signatures, 261
- 2011 ICMP Address Mask Request signatures, 261
- 2012 ICMP Address Mask Reply signatures, 261
- 2100 ICMP Network Sweep with Echo signatures, 265
- 2101 FTP RETR passwd signature, 376
- 2101 ICMP Network Sweep with Timestamp signatures, 265
- 2102 ICMP Network Sweep with Address Mask signatures, 266
- 2150 Fragmented ICMP Packet signatures, 266
- 2151 Large ICMP Packet signatures, 267
- 2152 ICMP Flood signatures, 267
- 2153 ICMP Smurf Attack signatures, 268
- 2154 Ping of Death Attack signatures, 268
- 2301 Telnet IFS=/ signature, 376
- 2302 Telnet /etc/shadow signatures, 377
- 2303 Telnet + + signatures, 377
- 3000 Series TCP signatures. *See* TCP signatures
- 3001 TCP Port Sweep signatures, 272
- 3002 TCP SYN Port Sweep signatures, 272
- 3003 Fragmented TCP SYN Port Sweep signatures, 273
- 3005 TCP FIN Port Sweep signatures, 273
- 3006 Fragmented TCP FIN Port Sweep signatures, 273
- 3010 TCP High Port Sweep signatures, 274
- 3011 TCP FIN High Port Sweep signatures, 275
- 3012 Fragmented TCP FIN High Port Sweep signatures, 275
- 3015 TCP Null Port Sweep signatures, 275
- 3016 Fragmented TCP Null Port Sweep signatures, 276
- 3020 TCP SYN-FIN Port Sweep signatures, 276
- 3021 Fragmented TCP SYN-FIN Port Sweep signatures, 277
- 3030 TCP SYN Host Sweep signatures, 278
- 3031 Fragmented TCP SYN Host Sweep signatures, 278
- 3032 TCP FIN Host Sweep signatures, 279

- 3033 Fragmented TCP FIN Host Sweep signatures, 279
- 3034 TCP NULL Host Sweep signatures, 279
- 3035 Fragmented TCP NULL Host Sweep signatures, 280
- 3037 Fragmented TCP SYN-FIN Host Sweep signatures, 280
- 3038 Fragmented NULL TCP Packet signatures, 281
- 3039 Fragmented Orphaned FIN Packet signatures, 282
- 3040 NULL TCP Packet signatures, 282
- 3041 SYN/FIN Packet signatures, 283
- 3042 Orphaned FIN Packet signatures, 283
- 3043 Fragmented SYN/FIN Packet signatures, 283
- 3045 Queso Sweep signatures, 277
- 3050 Half-Open SYN Attack signatures, 308
- 3100 Small Attack signatures, 284
- 3101 Sendmail Invalid Recipient signatures, 285
- 3102 Sendmail Invalid Sender signatures, 285
- 3103 Sendmail Reconnaissance signatures, 285
- 3104 Archaic Sendmail Attacks signatures, 286
- 3105 Sendmail Decode Alias signatures, 286
- 3106 Sendmail SPAM Attack signatures, 286
- 3107 Majordomo Exec Bug signatures, 287
- 3108 MIME Overflow Bug signatures, 287
- 3109 Qmail Length Crash signatures, 288
- 3150 FTP Remote Command Execution signatures, 288
- 3151 FTP SYST Command Attempt signatures, 289
- 3152 FTP CWD ~root Command signatures, 289
- 3153 FTP Improper Address Specified signatures, 289
- 3154 FTP Improper Port Specified signatures, 290
- 3155 FTP RETR Pipe Filename Command Execution signatures, 290
- 3156 FTP STOR Pipe Filename Command Execution signatures, 290
- 3157 FTP PASV Port Spoof signatures, 291
- 3200 WWW Phf Attack signatures, 292
- 3201 WWW General cgi-bin Attack signatures, 292
- 3202 WWW .url File Request signatures, 293
- 3203 WWW .lnk File Requested signatures, 293
- 3204 WWW .bat File Requested signatures, 294
- 3205 HTML File Has .url Link signatures, 294
- 3206 HTML File Has .lnk Link signatures, 294
- 3207 HTML File Has .bat Link signatures, 295
- 3208 WWW campas Attack signatures, 295
- 3209 WWW Glimpse Server Attack signatures, 295
- 3210 WWW IIS View Source Attack signatures, 296
- 3211 WWW IIS Hex View Source Attack signatures, 296
- 3212 WWW NPH-TEST-CGI Attack signatures, 296
- 3213 WWW TEST-CGI Attack signatures, 297
- 3214 IIS DOT DOT VIEW Attack signatures, 297
- 3215 IIS DOT DOT EXECUTE Bug signatures, 297
- 3216 IIS Dot Dot Crash Attack signatures, 298
- 3217 WWW php View File Attack signatures, 298
- 3218 WWW SGI Wrap Attack signatures, 298
- 3219 WWW PHP Buffer Overflow signatures, 299
- 3220 IIS Long URL Crash Bug signatures, 299
- 3221 WWW cgi-viewsource Attack signatures, 299
- 3222 WWW PHP Log Scripts Read Attack signatures, 299
- 3223 WWW IRIX cgi-handler Attack signatures, 300
- 3224 HTTP WebGais signatures, 300
- 3225 HTTP Gais Websendmail signatures, 300
- 3226 WWW Webdist Bug signatures, 301
- 3227 WWW Htmlscript Bug signatures, 301
- 3228 WWW Performer Bug signatures, 301
- 3229 Website Win-C Sample Buffer Overflow signatures, 301
- 3230 Website Uploader signatures, 302
- 3231 Novell Convert Bug signatures, 302
- 3232 Finger Attempt signatures, 302
- 3233 WWW count-cgi Overflow signatures, 303
- 3250 TCP Hijacking signatures, 308
- 3251 TCP Hijacking Simplex Mode signatures, 308
- 3300 NETBIOS OOB Data signatures, 303
- 3301 NETBIOS Stat signatures, 304
- 3302 NETBIOS Session Setup Failure signatures, 304
- 3303 Windows Guest Login signatures, 305
- 3304 Windows Null Account Name signatures, 305
- 3305 Windows Password File Access signatures, 305
- 3306 Windows Registry Access signatures, 306
- 3307 Windows Redbutton Attack signatures, 306
- 3308 Windows LSARPC Access signatures, 307
- 3309 Windows SRVSVC Access signatures, 307
- 3400 Sun Kill Telnet DoS signatures, 310
- 3401 Telnet-IFS Match signatures, 310
- 3405 Finger Bomb signatures, 310
- 3500 rlogin-froot signatures, 311

- 3525 IMAP Authenticate Overflow signatures, 311
- 3526 IMAP Login Buffer Overflow signatures, 311
- 3530 Cisco Secure ACS Oversized TACACS+ Attack signatures, 312
- 3540 Cisco Secure ACS CSAdmin Attack signatures, 312
- 3550 Pop Buffer Overflow signatures, 312
- 3575 INN Buffer Overflow signatures, 312
- 3576 INN Control Message Exploit signatures, 313
- 3600 IOS Telnet Buffer Overflow signatures, 313
- 3601 IOS Command History Exploit signatures, 313
- 3602 Cisco IOS Identity signatures, 314
- 3603 IOS Enable Bypass signatures, 314
- 3650 SSH RSAREF Buffer Overflow signatures, 314
- 3990 BackOffice BO2K TCP Non Stealth signatures, 315
- 3991 BackOffice BO2K TCP Stealth 1 signatures, 315
- 3992 BackOrifice BO2K TCP Stealth 2 signatures, 315
- 4000 Series UDP signatures. *See* UDP signatures
- 4002 UDP Flood signatures, 318
- 4050 UDP Bomb signatures, 318
- 4051 Snork signatures, 319
- 4052 Chargen DoS signatures, 319
- 4053 Back Orifice signatures, 320
- 4054 RIP Trace signatures, 320
- 4055 BackOrifice BO2K UDP signatures, 320
- 4100 TFTP Passwd signatures, 321
- 4150 Ascend Denial of Service signatures, 321
- 4200 Series Sensing Configuration Screen (CSPM), 389–392
- 4200 Series sensors, 77
  - appliances, 145
    - IDS-4210, 148–149
    - IDS-4230, 146–147
  - bootstrap, configuring, 151–158
  - checking, 168–169
  - configuration files, pushing to, 167–168
  - configuring
    - 4200 Series Sensing Configuration Screen (CSPM), 389–392
    - saving, 166–167
    - sysconfig-sensor command, 152–158
    - updating, 166–167
- CSPM Director
  - adding to, 158–169
  - installing within, 145
- default gateway, entering, 161–162
- logon accounts, 149–151
- management access, 149
- PDP (policy distribution point), selecting, 166
- PostOffice identification parameters, entering, 159–161
- settings, verifying, 163
- signature templates, entering, 162–163
- 4600 IOS UDP Bomb signature, 321
- 5000 Series Web/HTTP signatures, 321–349
- 5034 WWW IIS newdsn Attack signature, 324
- 5035 HTTP cgi HylaFAX Faxsurvey signature, 325
- 5036 WWW Windows Password File Access Attempt signature, 325
- 5037 WWW SGI MachineInfo Attack signature, 325
- 5038 WWW wwwsql File Read Bug signature, 326
- 5039 WWW Finger Attempt signature, 326
- 5040 WWW Perl Interpreter Attack signature, 326
- 5041 WWW anyform Attack signature, 327
- 5042 WWW CGI Valid Shell Access signature, 327
- 5043 WWW Cold Fusion Attack signature, 327
- 5044 WWW Webcom.se Guestbook Attacks signature, 328
- 5045 WWW xterm Display Attack signature, 328
- 5046 WWW dumpenv.pl Recon signature, 329
- 5047 WWW Server Side Include POST Attack signature, 329
- 5048 WWW IIS BAT EXE Attack signature, 329
- 5049 WWW IIS Showcode .asp Attack signature, 330
- 5050 WWW IIS .htr Overflow signature, 330
- 5051 IIS Double Byte Code Page signature, 330
- 5052 FrontPage Extensions PWD Open Attempt signature, 331
- 5053 FrontPage\_vti\_bin Directory List Attempt signature, 331
- 5054 WWWBoard Password signature, 331
- 5055 HTTP Basic Authentication Overflow signature, 331
- 5056 WWW Cisco IOS % % DoS signature, 332
- 5057 WWW Sambar Samples signature, 332
- 5058 WWW info2www Attack signature, 332
- 5059 WWW Alibaba Attack signature, 333

- 5060 WWW Excite AT-generate.cgi Access signature, 333
- 5061 WWW catalog\_type.asp Access signature, 333
- 5062 WWW classifieds.cgi Attack signature, 334
- 5063 WWW dmbldparser.exe Access signature, 334
- 5064 WWW imagemap.cgi Attack signature, 334
- 5065 WWW IRIX Infosrch.cgi Attack signature, 334
- 5066 WWW man.sh Access signature, 335
- 5067 WWW plusmail Attack signature, 335
- 5068 WWW formmail.pl Access signature, 335
- 5069 WWW whois\_raw.cgi Attack signature, 336
- 5070 WWW msacds.dll Access signature, 336
- 5071 WWW msacds.dll Attack signature, 336
- 5072 WWW bizdb 1-search Attack signature, 337
- 5073 WWW EZshopper loadpage.cgi Attack signature, 337
- 5074 WWW EZshopper search.cgi Attack signature, 337
- 5075 WWW IIS Virtualized UNC Bug signature, 337
- 5076 WWW webplus Bug signature, 338
- 5077 WWW Excite AT-admin.cgi Access signature, 338
- 5078 WWW Pirahna Password Attack signature, 339
- 5079 WWW PCCS MySQL Admin Access signature, 339
- 5080 WWW IBM WebSphere Access signature, 339
- 5081 WWW WinNT cmd.exe Access signature, 340
- 5083 WWW Virtual Vision FTP Browser Access signature, 340
- 5084 WWW Alibaba Attack 2 signature, 340
- 5085 WWW IIS Source Fragment Access signature, 341
- 5086 WWW WEBactive Logfile Access signature, 341
- 5087 WWW Sun Java signature, 341
- 5088 WWW Akopia MiniVend Access signature, 341
- 5089 WWW Big Brother Directory Access signature, 342
- 5090 WWW FrontPage htmage.exe Access signature, 342
- 5091 WWW Cart32 Remote Admin Access signature, 342
- 5092 WWW CGI-World Poll It Access signature, 343
- 5093 WWW PHP-Nuke admin.php3 Access signature, 343
- 5095 WWW CGI Script Center Account Manager Attack signature, 343
- 5096 WWW CGI Script Center Subscribe Me Attack signature, 344
- 5097 WWW FrontPage MS-DOS Device Attack signature, 344
- 5099 WWW GWScripts News Publisher Access signature, 344
- 5100 WWW CGI Center Auction Weaver File Access signature, 344
- 5101 WWW CGI Center Auction Weaver Attack signature, 345
- 5102 WWW phpPhotoAlbum explorer.php Access signature, 345
- 5103 WWW SuSE Apache CGI Source Attack signature, 345
- 5104 WWW YaBB File Access signature, 346
- 5105 WWW Ranson Johnson mailto.cgi Attack signature, 346
- 5106 WWW Ranson Johnson multiform.pl Access signature, 346
- 5107 WWW Mandrake Linux/Perl Access signature, 347
- 5108 WWW Netgrity Site Minder Access signature, 347
- 5109 WWW Sambar Beta search.dll Access signature, 347
- 5110 WWW SuSE Installed Packages Access signature, 348
- 5111 WWW Solaris Anwerbook2 Access signature, 348
- 5112 WWW Solaris Answerbook 2 Attack signature, 348
- 5113 WWW CommuniGate Pro Access signature, 349
- 5114 WWW IIS Unicode Attack signature, 349
- 51301 Rlogin IFS=/ signature, 376
- 51302 Rlogin /etc/shadow signature, 377
- 51303 Rlogin + + signature, 377
- 6000 Series cross-protocol signature.  
*See* cross-protocol signature
- 6001 Normal SATAN Probe signature, 350
- 6002 Heavy SATAN Probe signature, 350
- 6050 DNS HINFO Request signature, 351
- 6051 DNS Zone Transfer Request signature, 352

