



SYMBOLS

! command (Telnet), 53
! negation operator, 443
(pound symbol), 23, 432
* (asterisk), 67
- (hyphen), 84, 464
/ (slash), 24, 49
: (colon), 39
? command, 474
 telnet, 53
 tn-gw, 441
-4 option (opiekey), 562
-5 option (opiekey), 562
2600 Magazine, 135

A

-A option (netstat), 41
-a option
 arp, 46
 netstat, 41, 43
 opiekey, 562
 ruptime, 37

A security level, 62
ABOR command (FTP), 558, 569
Acceptable Use Policy (AUP), 109-111
access control programs, *see* InterLock;
 netac!; TCP Wrapper
Access Control Rule Base (ACRB),
 382, 385-387
access, granting, 111-115
access files
 /etc/hosts.equiv, 26-28
 .rhosts, 26-28
access lists
 defining, 238-239
 extended access lists, 240-243
 standard access lists, 239-240
access points, 125-127
access-class line configuration
 command, 243
accounts, managing, 134-135, 521-523
ACCT command (FTP), 558, 569
ACK flag, 212-215
 FTP (File Transfer Protocol), 268
 packet filters, 231



- ACRB (Access Control Rule Base), 382, 385-387
- activity management, session layer (OSI Model), 222-223
- Add button (Black Hole), 522
- Add command (Edit menu), 523, 531
- adding
 - icons, Black Hole, 527
 - MX (mail exchanger) records, 459-460
 - NNTP (Network News Transfer Protocol) client requests, 483
 - passwords, 69
 - users
 - authserv (authentication server)*, 472-480
 - Black Hole*, 523
- address spoofing (packet filtering), 143, 244-245
- Address table (Black Hole), 515
- addresses
 - IP (Internet Protocol), 9-18
 - classes*, 10-12
 - netmasks*, 12-15
 - notations*, 10-18
 - prefixes (CIDR)*, 16
 - spoofing*, 506
 - reserved, 11-12
- adduser username [longname]
 - command, 472
- administration commands, 32-48
 - arp, 45-47
 - dig, 47-48
 - finger, 39-40
 - ifconfig, 38-39
 - netstat, 40-44
 - ping, 33-36
 - uptime, 36-37
 - rwho, 37
 - traceroute, 44-45
- administrator commands, authserv, 472-474
- aging passwords, 72-75, 115
- Alarm system (Black Hole), 508
- alerting FireWall-1 packet filtering, 362
- algorithms
 - crypt(3), 88-89
 - Message Digest
 - MD4*, 162
 - MD5*, 163
- ALL keyword (TCP Wrapper), 358
- all option (Makefile), 172
- ALLO command (FTP), 558-569
- allow command (Drawbridge packet filter), 314-315
- Allow option (Transfer rule component), 516
- allow table (Drawbridge packet filter), 309
- analyzing traffic, 508
- anonymous FTP, 54-55, 560
 - configuring, 180-181
 - Gauntlet, 402-403
 - TIS Firewall Toolkit, 416-417
- ANS (Advanced Network Services)
 - InterLock, *see* InterLock
- APIs (application programming interfaces), 223
- APPE command (FTP), 558, 569
- application layer (OSI Reference Model), 223-224
 - dual-homed firewalls, 329-331
- application programming interfaces (APIs), 223
- application-level gateways, 350-354
 - circuit-gateways, 353-354
 - custom programs, 351-354



- proxy applications, 352-354
 - special-purpose code, 351
- applications, *see* software
- architecture, Firewall-1, 359-362
- ARP cache table, 341
- arp option (ifconfig), 20
- arp utility, 45-47
- ARPANET, 8
- ASCII dump file, 478
- ASN.1 (Abstract Syntax Representation, Rev 1), 223
- assembling netperm tables (TIS Firewall Toolkit), 431-433
- assigning
 - domains, 17
 - host names, 17-18
 - passwords, 475
- asterisk (*), 67
- Athena Widget set, 467
- audits, 61
 - FireWall-1 packet filtering, 362
 - InterLock, 380
 - network security, 112
 - Unix, 80
- AUP (Acceptable Use Policy), 109-111
- auth option
 - ftp-gw, 451
 - host access rules, 443
- authdump command, 477-479
- authenticating users
 - authserv, 475
 - Black Hole, 524-526
 - ftpd, 570
 - opieftpd, 560
 - TIS Firewall Toolkit, 418-420
- authentication server, *see* authserv
- authentication systems (encryption), 145-146
 - Kerberos, 91-92

- Authentication_List, 385
- authload command, 420, 478-479
- authmgr program, 476-477
- authserv (authentication server), 418-420, 467-480
 - authmgr program, 476-477
 - Black Hole, 507
 - commands
 - administrator*, 472-474
 - authdump*, 477
 - authload*, 478
 - compiling, 468
 - configuring, 419-420, 468
 - database, 478-479
 - passwords, assigning, 475
 - protocols, 475
 - reports, 491-492
 - rules, 420, 469-499
 - TIS Firewall Toolkit, 468
 - users, 468-480
 - adding*, 472-476
- authserver hostname option
 - rlogin-gw, 446
 - tn-gw, 439
- authserver rule, 469
- authsrv command, 471-472
- authsrv-summ.sh, 491

B

- b option (finger utility), 40
- b file type (Unix), 84
- B security level, 62
- backbone routers, CIDR (Classless Inter-Domain Routing), 16
- backups, 136-139
 - System Backup option (Gauntlet), 399



- baddir pathname option (smapd), 458
- badsleep seconds rule (authserv), 470
- Baseline Software, 555
- bastion hosts, 335-346
 - configuring, 343-346
 - deploying, 336
 - IAP (Internet Access Provider) packet filtering, 337-338
 - notation, 336
 - screened host gateways, 336-337
 - routing configuration*, 339-343
 - TIS Firewall Toolkit, 408-409
- BBN (Bolt Beranek and Newman, Inc.), 8
- Bellcore
 - URL, 163
 - mailing list, 553
 - see also* S/Key
- Berkely r utilities
 - rcmd, 51-52
 - rcp, 49-50
 - rlogin, 48-49
 - rsh, 50-51
- bi-network interface configuration, 343-344
- /bin/login file, 196-198
- bit-oriented netmasks, 15
- bits
 - octets, 13-15
 - permissions, 84
- Black Hole, 501-541, 556
 - advantages, 501-504
 - configuration, 528-537
 - DNS (Domain Name Service)*, 528-530
 - proxy agents*, 531-541
 - core modules, 506-509
 - Alarm system*, 508
 - DuhMail*, 508
 - Guardian*, 507
 - Oracle*, 507
 - proxy agents*, 507-508
 - report generator*, 508-509
 - extensions, 509
 - icons, adding, 527
 - interface, 512-514
 - kernal modifications, 506-507
 - log file, 513
 - network design, 510-512
 - reports, 537-540
 - Bytes Per Port*, 540
 - Connections Per Host*, 539-540
 - Top 10 Destinations*, 540
 - Total Bytes In/Out*, 539
 - Transactions Per Hour*, 538-539
 - rules, 514-516
 - security policies, 512
 - services, 521
 - system requirements, 504
 - transparent mode, 518
 - users, 521-527
 - accounts*, 521-523
 - authenticating*, 524-526
 - creating*, 523-524
 - groups*, 523
 - User icon*, 526-527
 - versions, 505
 - White Hole, compared, 511
- block device files, 84
- blocking
 - broadcast packets, 291
 - connections, 230
- Blue Lance, 555
- Bolt Beranek and Newman, Inc. (BBN), 8
- BOOTP daemon, 30
- Border Network Technologies, Inc., 555
- Borderware, 555



- breaking passwords, 75-77
- bridges, 284, 289-291
- broadcast data, UDP (User Datagram Protocol), 221
- broadcast option (ifconfig utility), 21
- brouters, 284
- BSD Unix
 - Gauntlet, 396
 - routing
 - disabling*, 332-334
 - static routes*, 342
- BSD/OS
 - kernal parameters, changing, 431
 - TIS Firewall Toolkit, compiling, 423-424
- bugs (software), 128
 - ftpd, 571
 - opieftpd, 561
 - opiekey, 562
 - rlogind, 577
 - telnet, 584
- Bugtraq list, 149-150
- building
 - network security policies, 99-100
 - TIS Firewall Toolkit, 405-408
- buttons
 - Disable user, 523
 - Update User window, 525-526
 - User Management window, 522
- BYE command, 264
- byte-oriented netmasks, 15
- Bytes Per Port report, 540