6052 DNS Zone Transfer from High Point signature, 352

6053 DNS Request for All Records signature, 353

6054 DNS Version Request signature, 353

6055 DNS Inverse Query Buffer Overflow signature, 353

6056 BIND NXT Buffer Overflow signature, 354

6057 BIND SIG Buffer Overflow signature, 354

6100 RPC Port Registration signature, 356

6101 RPC Port Unregistration signature, 356

6102 RPC Dump signature, 357

6103 Proxied RPC Request signature, 357

6104 RPC Set Spoof signature, 357

6105 RPC Unset Spoof signature, 358

6110 RPC RSTATD Sweep signature, 358

6111 RPC RUSERSD Sweep signature, 358

6112 RPC NFS Sweep signature, 359

6113 RPC MOUNTD Sweep signature, 359

6114 RPC YPPASSWDD Sweep signature, 359

6115 RPC SELECTION\_SVC Sweep signature, 359

6116 RPC REXD Sweep signature, 360

6117 RPC STATUS Sweep signature, 360

6118 RPC ttdb Sweep signature, 360

6150 ypserv Portmap Request signature, 361

6151 ypbind Portmap Request signature, 361

6152 yppasswdd Portmap Request signature, 361

6153 yupdated Portmap Request signature, 362

6154 ypxfrd Portmap Request signature, 362

6155 mountd Portmap Request signature, 363

6175 rexd Portmap Request signature, 363

6180 rexd Attempt signature, 363

6190 statd Buffer Overflow signature, 364

6191 RPC.tooltalk Buffer overflow signature, 364

6192 RPC mountd Buffer Overflow signature, 364

6193 RPC CMSD Buffer Overflow signature, 364

6194 sadmind RPC Buffer Overview signature, 365

6195 RPC and Buffer Overflow signature, 365

6200 Ident Buffer Overflow signature, 366

6201 Ident Newline signature, 367

6202 Ident Improper Request signature, 367

6250 FTP Authorization Failure signature, 368

6251 Telnet Authorization Failure signature, 368

6252 Rlogin Authorization Failure signature, 369

6253 POP3 Authorization Failure signature, 369

6255 SMB Authorization Failure signature, 369

6300 Loki ICMP Tunneling signature, 370

6302 General Loki ICMP Tunneling signature, 370

6500 RingZero Trojan signature, 366

6501 TFN Client signature, 371

6502 TFN Server Reply signature, 371

6504 Stacheldraht Server Reply signature, 372

6505 Trinoo Client Request signature, 373

6506 Trinoo Server Reply signature, 373

6507 TFN2K Control Traffic signature, 373

6508 mstream Control Traffic signature, 374

8000 Series string-matching signature, 375–378

## A

abnormal TCP packets, TCP signatures, 281–283

access

- administrative access, limiting, 36
- anonymous access, reducing, 36
- management access, 4200 Series Sensors, 149

access class signature, 235

access control lists (ACLs). *See* ACLs (access control lists)

accessing

- sensors, 757–759
- user accounts, 17

accounts

- access attacks, 17
- logon accounts, 4200 Series Sensors, 149–151
- netrangr account, 150

ACLs (access control lists), 237, 464. *See also* IP blocking

blocking

- applying to E1 interface, 660
- applying to external interfaces, 473
- applying to inbound traffic, 464
- applying to internal interfaces, 473

blocking

- enhancements, 619
- related tokens, 708–709

contents, displaying, 511

denied hosts, adding, 656

IP blocking

- anti-spoofing mechanisms, 466
- at the router, 468–469
- configuring, 474–476
- critical hosts, 467
- default block time, 470
- disabling, 477, 479
- duration of, 468

- entry points, 467
  - signature selection, 467
- IP blocking, implementing, 466
- logging policy violations, 653
- placement, 471–473
- signatures, 237
  - creating, 455–456
  - SYSLOG sources, defining, 456–457
  - tokens, 706
- actions
  - allowed by authorized hosts, 717
  - applying to signatures, 433–434
  - default, setting, 594
  - defining for Cisco IOS Firewall IDS, 582
- Actions group box (Event Viewer Preferences window)
  - Command Timeout, 208–209
  - Subnet Mask, 209
  - Time To Block, 209
- active Cisco Secure IDS version, displaying, 696
- active partition, 514
- Active Scripting Pages (ASPs), 339
- ad hoc attacks, 15
- Add Host Wizard
  - Host Type window, 545
  - sensors, adding, 541–549
  - Shunning Initialization window, 548
  - starting, 543
- Add Host Wizard (nrConfigure), 561
- Add Host Wizard Finished window (nrConfigure), 564
- Add Sensor Wizard, 159–160
- adding
  - Cisco IOS Firewall to Director configuration, 601–602, 604
  - comments to configuration files, 700
  - communication parameters to Cisco IOS Firewall IDS, 642–643
  - configured sensors to Director, 561
    - host type selection, 564
    - parameters, 563
  - connection signatures, 435–436
  - denied hosts to ACLs, 656
  - hosts to Director configuration, 560–561
  - IDS to CPM, 513
  - secondary Directors, 561
- Additional Destinations Configuration Screen (CSPM), 406
- address mask requests, 258
- addressing, PostOffice protocol, 89
- administrative access, limiting, 36
- advanced signature configuration, 451
  - Port Mapping, 453, 455
  - Signature Tuning, 451–453
- advanced signature filtering, 447–449
- Advisory/Related Information Links field (NSDB Related Vulnerability page), 197
- Affected Programs field (NSDB Related Vulnerability page), 196
- Affected Systems field (NSDB Related Vulnerability page), 196
- agents, 27
- alarm event record fields, log files, 741–744
- alarms, 468
  - benign triggers, 192
  - context buffer, viewing, 187, 189
  - deleting, 197–198
  - destinations, configuring, 716–717
  - Director platforms
    - displays, 80
    - responses, 81
  - expansion boundaries, modifying, 204–205
  - false positives, 182
    - reducing, 759–762
  - fields, 180
    - Count field, 181
    - Destination Information fields, 183
    - General Information fields, 181–182
    - Signature Information fields, 183–184
    - Source Information fields, 182
  - forwarding related tokens, 710
  - high-severity, 779
  - host names, resolving, 184–186
  - low-severity, 779
  - medium-severity, 779
  - notification queue, setting, 588–589
  - resuming display (Event Viewer), 199–200
  - Severity values, 184
    - configuring, 214
  - suspending display (Event Viewer), 199–200
  - temporary exclusions, 762
- AlarmThrottle master signature parameter, 630
- Alias field (NSDB Related Vulnerability page), 195

- analyzing network topology, 97
  - critical components, 100–101
  - entry points, 98–100
  - remote networks, 102
  - security policy restrictions, 102–103
  - size and complexity issues, 102
- anomaly detection, IDSs (Intrusion Detection Systems), 54–58
  - benefits, 56–58
  - drawbacks, 57–58
  - issues, 56
  - neutral networks, 56
  - rule-based approach, 55
  - statistical sampling, 55
- anonymous access, reducing, 36
- answers to review questions, 815–835
- anti-spoofing mechanisms, 466
- appliances, 4200 Series Sensors, 145
  - IDS-4210, 148–149
  - IDS-4230, 146–147
- application holes, 23
- Application Name field (Cisco Secure IDS alarm records), 182
- application partition, 515
- applications
  - TCP signatures, 309–315
  - UDP signatures, 319–321
- apply command, 517
- applying
  - ACLs
    - interface selection, 471–472
    - specifying traffic direction, 473
    - to E1 interfaces, 660
    - to external interfaces, 473
    - to inbound traffic, 464
    - to internal interfaces, 473
  - actions to signatures, 433–434
  - audit rules, 595, 597–598
  - initial configuration to ISDM, 499
  - saved configuration versions, 571
  - signature templates to sensors, 442
  - signature updates to ISDM, 517
  - transient configuration versions, 571
- architecture
  - Cisco Secure IDS sensors, 687
    - nr.fileXferd, 690
    - nr.loggerd, 689
    - nr.managed, 689
    - nr.packedd, 689
    - nr.postofficed, 689
    - nr.sapd, 689
  - CSPM Director, 690
    - services, 691–692
- archived log files, 740
- ARP (Address Resolution Protocol), 19
- ASPs (Active Scripting Pages), 339
- assigned port numbers, 435
- assigning
  - command and control port on ISDM, 502
  - signature templates to sensors, 442
- atomic signatures, 192, 233, 581
- ATOMIC.ICMP signature engine, 628
- ATOMIC.IPOPTIONS signature engine, 628
- ATOMIC.L3.IP signature engine, 628
- ATOMIC.TCP signature engine, 628
- ATOMIC.UDP signature engine, 629
- attacks, 6–7
  - ad hoc, 15
  - attributes, 7
  - common points of, 16
    - network protocols, 18–19
    - network resources, 16–17
  - DoS
    - distributed attacks, 27, 29
    - host resource starvation, 26
    - network resource overload, 24–25
    - out-of-bounds, 26
  - exploitation tools, 20
    - authentication compromises, 21–22
    - compromised trust relationships, 23–24
    - poorly configured services, 22
    - protocol weaknesses, 22
  - external threats, 9
  - goal setting, 11–12
  - ICMP, 266
  - internal threats, 9–10
  - Internet, usage estimates, 98
  - man-in-the-middle, 18
  - methodical, 15
  - patient, 16
  - publishing publicly, 57
  - reconnaissance, 12–13
  - reconnaissance tools, 19–20
  - script kiddies, 7–8



- spoofing, 19
- structured threats, 9
- surgical strikes, 15
- Trojan horses, 17
- UDP signatures, 318–319
- unstructured threats, 7–8
- variable time-to-live attacks, 63
- attributes of attackers, 7
- audit rules
  - configuring on Cisco IOS Firewall IDS, 593–598
  - creating, 595–598
  - packet auditing process, 593–594
- authentication
  - administrative access. limiting, 36
  - anonymous access, reducing, 36
  - common privilege groups, defining, 35–36
  - compromising, 21–22
  - failures, signatures, 367–369
  - improving, 35–36
  - one-time passwords, 36
  - trust relationships, minimizing, 36
- authorization, troubleshooting Oracle database, 731
- authorized hosts, 717
- automatic monitoring, network security, 43
- availability, 11

## B

---

- back doors, 24
- bandwidth consumption attacks, 24–25
- benign signatures, 238
- benign triggers, 192
- bin directory, 697
- blades
  - configuring multiple per chassis, 678
    - general setup, 680–685
    - limitations per IDSM, 678–679
    - network diagram, 680
    - VACL definition, 680
- Blank Left value (Event Viewer), configuring, 209–210
- Blank Right value (Event Viewer), configuring, 210
- blocking, 661
  - ACL enhancements, 619
  - Catalyst 5000 RSM, 619
  - IDSM, 620
  - master blocking sensor, 709
  - PIX, 619
  - related tokens, 708–709
  - sensors, 100
- Blocking Configuration Screen (CSPM), 397–400
- bootstraps, configuring on 4200 Series
  - sensors, 151–158
- boundaries, establishing, 37–39
- Boundaries group box (Event Viewer Preferences window), 212
- brute-force attacks, 21

## C

---

- cable requirements, laptop-to-COM port connections, 758
- Cannot write message to Director error, troubleshooting, 722
- capturing traffic, 495
  - SPAN feature (IDSM), 496
    - limitations, 497
    - spanning ports, 496
    - spanning VLANs, 496
  - VACLs, 497
    - interesting traffic, 498
    - limitations, 498
  - with IDSM, 490
- case studies
  - Cisco IOS Firewall IDS
    - general setup, 641–644
    - limitations, 639–640
    - network diagram, 640
    - required equipment, 640
    - troubleshooting tips, 644–650
  - configuring multiple blades per chassis, 678
    - general setup, 680–685
    - limitations per IDSM, 678
    - network diagram, 679
    - required equipment, 679
    - VACL definition, 680
  - router management, 657
    - general setup, 658–666
    - limitations, 657
    - network diagram, 658
    - required equipment, 658

- troubleshooting tips, 666–669
- SYSLOG files, reporting to sensors, 650
  - general setup, 651–655
  - limitations, 650
  - network diagram, 651
  - required equipment, 650
  - troubleshooting tips, 656–657
- tiered director hierarchy, 670
  - alarm delay limitations, 670
  - general setup, 671–675
  - network diagram, 670
  - required equipment, 670
  - troubleshooting tips, 675–678
- Catalyst 5000 RSM, blocking with, 619
- Catalyst 6000 IDSM, 489–490
  - blocking with, 620
  - commands, 509–512
  - comparing to traditional platforms, 491
  - disk structure
    - active partition, 514
    - application partition, 515
    - maintenance partition, 515
  - ID analysis, configuring, 501–507
    - assign command and control port, 502
    - clearing unwanted VLAN traffic, 507–509
  - images, updating, 515–516
  - initialization, 499–501
  - ports, 493–494
  - requirements, 492
  - software files, 516
    - updating, 517–518
  - traffic flow, 494
  - traffic, capturing, 495
    - SPAN, 496
    - VACLs, 497–498
  - verifying configuration, 509–513
- Cells group box (Event Viewer Preferences window), 209–210
- checking
  - configurations, sensors, 168–169
  - sensor errors, 421
- Cisco IOS Firewall IDS
  - actions,
    - defining, 582
    - configurable, 641
  - adding to Director configuration, 601–604
  - alarm notification queue, setting, 588–589
  - audit rules, configuring, 593–598
  - configuring
    - general setup, 641–644
    - limitations, 639–640
    - network diagram, 640
    - required equipment, 640
    - troubleshooting tips, 644–650
  - impact on network performance, 580
  - initialization, 583–589
  - PostOffice parameters, configuring, 584–585
  - prospective customers, 578
  - protected networks, defining, 587–588
  - signatures, 797–800
    - configuring, 589–592
    - excluding, 591–592
    - implementing, 581
    - response options, 581
  - verifying configuration, 598–601
- Cisco Secure Communications Deployment worksheet (CSPM), 124
- Cisco Secure IDS, 71
  - active version, displaying, 696
  - communications deployment worksheet, 803–805
  - configuration GUI, 691–692
  - configuring, 72–76
  - daemon, starting and stopping, 727
  - Director platforms, 80–83
  - directory structure, 696
    - bin directory, 697
    - etc directory, 698
    - install directory, 696
    - var directory, 698
  - functions and features, 72–76
  - Home submap, removing sensor icon, 567
  - IP blocking configuration, 474–476
  - log files, naming conventions, 739
  - modules, 77–80
  - PostOffice protocol, 84
  - sensors
    - architecture, 687
    - blocked addresses, viewing, 480–481
    - master blocking sensors, configuring, 479
    - Never Block Addresses, configuring, 478–479
    - nr.fileXferd, 690
    - nr.loggerd, 689

- nr.managed, 689
- nr.packetd, 689
- nr.postofficed, 689
- nr.sapd, 689
- platforms, 77–80
- services
  - stopping, 694
  - verifying operability, 695
- Signature Engine Supplement, 630
- user-defined signatures, 628–633
- User Guide, 148–149
- version 3.0, 614–620
  - configuration enhancements, 614–615
  - installation enhancements, 614–615
  - shunning enhancements, 618–620
  - signatures enhancements, 616–618
- version 4.0, 620–625
  - blocking, 624
  - configuration, 620–622
  - installation, 620–623
  - signatures, 623–624
- Cisco Secure Intrusion Detection Director (CSIDD).  
*See* CSIDD (Cisco Secure Intrusion Detection Director)
- Cisco Secure Policy Manager (CSPM). *See* CSPM
- Cisco Secure VPN Client, installing CSPM, 125
- Cisco Security Wheel, 34–42
- classes, signatures, 234–235
  - access class signatures, 235
  - denial of service class signatures, 235
  - informational class signatures, 234
  - reconnaissance class signatures, 234
- clear config command, 513
- clear ip audit configuration command, 600
- clear ip audit statistics command, 600
- clear trunk command, 509
- clearing unwanted VLAN traffic from IDSM, 507
- CLI (command-line interface), Catalyst 6000 switch commands, 509–512
- client-server configurations, CSPM, 120
- closing
  - active log files, 740
  - Configuration Library, 572
- collapsing columns (Event Viewer), 203–204
  - viewing fields, 201–202
- Color value (Event Viewer), configuring, 213
- columns
  - deleting, 205
  - expansion boundaries, modifying, 204–205
  - moving, 205
  - nrConfigure screen display, 558
  - selecting for display (Event Viewer), 207
- COM port (sensors)
  - configuring, 759
  - connecting to, 757–759
- command and control networks, Cisco Secure IDS deployment, 107
- command and control port, Catalyst 6000 IDSM, 494
- command event record fields, log files, 744–746
- Command Timeout value, configuring, 208–209
- commands
  - apply, 517
  - Catalyst
    - reset, 520–521
    - show module, 520
    - show port, 520
  - clear config, 513
  - clear ip audit configuration, 600
  - clear ip audit statistics, 600
  - clear trunk, 509
  - commit security acl, 506
  - cvtnrlog, 692
  - diag, 513
  - EXPN sendmail command, 233
  - GET command, 293
  - grep, 237, 751
  - ids-installer, 518
  - IDSM, 521
    - diag bootresults, 522
    - nrconns, 522
    - report systemstatus, 522
    - show errorfile, 523
  - ip audit name, 595
  - ip audit po protected, 587
  - ip audit po remote, 585
  - ip audit signature, 591
  - mailx, 732
  - more, 754, 756–757
  - nrconns, 694, 753
  - nrstart, 693, 727
  - nrstatus, 695, 750–751, 756
  - nrstatus command, 536

- nrstop, 694, 727
- nvers, 696
- ping, 750
- ping-R, 248
- redirect, 692
- session, 499
- session (Catalyst switch), 499
- set boot device, 514
- set security acl ip, 504–505
- set span, 503
- set trunk, 508
- show config, 509–510
- show configuration, 513
- show ip audit configuration, 643
- show ip audit debug, 600
- show ip audit interface, 644
- show ip audit statistics, 599
- show security acl, 511
- show span, 510–511
- snoop, 150
- Solaris, snoop, 752
- sysconfig-sensor, 152–158, 410
- sysconfig-sensor command, 540
  - exiting, 158
- tail command, 81
- tail -f, 753
- TRACEON, 320
- VERFY, 233
- write memory, 653
- comments, inserting in configuration files, 700
- commit security acl command, 506
- common privilege groups, defining, 35–36
- communication link (Director/sensor), verifying operability, 694, 753–754
- communication parameters, adding to Cisco IOS
  - Firewall IDS, 642–643
- communications deployment worksheet, Cisco
  - Secure IDS, 803–805
- comparing
  - Catalyst 6000 IDSM and traditional platforms, 491
  - MSFC and standalone routers, 492
- composite signatures, 192, 233
- compound signatures, 581
- confidentiality, 11, 39–41
- Configuration File Management Utility
  - removing sensors from nrConfigure
    - Director, 566
  - starting, 542
- configuration files, 699–700
  - auths, 717
  - comments, inserting, 700
  - CSIDD, creating, 535
  - daemons, 718
  - destinations, 716–717
  - hosts, naming convention, 714–715
  - intrusion detection, 700
  - loggerd.conf, tokens, 710
  - nr.postofficed.conf, fault management, 712–714
  - reviewing periodically, 45
  - routes file, 715–716
  - sensors, pushing to, 167–168
  - tokens, 699
    - DupDestination, 710
    - FilenameOfIPLog, 711
    - FilenameOfLog, 711
    - general signature, 702
    - internal network, 701
    - MinutesOfAutoLog, 711
    - MinutesOfAutoShun, 709
    - NameOfPacketDevice, 701
    - NetDevice, 708
    - NeverShunAddress, 709
    - NumberOfSwitchBytes, 711
    - NumberOfSwitchMinutes, 711
    - RecordOfDataSource, 707
    - RecordOfExcludedNetAddress, 707–708
    - RecordOfFilterName, 706
    - RecordOfStringName, 704–705
    - ShunInterfaceCisco, 708
    - SigOfFilterName, 706
    - SigOfStringMatch, 704–705
    - SigOfTcpPacket, 703–704
    - SigOfUdpPacket, 703–704
    - WatchDogInterval, 713
    - WatchDogNumProcessRestarts, 713
    - WatchDogProcDeadAlarmLevel, 714
    - WatchDogProcTimeOutAlarmLevel, 714
    - WatchDogResponseTimeout, 713

- Configuration Library
  - closing, 572
  - opening, 568
  - saved versions, applying, 571
  - transient versions, 569–571
  - versions
    - deleting, 571–572
    - numbering, 570
    - saving, 571
- Configuration Management Utilities (nrConfigure), troubleshooting, 733
- configuring
  - 4200 Series Sensors
    - bootstrap, 151–158
    - sysconfig-sensor command, 152–158
  - Catalyst 6000 IDSM
    - initialization, 499, 501
  - Cisco IOS Firewall IDS
    - audit rules, 593–595, 597–598
    - general setup, 641–644
    - initialization, 583–589
    - limitations, 639–640
    - network diagram, 640
    - PostOffice parameters, 584–585
    - required equipment, 640
    - signatures, 589–592
    - SPAM signatures, 589–590
    - troubleshooting tips, 644, 646–650
    - verification, 598–601
  - CSIDD
    - configuration files, 535
    - identification parameters, 532–534
    - signature responses, 665–666
  - CSPM, 119–136
  - domain name, 732
  - dual-homed Director, 666–669
  - Event Viewer
    - Blank Left value, 209–210
    - Blank Right value, 210
    - Color value, 213
    - Command Timeout value, 208–209
    - Default Expansion value, 212
    - Event Batching value, 213
    - Icon value, 213
    - Maximum Events Per Grid value, 212
    - Subnet Mask value, 209
    - Time To Block value, 209
  - events, destinations, 716–717
  - HTML browser, location, 558
  - IDSM
    - ID analysis, 501–509
    - verification, 509–513
  - IP blocking, 474
    - Never Block Addresses, 478–479
    - setting blocking device properties, 475–476
  - mail server, 732
  - master blocking sensors, 479
  - multiple blades per chassis, 678
    - general setup, 680–685
    - limitations per IDSM, 678
    - network diagram, 679
    - required equipment, 679
    - VACL definition, 680
  - nrConfigure, HTML browser, 558
  - sensors
    - advanced changes, 416–420
    - basic changes, 410–414
    - checking, 168–169
    - CSIDD, 540–549
    - COM port settings, 759
    - CSPM sensor configuration screens, 386–409
    - Director platforms, 81
    - error checks, 421
    - identification parameters, 410–411
    - installing, 105–111
    - internal networks, 412–413
    - IP fragment reassembly, 416–417
    - log files, 414–416
    - packet capture devices, 413–414
    - pushing new ones to, 420–421
    - saving, 166–167, 421
    - TCP session reassembly, 417–419
    - updating, 166–167, 421
  - signatures
    - actions, 433–434
    - advanced settings, 451–455
    - CSPM templates, 428–429
    - filtering, 444
    - simple signature filtering, 444, 447
    - string signatures, 437–438
  - TCP reset response, 72–74