C

- c count option (ping utility), 35
- c option
 - opiepasswd, 173, 563
 - opiesu, 567
- c file type (Unix), 85
- C security levels, 60-61
- c[onnect] command, 448
- c[onnect] hostname [port] command, 441
- cables, twisted-pair, 18
- calculating netmasks, 14
- calculators
 - external, 193
 - Macintosh, 192
 - Microsoft Windows (WinKey), 188, 193
 - Unix, 191-192
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), 62
- CD/DIR permission option (Black Hole), 517
- CDUP command (FTP), 558-569
- CellWave algorithm, 302
- CERT (Computer Emergency Response Team), 107, 123, 153-154
 - mailing lists, 150-151
- Challenge option (Transfer rule component), 516
- challenge/response mechanisms, 146
- changing kernel parameters, 431
- character device files, 85
- checksums, 144-145
- CHMOD command (FTP), 560, 570
- chokes, *see* screening routers
- chroot rootdir keyword, 435
- chroot, 413
 - jails, constructing, 120
 - TIS Firewall Toolkit, 416-417
- chroot(2) command, 571
- CIAC (Computer Incident Advisory Capability), 123, 156
- CIDR (Classless Inter-Domain Routing), 15-16



- circuit-gateways, 353-354
- Cisco routers
 - access lists, 371-372
 - packet filtering, 237-281
- classes (IP addresses)
 - class A, 10
 - class B, 11
 - class C, 11-12
 - class D, 10
 - dividing, 14
- classes table (Drawbridge packet filter), 309
- classless addresses, 15-16
- clear command (Filter Manager), 322
- clear text, 88
- client option (Makefile), 172
- clients
 - custom, 352
 - non-proxy-aware, 462-463
 - proxy-aware, 463
- close command
 - telnet, 52-53
 - tn-gw, 441
- CLOSE_WAIT socket state, 44
- CLOSED socket state, 44
- CLOSING socket state, 44
- cmd service specification, 577
- CNSRT (Computer Network Security Response Team), 156-157
- command mode, telnet utility, 52-53
- commands
 - access-class line configuration, 243
 - allow, 314-315
 - arp, 45-47
 - authdump, 477
 - authload, 478
 - authserv, 472-474
 - authsrv, 471-472
 - Berkely r, 48-52
 - rcmd*, 51-52, 190
 - rcp*, 49-50
 - rlogin*, 48-49
 - rsh*, 50-51
 - c[onnect], 448
 - chroot(2), 571
 - clear, 322
 - config, 333
 - cron, 479
 - crypt, 89, 142
 - crypt(1), 89
 - dig, 47-48
 - display, 476
 - Edit menu
 - Add*, 523, 531
 - Delete*, 523
 - Modify*, 523
 - Rules*, 523
 - File menu
 - Commit*, 514, 523, 525
 - Open*, 521
 - Revert*, 514
 - finger, 39-40
 - fixmake, 423
 - FTP, 54-56, 453, 558-559, 568-570
 - BYE*, 264
 - MODE*, 257
 - NOOP*, 257
 - PASS*, 254
 - PASV*, 257, 268-269
 - PORT*, 256-257, 376
 - QUIT*, 257, 264
 - RETR*, 257
 - STOR*, 257
 - STRU*, 257
 - TYPE*, 257
 - USER*, 252, 257