- connecting laptops/PCs to sensor COM port, 757–759
- connection signatures, 236, 434–435, 617, 791–793
  - adding, 435–436
  - modifying, 436
- Connection Status pane (Event Viewer), 214
  - Connection Status window, 215–216
  - Reset Statistics window, 220
  - Sensor Statistics window, 219
  - Service Status window, 216–218
  - Service Versions window, 218
- Connection Status window, 215–216
- Consequences field (NSDB Related Vulnerability page), 196
- content-based signatures, 192, 232
- context buffer, viewing, 187–189
- context signatures, 192, 232
- core dumps, 733
- corporate network reorganization, troubleshooting, 648–650
- Count field (Cisco Secure IDS alarm records), 181
- Countermeasures field (NSDB Related Vulnerability page), 197
- creating
  - ACL signatures, 455–456
  - advanced filters, 449
  - audit rules, 595, 597–598
  - signature templates, 440
  - string signatures, 438
  - VACLs, 504–505
- critical hosts, identifying, 467
- cross-protocol signatures (6000 Series), 349
  - authentication failures, 367–369
  - DDoS attacks, 371–374
  - DNS attacks, 351–354
  - Ident attacks, 366–367
  - Loki attacks, 370
  - RPC attacks, 355–366
  - SATAN attacks, 349–350
- CSIDD (Cisco Secure Intrusion Detection Director), 531
  - daemons, run verification, 536–537
  - Exclude mechanism, 760
  - HP Open View NNM
    - environment initialization, 537–539
    - starting, 537
  - installing, 531–535
    - configuration files, 535
    - identification parameters, 532–534
    - install script, 532
    - netrangr password, 532–533
    - rebooting, 535
  - NNM, navigation buttons, 539–540
  - sensors
    - adding, 541–549
    - configuring, 540–549
  - signatures responses, configuring, 665–666, 760–762
  - starting, 536–540
  - submaps, 538
  - verifying smid process, 756
- CSPM (Cisco Secure Policy Manager), 81, 117
  - 4200 Series Sensors
    - adding to Director, 158–169
    - installing, 145
  - Cisco Secure Communications Deployment worksheet, 124
  - Cisco Secure VPN Client, installing on, 125
  - database
    - alarms, removing, 197–198
    - rows, deleting, 199
    - entries, viewing, 178
  - Director platform
    - adding sensors to, 158–169
    - architecture, 690
    - operating as, 81–82
    - services, 691–692
    - smid process, verifying, 755
  - General tab, signature configuration, 428–429
  - hosts
    - adding to topology, 164–165
    - resolving names, 186
  - identification parameters, verifying, 659
  - installing
    - account information, 129
    - basic settings, 129
    - configuring, 119–121
    - finalization, 134–136
    - license acceptance, 126–127
    - modes, 127–130
    - PostOffice protocol, 132–135
    - requirements, 121–124
    - settings, 124–136
  - licensing options, 123–124

- logging on, 136
- manual blocking operations, 482–483
- sensor configuration screens, 386–409
  - 4200 Series Sensing Configuration Screen, 389–392
  - Blocking Configuration Screen, 397–400
  - Filtering Configuration Screen, 400–403
  - IDSM Sensing Configuration Screen, 392–397
  - Logging Configuration Screen, 402–406
  - Sensor Command Configuration Screen, 406–409
  - Sensor Internal Networks Configuration Screen, 389
  - Sensor Monitoring Configuration Screen, 388
  - Sensor Properties Configuration Screen, 387
- sensors, configuring within, 385–421
- service versions, obtaining, 218
- signatures
  - filtering, 760
  - templates, creating, 440
  - viewing properties, 430–431
- Signatures tab, 429
- software feature sets, 118–119
- starter videos, 137–139
- starting, 136–139
- string signatures, creating, 438
- support applications, 122
- TechSmith Screen Capture Codec, installing, 131
- Tools menu, View Sensor Events command, 178
- Windows NT 4.0 hosts, building, 125–126
- CSPM Event Viewer. *See* Event Viewer
- customizing Event Viewer, view settings, 207
- cvtnrlog.exe, 692

## D

- Daemon Versions window (Event Viewer), 218
- daemons
  - application ID, 718–719
  - configuration files, 699–700
  - fault management, related tokens, 713–714
  - operability, verifying, 536–537
- data integrity, 11
- data sources, public, 12
- databases
  - Cisco Secure IDS alarm records, fields, 181
  - CSPM, removing alarms, 197–198
  - NSDB
    - Exploit Signature page, 190–193
    - opening, 189
    - Related Vulnerability page, 194–197
  - Oracle
    - database instance name, changing, 730
    - troubleshooting, 728–729
- DDoS (distributed denial-of-service) attacks, 27
  - signatures, 371–374
- default actions, signature configuration, 594
- default block time, 470
- Default Expansion value (Event Viewer), configuring, 212
- Default signature template, 428
- defining
  - common privilege groups, 35–36
  - endpoints, 40–41
  - interesting traffic, 498
  - protected networks, 587–588
  - security zones, 38
  - signature severity, 430–431
  - SYSLOG sources for ACL signature monitoring, 456–457
  - untrusted links, 39
- Delete Selected Rows button (Event Viewer), 199
- deleting
  - alarms, 197–198
  - columns in Event Viewer, 205
  - saved configuration versions, 571–572
  - sensors from nrConfigure Director, 566
- denial-of-service attacks
  - anti-spoofing mechanisms, 466
  - class signatures, 235

- denied hosts, adding to ACLs, 656
- deploying sensors
  - installation, 103–111
  - preparation, 97–103
- Description column (nrConfigure screen display), 558
- Destination Address field (Cisco Secure IDS alarm records), 183
- Destination Information fields (Cisco Secure IDS alarm records), 183
- Destination Location field (Cisco Secure IDS alarm records), 183
- Destination Port field (Cisco Secure IDS alarm records), 183
- destinations file, 716–717
  - viewing, 754
- Details field (Cisco Secure IDS alarm records), 184
- device management
  - requirements, 465
  - sensors, 100, 107
- devices
  - blocking devices, configuring identification parameters, 475
  - hosts
    - /usr/nr/etc/hosts file entries, 714–715
    - IP address configuration, 715–716
    - names, resolving, 184–186
    - managed network devices, viewing, 482
    - MSFC versus standalone router, 492
- diag bootresults command (ISDM), 522
- diag command, 513
- Diagnostics mode (IDSM)
  - commands, 521
    - diag bootresults, 522
    - nrconns, 522
    - report system status, 522
    - show errorfile, 523
  - enabling on IDSM, 513
- dialog boxes, Sensor Identification, 159
- dictionary password crackers, 21
- Director platforms, 80–83
  - alarms
    - displays, 80
    - responses, 81
  - Cisco Secure IDS Director for UNIX, 82
  - communication with sensors, verifying, 753–754
  - compared, 83
  - CSIDD. *See* CSIDD
  - CSPM, 159
    - adding sensors to, 158–169
    - architecture, 690
    - operating as, 81–82
    - services, 691–692
    - smid process, verifying, 755
  - error log files, viewing, 756–757
  - features, 80
  - forwarding alarms, related tokens, 710
  - hosts, adding to configuration, 560–561
  - inability to write to socket, troubleshooting, 722
  - LD\_LIBRARY\_PATH variable,
    - troubleshooting, 724
  - overflowing socket buffer, troubleshooting, 722
  - permissions, troubleshooting, 722–723
  - secondary, adding, 561
  - semaphore files, troubleshooting, 723–724
  - sensors
    - 4200 Series Sensors, adding to, 158–169
    - logging, 726
    - maximum allowable alarms, 726
    - remote configuration, 81
    - routing threshold, 725
    - severity status, 725
  - Show Current Events window,
    - troubleshooting, 726
- directory structure (Cisco Secure IDS)
  - bin directory, 697
  - etc directory, 698
  - install directory, 696
  - var directory, 698
- Disable alarm level, 779
- disabling
  - debugging commands, 601
  - IP blocking, 477–479
  - signatures, 431–432, 761–762
- disk structure (IDSM)
  - active partition, 514
  - application partition, 515
  - maintenance partition, 515
- Display Popup Window status event, 212
- displaying
  - ACL contents, 511
  - active Cisco Secure IDS version, 696
  - blocked IP addresses, 480–481



- context buffer, 187–189
- log files, 179
- managed network devices, 482
- selected columns (Event Viewer), 207
- signature template, 428
- distributed attacks, 27, 29
- distributed configurations, CSPM, 120
- distributed denial-of-service (DDoS) attacks, 27, 371–374
- DNS (Domain Name System), 13
  - attack signatures, 351–354
  - cache poisoning, 23
  - host name resolution, 186
- documentation, security policies, 10–11
- domain name, configuring, 732
- Domain Name System (DNS). *See* DNS
- DOS (Disk Operating System), FAT (File Allocation Table), 121
- DoS (denial-of-service) attacks
  - distributed attacks, 27–29
  - host resource starvation, 26
  - network resource overload, 24–25
  - out-of-bounds, 26
- dual-homed Director, configuring, 666–669
- dual-tier signature response, 649–650
- DupDestination token, 710
- duplicate alarms, troubleshooting, 675
- duration of IP blocking time, selecting, 468

## E

- E1 interface, applying ACLs, 660
- echo requests, 258
- EDI (Event Database Interface), 691
- eliminating false positives from vulnerability scanner alarms, 645–647
- enabling
  - Diagnostic mode on IDSM, 513
  - Promiscuous mode on sniffing interface, 752
  - signatures, 431–432
  - Telnet, 466
- encryption
  - host-to-host encryption, 40
  - site-to-site encryption, 41
  - VPNs, 39
- endpoints, defining, 40–41

- engine-specific parameters, signatures, 630
- enhancements
  - Cisco Secure IDS
    - version 3.0, 614–620
    - version 4.0, 620–625
  - sensors, 625–628
  - version 3.0
    - configuration, 614–615
    - installation, 614–615
    - shunning, 618, 620
    - signatures, 616–618
  - version 4.0
    - blocking, 624
    - configuration, 620–622
    - installation, 620–623
    - signatures, 623–624
- entry points (networks)
  - IP blocking, 467
  - protecting with master blocking sensors, 470
  - sensors, 98–99
- environment variables, adding ORACLE\_HOME to LD\_LIBRARY\_PATH, 730
- error log files, viewing, 756–757
- errors
  - ICMP messages, 262
  - sensors, checking for, 168–169, 421
- /etc directory, 698
- evaluating
  - sensors, placement of, 46
  - professional security, 44
- Event Batching value (Event Viewer), configuring, 213
- event horizons, misuse detection, 60
- Event Severity Indicator group box (Event Viewer Preferences window), 213
- Event Viewer
  - alarms
    - collapsing columns, 203–204
    - deleting, 197–198
    - expanding collapsed columns, 201–202
  - blocked addresses, viewing, 480–481
  - columns
    - deleting, 205
    - moving, 205
    - selecting for display, 207
  - Connection Status pane, 214
  - Connection Status Window, 215–216

- Reset Statistics Window, 220
- Sensor Statistics Window, 219
- Service Status Window, 216–218
- Service Versions Window, 218
- Delete Selected Rows button, 199
- field expansion boundaries, modifying, 204–205
- log files, viewing, 179
- opening, 178
- Preferences window
  - Actions group box, 208–209
  - Boundaries group box, 212
  - Cells group box, 209–210
  - Event Severity Indicator group box, 213
  - Severity Mapping group box, 213
  - Status Events group box, 211
- resuming alarm display, 199–200
- Shunning Hosts window, 483
- suspending alarm display, 199–200
- events
  - destinations, configuring, 716–717
  - detection, verifying, 752
  - log files, 740–746
  - record fields
    - alarm event record fields, 741–744
    - command event record fields, 744–746
- EVS (Event Viewing System), 691
- Exclude mechanisms, 760
- excluding
  - false-positive alarms, 759–762
  - signatures, 591–592
- exclusion stance, security policies, 38
- exiting sysconfig-sensor script, 158
- expanding collapsed columns
  - all columns, 202
  - single column, 201
- expansion boundaries, modifying, 204–205
- Exploit Links field (NSDB Related Vulnerability page), 197
- Exploit Signature page (NSDB), 190–191
  - benign triggers, 192
  - implementation, 192
  - recommended alarm level, 192
  - signature description, 192
  - signature ID, 191
  - signature name, 190
  - signature structure, 192

- signature type, 192
- subsignature ID, 191
- user notes, 193
- vulnerability, 193
- Exploit Type field (NSDB Related Vulnerability page), 196
- exploitation tools, 20
  - application holes, 23
  - authentication compromises, 21–22
  - back doors, 24
  - compromised trust relationships, 23
  - poorly configured services, 22
  - protocol weaknesses, 22
- EXPN sendmail command, 233
- extended ACLs, 464
- external interfaces, applying ACLs, 473
- external threats, 9
- extranets, sensor placement, 104

## F

- false negatives, 58, 394
- false positives, 182, 394
  - benign triggers, 192
  - eliminating from vulnerability scanner alarms, 645–647
  - excluding, 759–762
  - IDSs (Intrusion Detection Systems), 55
- FAT (File Allocation Table), 121
- fault management, related tokens, 712–714
- fault tolerance, assigning multiple IP addresses per host, 715–716
- features of Catalyst 6000 IDS, comparing to traditional platforms, 491
- fields
  - Cisco Secure IDS alarm records
    - collapsing, 203–204
    - Count field, 181
    - destination information fields, 183
    - expansion boundaries, modifying, 204–205
    - general information fields, 181–182
    - signature information fields, 183–184
    - source information fields, 182
    - viewing, 180
  - event record fields, 740–746