- genkey, 321
- hostname, 17
- ICMP ECHO_REQUEST, 33
- ifconfig, 19-22, 38-39
- key, 189, 572
- keyinfo, 572
- keyinit, 187, 573-574
- kill, 427, 469
- list, 475-476
- ls, 83
- make, 171, 174-175, 186, 332-334, 423
- make install, 177, 424-426
- mfs, 429
- Navigate menu
 - Follow*, 523
 - New*, 523
 - Open*, 523-525
 - Top*, 523
 - Up*, 523
- netscan, 488
- netstat, 40-44, 335, 429
- newgrp, 71
- newkey, 321
- nslookup, 31, 460
- opieftpd, 558
- opieinfo, 176, 565
- opiekey, 174-175, 561-562
- opielogin, 176, 182-183, 566
- opiepasswd, 173, 183, 563
- opiesu, 175, 183, 567
- passwd, 69
- ping, 33-36, 322
- portscan, 429
- ps, 426, 429, 506
- pwconv, 68
- query, 322
- quote, 480
- reboot, 322
- reject, 314
- remsh, 50
- reset, 322
- route, 342
- runtime, 36-37
- rwho, 37
- set target, 320
- skey, 194
- store, 479
- strings, 333
- su, 582
- telnet, 52-53, 352, 441
- traceroute, 44-45
- upload, 321
- user-management (Black Hole), 523
- uuencode, 142
- xbh menu, Reports, 537
- comment field, /etc/passwd file, 66
- Commercial S/Key Version 2.0, 160
- commercial software vendors, 552, 555-556
- Commit command (Black Hole), 514, 523-525
- Common Criteria, 62-64
- compiling
 - authsrv (authentication server), 468
 - source code
 - LogDaemon*, 185-187
 - OPIE (One-Time Passwords In Everything)*, 170-172
 - TCP Wrapper, 186-187
 - TIS Firewall Toolkit
 - BSD/OS*, 423-424
 - SunOS*, 423
 - x-gw proxy agent, 423
- compromised systems, 510
- Computer Associates CA, 556



- Computer Emergency Response Team (CERT), 107, 123, 153-154
- Computer Incident Advisory Capability (CIAC), 123, 156
- Computer Network Security Response Team (CNSRT), 156-157
- Computer Oracle and Password Program (COPS), 550
- Computer Security Resource and Response Center (CSRC), 155
- Computer Underground Digest*, 135, 150
- computers, security
 - encryption, 87-90
 - IP (Internet Protocol) spoofing, 92
 - Kerberos, 90-92
 - network equivalency, 80-83
 - passwords
 - aging*, 72-75
 - files*, 65-72
 - permissions, 84-87
 - policies, 65
 - security levels, 60-64
 - TCB (Trusted Computer Base), 78-80
 - vandalism, 75-77
- config command, 333
- configuration files
 - /etc/ethers*, 23
 - /etc/hosts*, 22-23
 - /etc/inetd.conf*, 25
 - /etc/networks*, 23
 - /etc/protocols*, 24
 - /etc/services*, 24-25
- configuration management, 135-136
- configuring
 - authserv (authentication server), 419-420, 468
 - bastion hosts, 336, 343-344, 408-409
 - Black Hole, 528-537
 - DNS (Domain Name Service)*, 528-530
 - proxy applications*, 531-541
 - equivalency
 - host*, 27, 80
 - user*, 28, 82-84
 - FTP (File Transfer Protocol), 180-181
 - Gauntlet, 397-401
 - interfaces, ifconfig utility, 19-22
 - InterLock, 383-385
 - KarlBridge packet filter, 286-301
 - NNTP (Network News Transfer Protocol) clients, 483
 - OTP (one-time password system)
 - users, 194-196
 - packet filters, 227-229
 - plug-gw application, 481-483
 - screened host gateways, 339-343
 - smap program, 455-457
 - smapd daemon*, 457-459
 - TIS Firewall Toolkit
 - authserv (authentication server)*, 467-480
 - netacl*, 433-438
 - netperm table*, 431-433
 - plug-gw application*, 481-482
 - proxy agents*, 444-467
 - routing*, 430-431
 - services*, 426-430
- Connect rule component (Black Hole), 516-517
- connecting ports, 53
- connection acknowledgment packets, 214
- connectionless protocols, 221
- connections
 - allowing, 232
 - blocking, 230



FTP proxy, 453-454
 networks, 139-140
 port 5555, 247
 rlogin proxy, 447-449
 Connections Per Host report, 539-540
 control connection (FTP), 248
 control modules (FireWall-1), 360-363
 conventions, netperm table, 432
 COPS (Computer Oracle and Password Program), 550
 Copy button (Black Hole), 522
 copy protection daemon, 29
 copyrighted software, 110
 Crack, 550-551
 cracking passwords, 76-77
 CRCs (Cyclic Redundancy Checksums), 144
 creating users, Black Hole, 523-525
 crit message level (Black Hole), 513
 cron command, 479
 crypt keys, 90
 crypt command, 89, 142
 crypt(3) algorithm, 88-89
 cryptographic checksums, 145
 CSRC (Computer Security Resource and Response Center), 155
 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria, 62
The Cuckoo's Egg, 128
 custom clients, proxy applications, 352
 custom programs, application-level gateways, 351-354
 Cut button (Black Hole), 522
 CWD command, 558, 569
 Cybersafe Challenger, 556
 Cyclic Redundancy Checksums (CRCs), 144

D

-d option
 arp, 46
 ftpd, 568
 opieftpd, 558
 opiekey, 562
 ping, 35
 d file type (Unix), 84
 D1 security level, 60
 daemons, 9, 28-32
 bootpd, 30
 FTP (File Transfer Protocol), testing, 178-179
 inetd, 32
 ldsocket, 28-29
 lpd (line printer), 29
 named, 31
 opieftpd, 180-181
 rarpd, 29
 routed, 30
 rwho, 32
 sendmail, 9
 slink, 28
 smapped, 454
 configuring, 457-460
 rules, 458
 snmpd, 29
 syslogd, 31
 daily-report.sh, 491
 DARPA (Defense Advanced Research Projects Agency), 8, 153
 data
 accessing, FireWall-1 packet filtering, 362
 encrypting, 87-90, 140-146
 KarlBridge packet filter, 289-290



- security risk analysis, 106
- sharing, 327
- data connection (FTP), 248
- Data Encryption Standard (DES), 88, 141
- data link layer (OSI Reference Model), 206
- database pathname rule (authserv), 470
- databases
 - authserv (authentication server), 469-472
 - authmgr program*, 476-477
 - commands*, 477-479
 - backing up*, 479
 - OTP (one-time password system), testing, 187
 - policy database (Black Hole), 514-520
 - rules*, 514-516
- DDN (Defense Data Network), 154
- debug option (ifconfig utility), 21
- decryption, 140
- default netmasks, 12-13
- default-gopher server option (http-gw), 461
- default-httpd server option (http-gw), 462
- Defense Advanced Research Projects Agency (DARPA), 8, 153
- Defense Data Network (DDN), 154
- defining
 - access lists, 238-239
 - groups, 83
 - principals, 91
 - security policies, 65
 - sys_errlist, 424
 - users, 83
- DELE command (FTP), 558, 569
- Delete button (Black Hole), 522
- Delete command (Edit menu), 523
- Delete/Rename Permission option (Black Hole), 517
- deleting users, Black Hole, 523
- deluser username command, 472
- Demilitarized Zone (DMZ), bastion hosts, 344-346
- denial messages, tn-gw, 440
- denial-msg filename option
 - ftp-gw, 450
 - rlogin-gw, 445
 - tn-gw, 439
- deny option
 - ftp, 466
 - http-gw, 464
- Deny option (Transfer rule component), 516
- deny-hosts option
 - http-gw, 464
 - netacl program, 434
- deny-summ.sh (service denial usage report), 492-498
- denydest-msg filename option
 - ftp-gw, 450
 - rlogin-gw, 446
 - tn-gw, 439
- deploying bastion hosts, 336
- DES (Data Encryption Standard), 88, 141
 - Drawbridge packet filter, 304, 319
 - File Manager, 321
 - Filter Manager, 321
- designing
 - networks, Black Hole, 510-512
 - packet filters, 229-233
 - security policies, 99-100
- dest option
 - ftp-gw, 451
 - host access rules, 442