- alarm event record fields, 741–744
- command event record fields, 744–746

- File Allocation Table (FAT), 121

- FilenameOfIPLog token, 711

- FilenameOfLog token, 711

- files, core dumps, 733

- Filtering Configuration Screen (CSPM), 400–403

- filtering signatures, 760

  - simple signature filtering, 444, 447

  - advanced signature filtering, 447–449

- finalization, CSPM installation, 134–136

- firewall sandwich configuration, sensors, 108

- firewalls, 37

  - IOS Firewall IDS signatures, 797–800

- Fix/Upgrade/Patch field (NSDB Related

  - Vulnerability page), 197

- FLOOD signature engines, 629, 633

- formats of IP session logs, 618

- forwarding alarms, related tokens, 710

- fragmentation, 391

  - IP signatures, 250–256

- FTP attacks, TCP signatures, 288–291

- FTP transfer, related tokens, 711

- functionality of nrConfigure, 556

## G

- gateways, entering sensors, 161–162

- general information fields (Cisco Secure IDS alarm records), 181–182

- general signature token, 702

- general signatures, 780–790

- General tab (CSPM), signature template

  - configuration, 428–429

- GET command, 293

- gigabit IDSM, 627

- globally disabling signatures, 590–591, 761–762

- goal setting for attacks, 11–12

- grep command, 237, 751

- groups

  - common privilege groups, defining, 35–36

  - users, 54

## H

- hacking tools

  - exploitation tools, 20

    - application holes, 23

    - authentication compromises, 21–22

    - back doors, 24

    - compromised trust relationships, 23–24

    - poorly configured services, 22

    - protocol weaknesses, 22

  - reconnaissance tools, 19–20

  - script kiddies, 7–8

  - user attributes, 7

- handlers, 27

- hardware

  - CSPM requirements, 123

  - installing RUs (rack units), 146

- hiding nrConfigure status line, 559

- hierarchical director design, 670

  - alarm delay limitations, 670

  - general setup, 671–675

  - network diagram, 670

  - required equipment, 670

  - troubleshooting tips, 675–678

- high ports versus low ports, 274

- High-severity alarms, 779

  - signatures, 239

- hijack attacks, TCP signatures, 307–309

- host names

  - PostOffice protocol, 88

  - resolving, 184–186

- host sweeps, TCP signatures, 277–280

- Host Type window, Add Host Wizard, 545

- host-based IDSs, 61

  - benefits, 62–63

  - drawbacks, 62–63

- hosts

  - /usr/nr/etc/hosts file entries, 714–715

  - authorized, 717

  - compromised trust relationships, 23

  - CSPM, adding to topology, 164–165

  - excluding from alarm reporting, 760

  - inclusions, 618

  - IP address configuration, 715–716

  - manual blocking operations, 483

  - population estimates, 98

  - secondary Directors, adding, 561

Windows NT 4.0 hosts, building, 125–126  
 host-to-host encryption, 40  
 HP Open View Network Node Manager (NNM).  
   *See* NNM (Network Node Manager)  
 HTML browser, configuring, 558  
 HTTP/Web signatures, 321–349  
 hubs, 101, 490  
 hybrid IDSs, 66

ICMP (Internet Control Message Protocol), 13, 257  
   attacks, 266  
   echo requests, 13  
   error messages, 262  
   ping sweeps, 264  
   query messages, 258  
   signatures, 257–268  
 Icon value (Event Viewer), configuring, 213  
 ID analysis, IDSM configuration, 501–507  
   assigning command and control port, 502  
   clearing unwanted VLAN traffic, 507–509  
 Ident protocol, attack signatures, 366–367  
 identification parameters  
   CSIDD, configuring, 532–534  
   sensors, 410–411  
   verifying on Director, 652  
 identifiers, PostOffice protocol, 87–89  
 identifying critical hosts, 467  
 IDS Module (IDSM). *See* IDSM (IDS Module)  
 IDS-4210 appliance, 4200 Series Sensors, 78,  
   148–149  
 IDS-4230 appliance, 4200 Series Sensors, 78,  
   146–147  
 ids-installer command, 518  
 IDSM (IDS Module), 79, 489–490, 620  
   adding to CSPM, 513  
   blades, configuring multiple per chassis, 678  
     general setup, 680–685  
     limitations, 678–679  
     network diagram, 680  
     VACL definition, 680  
   blocking with, 620  
   clearing unwanted VLAN traffic, 507

Diagnostic mode  
   commands, 521–523  
   enabling, 513  
 disk structure  
   active partition, 514  
   application partition, 515  
   maintenance partition, 515  
 images, updating, 515–516  
 initializing, 499–501  
 monitoring port, configuring as destination port,  
   503–505  
 oversubscription, preventing, 682  
 partitions, updating, 518  
 ports, 493–494  
 removing configuration, 513  
 requirements, 492  
 software files, 516  
   updating, 517–518  
 status LEDs, troubleshooting, 519  
 traffic, capturing, 490, 494–495  
   SPAN, 496  
   VACLs, 497–498  
   verifying configuration, 509–513  
 IDSM Sensing Configuration Screen (CSPM),  
   392–397  
 IDSM Setup utility, 499–501  
 IDSs (Intrusion Detection Systems), 53  
   Cisco Secure IDS  
     configuring, 72–76  
     functions and features, 72–76  
   false negatives, 58  
   host-based IDSs, 61  
     benefits, 62–63  
     drawbacks, 62–63  
   hybrid IDSs, 66  
   locations, monitoring, 61–66  
   network-based IDSs, 63–65  
     benefits, 65  
     drawbacks, 65–66  
   training preparation, 57  
   triggers, 54  
     anomaly detection, 54–58  
     misuse detection, 58–60  
 implementing  
   IP blocking, 466  
   signatures on Cisco IOS Firewall IDS, 581  
 improving network security, 44–46

- inclusion stance, security policies, 38
- inclusions, hosts, 618
- informational class signatures, 234
- infrastructure, topology analysis, 101
- initializing
  - Cisco IOS Firewall IDS, 583–589
  - HP Open View NNM environment, 537–539
  - IDS, 499, 501
- inserting comments in configuration files, 700
- install directory, 696
- installation
  - CSIDD, 531–535
    - configuration files, 535
    - Director script, running, 532
    - identification parameters, 532–534
    - install script, 532
    - netrangr password, 532–533
    - rebooting, 535
  - CSPM
    - 4200 Series Sensors, 145
    - account information, 129
    - basic settings, 129
    - Cisco Secure VPN Client, 125
    - configuring, 119–121
    - finalization, 134–136
    - license acceptance, 126–127
    - modes, 127–130
    - PostOffice protocol, 132–135
    - requirements, 121–124
    - settings, 124–136
    - TechSmith Screen Capture Codec, 131
  - RUs (rack units), 146
  - sensors, 103–111
  - version 3.0 enhancements, 614–615
  - version 4.0 enhancements, 620–622
- installed sensors, adding to Director
  - configuration, 560
- integrity of data, 11
- interesting traffic, defining, 498
- interfaces
  - ACL placement, 472–473
  - external, applying ACLs, 473
  - internal, applying ACLs, 473
  - Promiscuous mode, enabling, 752
  - sensors, 97
- internal networks
  - sensors, configuring, 412–413
  - token, 701
- internal threats, 9–10
- Internet Control Message Protocol (ICMP).  
*See* ICMP
- Internet
  - usage estimates, 98
  - entry points, sensors, 98–99
- Internet Protocol Security Architecture (IPSec),  
IP layer security, 110
- intranets, sensors
  - entry points, 99
  - placement, 105
- intrusion detection, configuration files, 700
- Intrusion Detection Systems (IDSs). *See* IDSs  
(Intrusion Detection Systems)
- IOS Firewall IDS signatures, 797–800
- IP addressing. *See also* IP blocking
  - ARP, 19
  - DNS, 13
  - Never Block Addresses, specifying, 478–479
- ip audit name command, 595
- ip audit po protected command, 587
- ip audit po remote command, 585
- ip audit signature command, 591
- IP blocking, 76, 463–464
  - anti-spoofing mechanisms, 466
  - at the router, 468–469
  - configuring, 474–476
  - critical hosts, 467
  - default block time, 470
  - disabling, 477–479
  - duration of, 468
  - entry points, 467
  - implementing, 466
  - manual blocking operations, 482–483
  - removing blocked hosts/networks, 483–484
  - signature selection, 467
  - viewing blocked addresses, 480–481
- IP fragments, configuring reassembly, 416–417
- IP layer security (IPSec), 110
- IP log files
  - formats, 618
  - naming conventions, 738
  - response actions, 76, 433

IP signatures (1000 Series signatures), 245  
     bad IP packets, 256–257  
     IP fragmentation, 250–256  
     IP options, 246–250  
 IPSec (Internet Protocol Security Architecture), IP  
     layer security, 110  
 ISDM, gigabit ISDM, 627

## J-L

Java Server Pages (JSPs), 339

laptops, connecting to sensors, 757–759  
 Last Modified column (nrConfigure screen  
     display), 558  
 LD\_LIBRARY\_PATH environment variable, adding  
     ORACLE\_HOME/lib, 730  
 LD\_LIBRARY\_PATH variable,  
     troubleshooting, 724  
 Legacy Cisco Secure IDS Web attacks, TCP  
     signatures, 291–303  
 Level field (Cisco Secure IDS alarm records), 184  
 levels, logging, 737–738  
 licensing CSPM, 123–124  
     acceptance, 126–127  
 limitations  
     of SPAN, 497  
     of VACLs, 498  
 limiting access, 36  
 line cards  
     Catalyst 6000 ISDM, comparing to  
         appliance, 491  
     ISDM, 489–490  
         adding to CSPM, 513  
         blades, configuring multiple per chassis,  
             678–685  
         capturing traffic, 490  
         Diagnostic mode, enabling, 513  
         disk structure, 514–515  
         ID analysis configuration, 501–509  
         images, updating, 515–516  
         initializing, 499, 501  
         monitoring port, configuring as  
             destination port, 503–505  
         partitions, updating, 518  
         ports, 493–494

    removing configuration, 513  
     requirements, 492  
     software files, 516–518  
     traffic flow, 494  
     verifying configuration, 509–513  
 links. defining untrusted, 39  
 Lite Licensing, CSPM, 124  
 Local Date field (Cisco Secure IDS alarm  
     records), 181  
 Local Time field (Cisco Secure IDS alarm  
     records), 181  
 location of HTML browser, selecting, 558  
 log files, 737  
     active log files, closing, 740  
     archived log files, 740  
     automatic FTP transfers, configuring, 415  
     Cisco Secure IDS log files, naming  
         conventions, 739  
     error log files, viewing, 756–757  
     event detection, verifying, 752  
     event record fields, 740–746  
         alarm event fields, 741–744  
         command event fields, 744–746  
     IP log files,  
         formats, 618  
         naming conventions, 738  
     locations, 740  
     logging levels, 737–738  
     naming conventions, 738–739  
     sensors  
         configuring, 414–416  
         generating, 414  
     Service Error log files, naming  
         conventions, 739  
     viewing, 179  
 loggerd.conf file, tokens, 711  
 logging  
     levels, 737–738  
     policy violations on ACLs, 653  
     related tokens, 710  
     troubleshooting, 726  
 Logging Configuration Screen (CSPM), 402–406  
 logons  
     4200 Series Sensors, 149–151  
     access attacks, 17  
     CSPM, 136  
     sensors, 757–759

Loki attack signatures, 370  
low ports, versus high ports, 274  
low-severity alarms, 779  
low-severity signatures, 238

## M

---

mail attacks, TCP signatures, 284–288  
mail server, configuring, 732  
mailing lists, security, 45  
mailx command, 732  
maintenance partition, 515  
managed network devices, viewing, 482  
managed.conf file

- DupDestination token, 709
- MinutesOfAutoShun token, 709
- NetDevice token, 708
- NeverShunAddress token, 709
- ShunInterfaceCisco token, 709

management access, 4200 Series Sensors, 149  
managing routers, 657

- general setup, 658–666
- limitations, 657
- network diagram, 658
- required equipment, 658
- troubleshooting tips, 666–669

man-in-the-middle attacks, 18  
manual IP blocking operations, 482–483  
manual monitoring, network security, 42  
MAPI (Messaging API), 122  
master blocking sensor, 470, 709  
Master Blocking Sensor Configuration Screen (CSPM), 400, 479  
master Director, adding additional secondary Directors, 561  
master signature parameters, 630  
maximum allowable alarms, 726  
Maximum Events Per Grid value (Event Viewer), configuring, 212  
maximum transmission units, 250, 391  
MaxInspectLength master signature parameter, 630  
MCI (Media Control Interface), 122  
Media Control Interface (MCI), 122  
Medium severity alarms, 779  
medium-severity signatures, 239  
messages, propagating through tiered Director hierarchy, 670–675  
Messaging API (MAPI), 122  
methodologies for attacks

- ad hoc attacks, 15
- methodical attacks, 15
- patient attacks, 16
- surgical strikes, 15

Microsoft Active Scripting Pages (ASPs), 339  
Microsoft Internet Explorer 5.x, CSPM, 122  
MinHits master signature parameter, 630  
minimizing trust relationships, 36  
MinutesOfAutoLog token, 711  
MinutesOfAutoShun token, 709  
misuse detection, IDSs (Intrusion Detection Systems), 58–60

- benefits, 59
- drawbacks, 59–60
- event horizons, 60

modifying

- connection signatures, 436
- database instance name, 730
- field expansion boundaries, 204–205
- Port Mapping configuration, 454–455

modules, platforms, 77–80  
monitoring

- locations, IDSs (Intrusion Detection Systems), 61–66
- security, 42–45

monitoring port, Catalyst 6000 IDSM, 494

- configuring as destination port, 503–505
- VACLs, building, 504–505

more command, 754–757  
MSFC, comparing to standalone routers, 492  
MTUs (maximum transmission units), 250, 391

## N

---

Name field (Cisco Secure IDS alarm records), 181  
NameOfPacketDevice token, 701  
naming conventions

- hosts, 714–715
- log files, 738–739
- organizations, 714–715

navigation buttons, HP OpenView NNM, 539–540  
NetBIOS attacks, TCP signatures, 303–307

- NetDevice token, 708
- netrangr account, 150, 532–533
- network function-based placement, sensors, 104–105
- Network Interface Name, verifying, 751
- Network Node Manager (NNM). *See* NNM (Network Node Manager)
- Network Topology tree (NTT), 82
- network-based IDSs, 63–65
  - benefits, 65
  - drawbacks, 65–66
- networks
  - attack points, 16
    - protocols, 18–19
    - resources, 16–17
  - resources
    - starvation attacks, 26
    - unsecured, 24
  - security
    - monitoring, 42
    - Security Wheel, 34–42
    - testing, 43–44
  - topology analysis, 97
    - critical components, 100–101
    - entry points, 98–100
    - remote networks, 102
    - security policy restrictions, 102–103
    - size and complexity issues, 102
- neutral networks, anomaly detection, 56
- Never Block Addresses, specifying, 478–479
- NeverShunAddress token, 709
- newly installed sensors, adding to Director
  - configuration, 560
- NNM (Network Node Manager), 531
  - environment initialization, 537–539
  - navigation buttons, 539–540
  - starting, 537
- non-sniffing sensors, troubleshooting, 749–757
- nr.fileXferd.conf, 690
- nr.loggerd.conf, 689
- nr.managed.conf, 689
- nr.packetd.conf, 689
- nr.postofficed.conf, 689
- nr.postofficed service (CSPM Director), 691
- nr.postofficed.conf, fault management, 712–714
- nr.sapd.conf, 689
- nr.smid service (CSPM Director), 691
- nrConfigure
  - Add Host Wizard, 561
  - Add Host Wizard Finished window, 564
  - configured sensors, adding to Director, 561–564
  - functionality, 556
  - HP-UX performance, troubleshooting, 733
  - HTML browser
    - configuring, 558
    - selecting location, 558
  - screen display, 556
    - columns, 558
    - hiding status line, 559
  - sensors
    - removing, 566
    - verifying installation, 565
  - starting, 556
  - troubleshooting, 733
- nrconns command, 522, 694, 753
- nrstart command, 693, 727
- nrstatus command, 536, 695, 750–751, 756
- nrstop command, 694, 727
- NSDB (Network Security Database)
  - Exploit Signature page, 190–191
    - benign triggers, 192
    - implementation, 192
    - recommended alarm level, 192
    - signature description, 192
    - signature ID, 191
    - signature name, 190
    - signature structure, 192
    - signature type, 192
    - subsignature ID, 191
    - user notes, 193
    - vulnerability, 193
  - HTML browser configuration, 733
  - opening, 189
  - Related Vulnerability page, 194
    - Advisory/Related Information Links field, 197
    - Affected Programs field, 196
    - Affected Systems field, 196
    - Alias field, 195
    - Consequences field, 196
    - Countermeasures field, 197
    - Exploit Links field, 197
    - Exploit Type field, 196



- Fix/Upgrade/Patch Links field, 197
- Severity Level field, 196
- User Notes field, 197
- Vulnerability Description field, 196
- Vulnerability ID field, 195
- Vulnerability Name field, 195
- Vulnerability Type field, 196

- NTT (Network Topology tree), 82
- numbering configuration versions, 570
- NumberOfSwitchBytes token, 711
- NumberOfSwitchMinutes token, 711
- nvers command, 696
- NXT resource record, 354

## O

---

- obtaining CSPM service versions, 218
- one-time passwords, 36
- online help, browser configuration, 733
- opening
  - Configuration Library, 568
  - Event Viewer, 178
  - NSDB, 189
- operating system requirements for CSPM, 121
- options, IP signatures, 246, 248–250
- Oracle database
  - instance name, modifying, 730
  - troubleshooting, 728
    - authorization, 731
    - installation, 728–729
    - JDBC-related error messages, 732
    - SQLPlus, 729
    - TNS error message, 731
  - USER/PASSWORD error message, troubleshooting, 731
- Organization Name field (Cisco Secure IDS alarm records), 182
- organization names
  - naming conventions, 714–715
  - PostOffice protocol, 88–89
- Organization/Host column (nrConfigure screen display), 558
- organizations file, 714
- orphaned FIN packets, 282
- out-of-bounds attacks, 26

- output fields
  - show config command, searching, 510
  - show span command, 511
- overflowing socket buffer, troubleshooting, 722
- oversubscription, preventing on IDSMs, 682

## P

---

- packet auditing process, 593–594
- packet capture device, sensor configuration, 413–414
- packet payload, 232
- packetd process, verifying, 750–751
- packetd.conf file
  - MinutesOfAutoLog token, 711
  - NameOfPacketDevice token, 701
  - RecordOfDataSource token, 707
  - RecordOfExcludedNetAddress token, 707–708
  - RecordOfFilterNameName token, 706–707
  - RecordOfInternalAddress token, 702
  - RecordOfStringName token, 704–705
  - SigOfFilterNameName token, 706
  - SigOfGeneral token, 702
  - SigOfStringName token, 704–705
  - SigOfTcpPacket token, 703
  - SigOfUdpPacket token, 703–704
- packets
  - bad IP packet signatures, 256–257
  - ICMP echo requests, 13
  - orphaned FIN packets, 282
  - packet payload, 232
  - sniffing, 64, 97
  - spoofing, 19
  - state information, 233
  - switch-forwarding path, 490–491
  - TTL value, 62
- parameters
  - apply command, 517
  - cvtnrlog command, 692
  - IDSM-specific, 501
  - ip audit name command, 597
  - PostOffice, 584–586
  - report systemstatus command (ISDM), 522
  - reset command (Catalyst), 520–521
  - set security acl ip command, 505
  - set trunk command, 508

- show errorfile command (ISDM), 523
- show module command (Catalyst), 520
- show port command (Catalyst), 520
- show security acl command, 512
- show span command, 510–511
- signatures
  - engine-specific parameters, 630
  - master signature parameters, 630
- tokens, 699
- partitions (ISDM), updating, 518
- passwords
  - crackers, 21
  - netrangr password, setting, 532–533
  - one-time, 36
  - Oracle database, troubleshooting, 731
  - telnetting to sensor COM port, 758
- patient attacks, 16
- patterns of traffic, determining, 37
- PCs, connecting to sensors, 757–759
- PDP (policy distribution point), 409
  - sensor selection, 166
- PEPs (policy enforcement points), 167–168
- perimeter protection, sensor placement, 104
- perimeter routers, 98
- permissions, troubleshooting, 722–723
- ping command, 750
- Ping of Death attack, 26
- ping sweeps, 13
  - ICMP, 264
- ping-R command, 248
- pings, 13
- PIX, blocking with, 619
- placement
  - of sensors
    - evaluating, 46
    - extranets, 104
    - intranets, 105
    - network function-based placement, 104–105
    - perimeter protection, 104
    - remote access servers, 105
  - of ACLs, 471–473
- platforms
  - modules, 77–80
  - sensors, 77–80
- policies (security). *See* security policies
- policy distribution point (PDP), 166, 409
- policy enforcement points (PEPs), 167–168
- policy violation signatures, 388
  - (10000 Series), 378
- policy violations, logging on ACLs, 653
- poorly configured services, 22
- port mapper, 355
- Port Mapping, 453, 455
- Port Mapping Configuration screen (CSPM), 396
- Port parameter (connection signatures), 434–435
- port scans
  - TCP signatures, 271–277
  - UDP signatures, 317
- ports
  - attacks on, 22
  - Catalyst 6000 ISDM, 493–494
  - high ports, 274
  - low ports, 274
  - switch-forwarding path, 490–491
- PostOffice
  - Command Timeout value, 209
  - connection status, verifying, 753
- PostOffice protocol, 84
  - addressing scheme, 89
  - benefits, 87
  - CSPM, installing, 132–135
  - fault tolerance, 86
  - features, 85
  - identifiers, 87–89
  - redundancy, 85
  - reliability, 85
  - sensor identification parameters, entering, 159–161
- postoffice.conf file
  - WatchDogInterval token, 713
  - WatchDogNumProcessRestarts token, 713
  - WatchDogProcDeadAlarmLevel token, 714
  - WatchDogProcTimeoutAlarmLevel token, 714
  - WatchDogResponseTimeout token, 713
- previously configured sensors, adding as host, 561
- privilege escalation attacks, 17
- professional security evaluations, conducting, 44
- profile-based detection. *See* anomaly detection
- Promiscuous mode, enabling on sniffing interface, 752
- propagating messages through tiered Director hierarchy, 670–675

- properties (signatures), defining severity of, 430–431
- protected networks, defining, 587–588
- protocols
  - ICMP (Internet Control Message Protocol), 257
  - PostOffice protocol, 84
  - weaknesses, 22
- proxy sensors, master blocking sensors, 470
- public data sources, attacks on, 12
- publishing attacks publicly, 57

## Q-R

---

- query messages (ICMP), 258
- rack units (RUs), 146
- RDBMS (relational database management systems), troubleshooting SQL queries, 732
- rebooting, 535
- recommended alarm level, 192
- reconnaissance for attacks, 12–13
- reconnaissance class signatures, 234
- reconnaissance tools, 19–20
- RecordOfDataSource token, 707
- RecordOfExcludedNetAddress token, 707–708
- RecordOfFilterName token, 706
- RecordOfStringName token, 704–705
- records (CSPM database)
  - fields
    - Count field, 181
    - Destination Information fields, 183
    - General Information fields, 181–182
    - Signature Information fields, 183–184
    - Source Information fields, 182
  - viewing, 179–180
- recovering deleted sensor configuration information, 567
- redirect command, 692
- reducing false-positive alarms, 759–762
- redundancy, multiple hosts per IP address configuration, 715–716
- regular expressions, sensors, 236
- Related Vulnerability page (NSDB), 194
  - Advisory/Related Information Links field, 197
  - Affected Programs field, 196
  - Affected Systems field, 196
  - Alias field, 195
  - Consequences field, 196
  - Countermeasures field, 197
  - Exploit Links field, 197
  - Exploit Type field, 196
  - Fix/Upgrade/Patch Links field, 197
  - Severity Level field, 196
  - User Notes field, 197
  - Vulnerability Description field, 196
  - Vulnerability ID field, 195
  - Vulnerability Name field, 195
  - Vulnerability Type field, 196
- relationships (trust relationships), minimizing, 36
- remote access entry points, sensors, 99
- remote access servers, sensor placement, 105
- Remote Procedure Call (RPC), 355–366
- remote reconnaissance, 12–13
- remote sensor configuration, 110
- removing
  - alarms, 197–198
  - blocked hosts/networks, 483–484
  - columns in Event Viewer, 205
  - ISDM line card configuration, 513
  - saved configuration versions, 571–572
  - sensor icon from Cisco Secure IDS Home submap, 567
  - sensors from nrConfigure Director, 566
- reorganization of corporate networks, troubleshooting, 648–650
- report system status command (ISDM), 522
- reporting SYSLOG files to sensor, 650
  - general setup, 651–655
  - limitations, 650
  - network diagram, 651
  - required equipment, 650
  - troubleshooting tips, 656–657
- repositioning columns in Event Viewer, 205
- requirements
  - Catalyst 6000 ISDM line card, 492
  - device management, 465
- reset command (Catalyst), 520–521
- Reset Statistics window (Event Viewer), 220
- ResetAfterIdle master signature parameter, 630
- resolving host names, 184–186
- resource records, 354

- resources
    - unsecured, 24
    - vulnerability to attacks, 16–17
  - responses
    - to alarms, Director platforms, 81
    - to signatures, CSIDD configuration, 665–666
  - restricting access, 36
  - resuming alarm display (Event Viewer), 199–200
  - review questions, answers, 815–835
  - reviewing configuration files periodically, 45
  - root installation directory, 696
  - routers
    - managing, 657
      - general setup, 658–666
      - limitations, 657
      - network diagram, 658
      - required equipment, 658
      - troubleshooting tips, 666–669
    - perimeter routers, 98
  - routes file, 715–716
  - rows, deleting from CSPM database, 199
  - RPC (Remote Procedure Call), attack signatures, 355–366
  - rule-based approach, anomaly detection, 55
  - RUs (rack units) installations, 146
- ## S
- 
- SAPD (Security Analysis Package Daemon), 689
  - SAPI (Speech API), 122
  - SATAN (Security Analysis Tool for Auditing Networks), 349–350
  - saved versions, deleting, 571–572
  - saving
    - configuration versions, 571
    - sensor configurations, 166–167, 421
  - scanners (security), 43–44
  - screen display, nrConfigure, 556
    - Organization/Host column, 558
    - status line, hiding, 559
  - script kiddies, 7–8
  - scripts
    - start.sh, 729
    - sysconfig-director, HTML browser configuration, 558
    - sysconfig-sensor, 150, 410, 540
      - exiting, 158
  - SDM (Sensor Device Manager), 628
  - searching show config command output, 510
  - secondary Directors, adding, 561
  - Secure IDS
    - communications deployment worksheet, 803–805
    - submap, verifying sensor installation, 566
  - security
    - authentication, improving, 35–36
    - boundaries, establishing, 37–39
    - confidentiality, VPNs, 39–41
    - configuration, verifying, 46
    - configuration files, reviewing, 45
    - firewalls, 37
    - improving, 44–46
    - mailing lists, 45
    - monitoring, 42
    - news, monitoring, 44–45
    - professional evaluations, conducting, 44
    - security policies, 34, 38
    - security scanners, 43–44
    - security wheel, 34–42
    - security zones, defining, 38
    - sensors, placement of, 46
    - testing, 43–44
    - vulnerability patching, 41–42
    - Web sites, 45
  - Security Analysis Tool for Auditing Networks (SATAN), 349–350
  - security policies, 10–11, 33
    - stances, 38
  - security scanners, 43–44
  - Security Wheel, 34–42
    - improving security, 44–46
    - monitoring security, 42
    - testing security, 43–44
  - security zones, defining, 38
  - selecting
    - columns for display (Event Viewer), 207
    - HMTL browser location, 558
    - multiple signatures for advanced filtering, 448
  - semaphore files, troubleshooting, 723–724
  - Sensor Advanced Configuration Screen (CSPM), 404
  - sensor appliance, 625–628

- Sensor CA (control agent), 691
- Sensor Command Configuration screen (CSPM), 406–409
- Sensor Device Manager (SDM), 628
- Sensor Identification dialog box, 159
- Sensor Internal Networks Configuration screen (CSPM), 389
- Sensor Monitoring Configuration screen (CSPM), 388
- Sensor Name field (Cisco Secure IDS alarm records), 182
- Sensor Properties Configuration screen (CSPM), 387
- Sensor Statistics window (Event Viewer), 219
- sensors
  - 4200 Series Sensors
    - appliances, 145
      - IDS-4210, 148–149
      - IDS-4230, 146–147
    - configuring, 151–158
    - CSPM, 145
    - logon accounts, 149–151
    - management access, 149
  - ACL signatures, creating, 455–456
  - adding, CSIDD, 541–542, 544–549
  - adding to Director configuration, 560–561
  - alarm logging, troubleshooting, 726
  - blocking, 100
  - Cisco Secure IDS, architecture, 687–690
  - COM port settings, configuring, 759
  - communication with Director, verifying, 753–754
  - configuration files, pushing to, 167–168
  - configuring
    - advanced changes, 416–420
    - basic changes, 410–414
    - checking, 168–169
    - CSIDD, 540–549
    - CSPM, 385–394, 396–421
    - CSPM sensor configuration screens, 386–409
    - error checks, 421
    - identification parameters, 410–411
    - internal networks, 412–413
    - IP fragment reassembly, 416–417
    - log files, 414–416
    - packet capture device, 413–414
    - pushing new ones to, 420–421
    - saving, 166–167, 421
    - TCP session reassembly, 417–419
    - updating, 166–167, 421
  - default gateway, entering, 161–162
  - deploying, preparation for, 97–103
  - destinations file, viewing, 754
  - device management, 465
    - configuring, 661–666
    - requirements, 465
  - enhancements, 625–628
    - sensor appliance, 625–628
  - entry points, 98
    - Internet entry points, 98–99
    - intranet entry points, 99
    - remote access entry points, 99
  - error log files, viewing, 756–757
  - installing, 103–111
  - interfaces, 97
  - logging into, 757–759
  - master blocking sensors, 470, 709
  - maximum allowable alarms,
    - troubleshooting, 726
  - non-sniffing, troubleshooting, 749–757
  - packetd process, verifying, 750–751
  - packet sniffing, 97
  - PDP (policy distribution point), selecting, 166
  - placement
    - evaluating, 46
    - extranets, 104
    - intranets, 105
    - network function-based placement, 104–105
    - perimeter protection, 104
    - remote access servers, 105
  - platforms, 77–80
  - PostOffice identification parameters, entering, 159–161
  - previously configured, adding to Director, 561, 563–564
  - regular expressions, 236
  - remote configuration, Director platforms, 81
  - removing from nrConfigure Director, 566
  - removing icon from Cisco Secure IDS Home submap, 567
  - routing threshold, troubleshooting, 725
  - SDM (Sensor Device Manager), 628

- Secure IDS submap installation, verifying, 566
  - settings, verifying, 163
  - severity status, troubleshooting, 725
  - signature templates, 439
    - assigning, 442
    - creating, 440
    - entering, 162–163
  - signatures, 231
    - advanced configuration, 451, 453, 455
    - advanced filtering, 447–449
    - applying actions, 433–434
    - atomic signatures, 233
    - classes, 234–235
    - composite signatures, 233
    - connection signatures, 434–435, 791–793
    - content-based signatures, 232
    - context-based signatures, 232
    - enabling/disabling, 431–432
    - filtering, 444, 447
    - general signatures, 780–790
    - globally disabling, 761–762
    - implementations, 765–776
    - implementing, 232–233
    - policy violation signatures, 388
    - severity, 237–239
    - severity levels, viewing, 750
    - string signatures, 437–438, 794
    - structures, 233, 765–776
    - types, 235–237
  - stateful sensors, 622
  - statistics, resetting, 220
  - transparent stateful sensors, 622
  - verifying nrConfigure installation, 565
- servers, topology analysis, 100
- Service Error log files, naming conventions, 739
- service packs (IDSM), updating, 517–518
- SERVICE signature engines, 629
- Service Status window (Event Viewer), 216–218
- Service Versions window (Event Viewer), 218
- services
  - application ID, 718–719
  - Cisco Secure IDS, 688–689
    - starting, 693
    - stopping, 694
    - verifying operability, 695
  - configuration files, 699–700
  - CSPM Director, 691–692
    - fault management, related tokens, 713–714
  - session command, 499
  - set boot device command, 514
  - set security acl ip command, 504–505
  - set span command, 503
  - set trunk command, 508
  - severity of signatures, 237
    - high-severity, 239
    - low-severity, 238
    - medium-severity, 239
  - Severity field (Cisco Secure IDS alarm records), 184
  - Severity Level field (NSDB Related Vulnerability page), 196
  - Severity Mapping group box (Event Viewer Preferences window), 213
  - show config command, 509–510
  - show configuration command, 513
  - Show Current Events window (Director), troubleshooting, 726
  - show errorfile command (IDSM), 523
  - show ip audit configuration command, 643
  - show ip audit debug command, 600
  - show ip audit interface command, 600, 644
  - show ip audit statistics command, 599
  - show module command (Catalyst), 520
  - show port command (Catalyst), 520
  - show security acl command, 511
  - show span command, 510–511
  - Show Status Events in Grid status event, 212
  - ShunInterfaceCisco token, 708
  - shunning, enhancements
    - version 3.0, 618–620
    - version 4.0, 624
  - Shunning Hosts pop-up window (Event Viewer), 483
  - Shunning Initialization window, Add Host Wizard, 548
  - SIG resource record, 354
  - SIGID master signature parameter, 630
  - signature engines, 628–629
  - Signature ID field (Cisco Secure IDS alarm records), 184
  - signature information fields (Cisco Secure IDS alarm records), 183–184
  - Signature Parameter Editor, 453
  - signature templates, 439
    - applying to sensor, 442
    - assigning to sensors, 442

- configuring
  - General tab (CSPM), 428–429
  - Signatures tab (CSPM), 429
- creating, 440
- sensors, entering, 162–163
- viewing, 428
- Signature Tuning, 451–453
- Signature Tuning Parameters Screen (CSPM), 396
- signature-based detection, 58–60
- signatures, 231, 245, 268. *See also* ACLs
  - actions, configuring, 433–434
  - advanced configuration, 451
    - Port Mapping, 453, 455
    - Signature Tuning, 451, 453
  - advanced filtering, 447–449
  - atomic, 233, 581
  - audit rules, creating, 595, 597–598
  - benign, 238
  - classes, 234–235
    - access class signatures, 235
    - denial of service class signatures, 235
    - informational class signatures, 234
    - reconnaissance class signatures, 234
  - composite, 233
  - compound, 581
  - configuring on Cisco IOS Firewall IDS, 589–592
  - connection, 434–435, 617, 791–793
    - adding, 435–436
    - modifying, 436
  - content-based, 232
  - context-based, 232
  - cross-protocol (6000 Series), 349
    - authentication failures, 367–369
    - DDoS attacks, 371–374
    - DNS attacks, 351–354
    - Ident attacks, 366–367
    - Loki, 370
    - RPC attacks, 355–366
    - SATAN attacks, 349–350
  - default actions, setting, 594
  - definitions, 631
  - disabling, 431–432
  - excluding, 591–592
  - Exploit Signature page (NSDB)
    - benign triggers, 192
    - implementation, 192
    - opening, 191
    - recommended alarm level, 192
    - signature description, 192
    - signature ID, 191
    - signature name, 190
    - signature structure, 192
    - signature type, 192
    - subsignature ID, 191
    - user notes, 193
    - vulnerability, 193
  - false positives, 182
  - filtering
    - advanced, 447–449
    - simple, 444, 447
  - flood signatures, 633
  - general, 780–790
  - globally disabling, 590–591, 761–762
  - ICMP, 257–268
  - implementations, 232–233, 581, 765–776
  - IOS Firewall IDS signatures, 797–800
  - IP signatures, 245
    - bad IP packets, 256–257
    - IP fragmentation, 250–256
    - IP options, 246–250
  - parameters
    - engine-specific parameters, 630
    - master signature parameters, 630
  - policy violation signatures, 378, 388
  - severity, 237–239
    - defining, 430–431
    - high-severity, 239
    - low-severity, 238
    - medium-severity, 239
    - viewing, 750
  - signature engines, 628–629
  - SPAM, configuring on Cisco IOS Firewall IDS, 589–590
  - string, 632, 794
    - configuring, 437–438
    - creating, 438
  - string-matching, 375–378
  - structure, 192, 233, 765–776
  - Sweep signatures, creating, 631
  - TCP signatures
    - abnormal TCP packets, 281–283
    - applications, 309–315
    - FTP attacks, 288–291

- hijack attacks, 307–309
- host sweeps, 277–280
- Legacy Cisco Secure IDS Web attacks, 291–303
- mail attacks, 284–288
- NetBIOS attacks, 303–307
- port scans, 271–277
- SYN flood attacks, 307–309
- traffic records, 269–271
- thresholds, configuring, 616
- tuning, 760–762
- types, 235–237
  - ACLs (access control lists), 237
  - connection signatures, 236
  - general, 235–236
  - string signatures, 236
- UDP signatures (4000 Series), 316
  - applications, 319–321
  - attacks, 318–319
  - port scans, 317
  - traffic records, 316–317
- user defined signatures, 617, 628–633
- version 3.0 enhancements, 616–618
- version 4.0 enhancements, 623–624
- Web/HTTP signatures (5000 Series), 321
  - Web attacks, 322–349
- Signatures tab (CSPM), signature template configuration, 429
- SigOfFilterName token, 706
- SigOfStringMatch token, 704–705
- SigOfTcpPacket token, 703–704
- SigOfUdpPacket token, 703–704
- simple signature filtering, configuring, 444, 447
- site-to-site encryption, 41
- smid process, verifying on Director, 754, 756
- smid.conf file (DupDestination token), 710
- SMTP (Simple Mail Transfer Protocol) attacks, 284–288
- sniffing packets, 64, 97
- snoop command, 150
  - Solaris, 752
- software
  - CSPM
    - feature sets, 118–119
    - requirements, 121
  - IDS, 516–518
  - Solaris snoop command, 752
  - sorting columns in Event Viewer, 207
  - Source Address field (Cisco Secure IDS alarm records), 182
  - source information fields (Cisco Secure IDS alarm records), 182
  - Source Location field (Cisco Secure IDS alarm records), 182
  - Source Port field (Cisco Secure IDS alarm records), 182
  - SPAM signature, configuring on Cisco IOS Firewall IDS, 589–590
  - SPAN feature (Catalyst 6000 IDSM), 490
    - limitations, 497
    - spanning ports, 496
    - spanning VLANs, 496
  - specifying Never Block Addresses, 478–479
  - Speech API (SAPI), 122
  - spoofing attacks, 19
  - SQL queries, troubleshooting, 732
  - SQLPlus, troubleshooting, 729
  - stances on security policies, 38
  - standalone configurations
    - CSPM, 120
    - sensors, 106
  - standalone routers versus MSFC, 492
  - standard deviation, calculating, 55
  - start.sh script, 729
  - starting
    - Add Host Wizard, 543
    - Cisco Secure IDS daemon, 727
    - Cisco Secure IDS services, 693
    - CSIDD, 536–538, 540
    - HP OpenView NNM, 537
    - nrConfigure, 556
  - state information, packets, 233
  - stateful sensors, 622
  - statistical sampling, anomaly detection, 55
  - statistics, resetting for sensors, 220
  - Status Events group box (Event Viewer Preferences window), 211
  - status LED (IDSM), troubleshooting, 519
  - stopping
    - Cisco Secure IDS daemon, 727
    - Cisco Secure IDS services, 694
  - STRING signature engine, 629



- string signatures, 236, 632, 794
  - configuring, 437–438
  - creating, 438
- string-matching signatures(8000 Series), 375
  - custom, 375
  - TCP application signatures, 375–378
- structured attacks, 9
  - methodical, 15
  - patient attacks, 16
  - surgical strikes, 15
- structure of signatures, 765–776
- submaps (Director), 538
- Subnet Mask value, configuring, 209
- SubSig master signature parameter, 630
- subsignature ID, 191
- subsignature indicators, 448
- SUID file permission bit, 723
- support applications, CSPM, 122
- surgical strike attacks, 15
- suspending alarm display (Event Viewer), 199–200
- sweep signature engines, 629
- sweep signatures, creating, 631
- switches, Catalyst 6000 IDSM, 489–490, 492
  - capturing traffic, 495–498
  - commands, 509–512
  - comparing to traditional platforms, 491
  - ports, 493–494
  - traffic flow, 494
- switch-forwarding path, 490–491
- SYN flood attacks, 26
  - TCP signatures, 307–309
- sysconfig-director script, HTML browser
  - configuration, 558
- sysconfig-sensor command, 152–158
- sysconfig-sensor script, 150, 410, 540
  - exiting, 158
- SYSLOG files
  - defining for ACL signature administration, 456–457
  - reporting to sensors, 650
    - general setup, 651–655
    - limitations, 650
    - network diagram, 651
    - required equipment, 650
    - troubleshooting tips, 656–657

## T

---

- tail command, 81
- tail -f command, 753
- TAPI/MAPI (CSPM), 122
- TCP (Transmission Control Protocol), 73
  - application signatures, 375–378
  - reassembly, configuring, 417–419
  - reset action, 72–74, 433
  - traffic records, 269
- TCP signatures (3000 Series), 268
  - abnormal TCP packets, 281–283
  - applications, 309–315
  - FTP attacks, 288–291
  - hijack attacks, 307–309
  - host sweeps, 277–280
  - Legacy Cisco Secure IDS Web attacks, 291–303
  - mail attacks, 284–288
  - NetBIOS attacks, 303–307
  - port scans, 271–277
  - SYN flood attacks, 307–309
  - traffic records, 269–271
- tcpdump, 618
- TechSmith Screen Capture Codec, CSPM
  - installation, 131
- Telephony Application Programming Interface (TAPI), 122
- Telnet
  - connecting to sensor COM port, 758
  - enabling, 466
- templates, 439
  - assigning to sensors, 442
  - configuring
    - General tab (CSPM), 428–429
    - Signatures tab (CSPM), 429
  - creating, 440
  - signatures, disabling/enabling, 431–432
- temporary exclusions (alarms), 762
- testing network security, 43–44
- threats to security, 6–7
  - ad hoc attacks, 15
  - attacker attributes, 7
  - distributed attacks, 27, 29
  - DoS attacks
    - out-of-bounds attacks, 26
  - external, 9

- goal setting, 11–12
- host resource starvation attacks, 26
- internal, 9–10
- methodical attacks, 15
- network attack points, 16
  - network protocols, 18–19
  - network resources, 16–17
- network resource overload, 25
- reconnaissance attacks, 12–13
- slow attacks, 16
- structured, 9
- surgical strike attacks, 15
- unstructured, 7–8
- thresholds (signatures), tuning, 616
- ThrottleInterval master signature parameter, 630
- tiered director hierarchy, 670
  - alarm delay limitations, 670
  - general setup, 671–675
  - network diagram, 670
  - required equipment, 670
  - troubleshooting tips, 675–678
- Time To Block value, configuring, 209
- tooggling nrConfigure status line, 559
- tokens, 699
  - DupDestination, 710
  - FilenameOfIPLog, 711
  - FilenameOfLog, 711
  - general signature, 702
  - internal network, 701
  - MinutesOfAutoLog, 711
  - MinutesOfAutoShun, 709
  - NameOfPacketDevice, 701
  - NetDevice, 708
  - NeverShunAddress, 709
  - NumberOfSwitchBytes, 711
  - NumberOfSwitchMinutes, 711
  - RecordOfDataSource, 707
  - RecordOfExcludedNetAddress, 707–708
  - RecordOfFilterName, 706
  - RecordOfStringName, 704–705
  - ShunInterfaceCisco, 708
  - SigOfFilterName, 706
  - SigOfStringMatch, 704–705
  - SigOfTcpPacket, 703–704
  - SigOfUdpPacket, 703–704
  - WatchDogInterval, 713
  - WatchDogNumProcessRestart, 713
  - WatchDogProcDeadAlarmLevel, 714
  - WatchDogProcTimeOutAlarmLevel, 714
  - WatchDogResponseTimeout, 713
- tools for hacking
  - exploitation tools, 20
    - application holes, 23
    - authentication compromises, 21–22
    - back doors, 24
    - compromised trust relationships, 23
    - poorly configured services, 22
    - protocol weaknesses, 22
    - reconnaissance tools, 19–20
- Tools menu (CSPM), View Sensor Events
  - command, 178
- topology
  - analysis, 97
    - critical components, 100–101
    - entry points, 98, 100
    - remote networks, 102
    - security policy restrictions, 102–103
    - size and complexity issues, 102
  - CSPM, adding to, 164–165
- TRACEON command, 320
- traffic
  - capturing, 495
    - SPAN feature (IDSM), 496
    - VACLs, 497–498
  - capturing with IDSM, 490
  - extended ACLs, applying to inbound
    - traffic, 464
  - manual blocking, 482–483
  - overloaded sensors, troubleshooting, 656–657
  - packetd process, verifying, 750–751
  - patterns, determining, 37
  - records
    - TCP, 269
    - TCP signatures, 269–271
    - UDP signatures, 316–317
  - security policies, 10–11
  - statistics, viewing, 219
  - switch-forwarding path, 490–491
  - to IDSM line card, 494
  - transferring hubs, 101
  - VLANs, clearing from IDSM, 507

- transient configuration versions, 569–570
  - applying, 571
  - numbering, 570
  - saving, 571
- Transmission Control Protocol (TCP). *See* TCP
- transparent stateful sensors, 622
- triggers, 248
  - benign, 192
  - context buffer, viewing, 187, 189
  - IDSs (Intrusion Detection Systems), 54
    - anomaly detection, 54–58
    - misuse detection, 58–60
- Trojan horse programs, 17
- troubleshooting
  - Cisco IOS Firewall IDS, debug commands, 601
  - Director
    - inability to write to socket, 722
    - LD\_LIBRARY\_PATH variable, 724
    - maximum allowable alarms, 726
    - overflowing socket buffer, 722
    - permissions, 722–723
    - semaphore files, 723–724
    - sensor alarm logging, 726
    - sensor routing threshold, 725
    - sensor severity status, 725
    - Show Current Events window, 726
  - duplicate alarms, 675
  - IDS/MS, status LEDs, 519
  - non-sniffing sensors, 749–754, 756–757
  - nrConfigure, 733
  - Oracle database, 728
    - authorization, 731
    - installation, 728–729
    - JDBC-related error messages, 732
    - passwords, 731
    - SQLPlus, 729
  - RDBMS, SQL queries, 732
  - reorganization of corporate networks, 648–650
  - sensors, Cisco Secure IDS daemon
    - services, 727
- trust relationships, 17
  - compromised, 23
  - minimizing, 36

- tuning signatures
  - reducing false-positive occurrences, 759–762
  - thresholds, 616
- Type parameter (connection signatures), 434–435

---

## U

- UDP signatures (4000 Series), 316
  - applications, 319–321
  - attacks, 318–319
  - port scans, 317
  - traffic records, 316–317
- UNIX, core dumps, 733
- Unlimited Licensing, CSPM, 124
- unsecured resources, 24
- unstructured attacks, ad hoc, 15
- unstructured threats, 7–8
- untrusted links, defining, 39
- updating
  - IDS/MS
    - images, 515–516
    - partitions, 514–515, 518
    - software files, 517–518
    - sensor configurations, 166–167, 421
- usage estimates, Internet, 98
- user accounts, access attacks, 17
- user-defined signatures, 617, 628–633
- user groups, 54
- User Notes field (NSDB Related Vulnerability page), 197
- utilities
  - cvtnrlog.exe, 692
  - IDS/MS Setup, 499, 501

---

## V

- VACL (VLAN ACL) feature
  - capturing traffic, 497
  - Catalyst 6000 switches, 490
- var directory, 698
- variable time-to-live attacks, 63

## verifying

- Cisco IOS Firewall IDS configuration, 598–601, 643–644
- event detection, 752
- identification parameters on Director, 652
- IDSM configuration, 509–513
- Network Interface Name, 751
- nrConfigure sensor installation, 565
- operability of Director/sensor link, 694
- Oracle database installation, 728–729
- packetd process, 750–751
- Secure IDS submap sensor installation, 566
- security configuration, 46
- sensor/Director communication, 753–754
- smid process on Director, 754, 756

## version 3.0 (Cisco IDS), 614–620

- configuration enhancements, 614–615
- enhancements, shunning, 61–620
- installation enhancements, 614–615
- signatures enhancements, 616–618

## version 4.0 (Cisco IDS), 620–625

- blocking enhancements, 624
- configuration enhancements, 620–622
- installation enhancements, 620–623
- signature enhancements, 623–624

## versions

- applying, 571
- deleting, 571–572
- numbering, 570
- saving, 571

## viewing

- ACL contents, 511
- alarm fields, 180–184
- blocked IP addresses, 480–481
- collapsed fields in Event Viewer, 201–202
- context buffer, 187, 189
- CSPM database entries, 178
- error log files, 756–757
- log files, 179
- managed network devices, 482
- sensor destinations file, 754
- sensor statistics, 219
- signature severity levels, 750
- signature template, 428

Virtual Private Networks (VPNs). *See* VPNs

## VPNs

- confidentiality, providing, 39–41
- encryption, 39
  - host-to-host encryption, 40
  - site-to-site encryption, 41
- endpoints, defining, 40–41

## VRFY command, 233

Vulnerability Description field (NSDB Related Vulnerability page), 196

Vulnerability ID field (NSDB Related Vulnerability page), 195

Vulnerability Name field (NSDB Related Vulnerability page), 195

vulnerability scanners, troubleshooting false positives, 644–647

## vulnerability to attacks

- network attack points, 16
  - network protocols, 18–19
  - network resources, 16–17
- patching, 41–42

Vulnerability Type field (NSDB Related

Vulnerability page), 196

---

## W-Z

war-dialers, 105

WatchDogInterval token, 713

WatchDogNumProcessRestarts token, 713

WatchDogProcDeadAlarmLevel token, 714

WatchDogProcTimeOutAlarmLevel token, 714

WatchDogResponseTimeout token, 713

Web sites, security, 45

Web/HTTP signatures (5000 Series), 321

Web attacks, 322–349

well-known ports, attacks on, 22

Whack-a-Mole, 24

Windows NT hosts, building, 125–126

wizards

Add Host Wizard, 541–549

Add Sensor Wizard, 159–160

write memory command, 653