- dest-address option (ifconfig utility), 21
- Destination message, 33
- Destination rule component (Black Hole), 516
- destinations, listing, 443
- Destinations report, 540
- detecting unauthorized activity, 131
- diagnostics
 - rexecd, 575
 - rlogind, 577
 - rshd, 578
- dial-back modems, 131
- dialup lines, 126-127
- dialup passwords, adding, 69
- differential backups, 138
- dig (domain information groper) utility, 47-48
- dir function, 465
- directories
 - ftp, 560, 571
 - permissions, 85
 - Unix, 84
- directory field, /etc/passwd file, 66
- directory pathname option
 - ftp-gw, 450
 - http-gw, 461
 - rlogin-gw, 445
 - smap, 456
 - smapd, 458
 - tn-gw, 439
- Disable user button, 523
- disabling
 - IP (Internet Protocol) forwarding, 333, 430-431
 - routing, 332-334
 - services, TIS Firewall Toolkit, 426-430
 - user accounts, Black Hole, 523
- Discretionary Access Controls, 61
- Discretionary Security Protection system, 60-61
- disk partitions, 335
- display command, 53, 476
- display username command, 473
- dividing networks, 13-15
- DMZ (Demilitarized Zone), bastion hosts, 344-346
- DNC daemons, 31
- DNS (Domain Name Service), 16
 - Black Hole, configuring, 528-530
 - files, MX (mail exchanger) records, 459-460
 - spoofing, preventing, 433
 - UDP (User Datagram Protocol), 222, 273
- DNS Configuration option (Gauntlet), 401
- Do not log option (Black Hole), 517
- doc directory, Drawbridge packet filter, 306
- DOE Computer Incident Advisory Capability (CIAC), 156
- Domain Name Service, *see* DNS
- domains, assigning, 17
- dotted-decimal notation, 10
 - extended access lists, 241
 - standard access lists, 239
- down option (ifconfig utility), 20
- downloading
 - LogDaemon, 184
 - TCP Wrapper, 184
 - TIS Firewall Toolkit, 422-423
- Drawbridge packet filter, 304-312
 - commands
 - allow*, 314-315
 - reject*, 314



- configuration files, 315-317
- DES support, 304
- directories
 - doc*, 306
 - fc*, 306
 - filter*, 306
 - fm*, 306
- Filter Compiler, 305-307
- filter language, 312-317
- Filter Manager, 305-307, 319-322
- FILTER.EXE, 317-319
- halting, 319
- host classes, 314
- service specifications, 309-317
- software, extracting, 305-307
- tables
 - allow*, 309
 - classes*, 309
 - generating*, 308
 - network*, 308
 - reject*, 309
- TCP filtering, 308-309
- utilities, 305
- drawbridge-1.1-des.tar.Z, 304
- drawbridge-1.1.tar.Z, 304
- Drop option (Transfer rule component), 516
- dual-homed firewalls
 - application forwarders, 329
 - application layer, 331
 - disk partitions, 335
 - /etc/inetd.conf, 335
 - /etc/services, 335
 - logins, 329, 331
 - programming tools, 335
 - routing, disabling, 332-334
 - security, 334-335
 - services, 335

- SUID/SGID permissions, 335
- Unix, 331
- zones of risk, 329
- dual-homed hosts
 - data sharing, 327
 - firewalls, 327-335
 - login security, 334-335
- DuhMail (Black Hole), 508
- dump files, 478

E

- e-mail
 - address spoofing, 143
 - Electronic Mail Configuration option (Gauntlet), 401
 - InterLock SMTP gateway services, 389-390
 - mailing lists, 147-152
 - signal-to-noise ratios, 147-148
- EAL security levels, 63
- echo feature (OPIE passwords), 176
- Echo Reply/Request messages, 34
- Edit menu commands
 - Add, 523, 531
 - Delete, 523
 - Modify, 523
 - Rules, 523
- editing files
 - /etc/inetd.conf, 427
 - /etc/services, 438
 - Makefile, 188, 423-424
- Electronic Mail Association (EMA), 116
- Electronic Mail Configuration option (Gauntlet), 401
- Elite16 Ethernet cards, 317
- EMA (Electronic Mail Association), 116
- enable username command, 473



- enabling transparent mode (Black Hole), 518
- encrypted field, /etc/passwd file, 66
- encrypting
 - files, 89-90
 - passwords, 87-89
- encryption, 140-146
 - checksums, 144-145
 - crypt command, 142
 - DES (Data Encryption Standard), 141
 - information integrity, 144
 - KarlBridge packet filter, 289
 - origin authentication, 143
 - PEM (Privacy Enhanced Mail), 142
 - public-key, 509
 - smart cards, 146
- endpoints (packet filters), 235
- Enigma, 142
- external DNS (Domain Name Service), configuring, 530
- Entrust, 509
- environ command (telnet), 53
- environment variables (su), 583
- equivalency, 80-83
 - host, 27, 80-81
 - root, 81
 - users, 28, 82-83
- error messages
 - Black Hole, 513
 - LogDaemon, 575-578
- errors, reporting, 273
- ESTABLISHED socket state, 44
- /etc/dialups file, 68-70
- /etc/ethers file, 23
- /etc/ftpusers file, 54-55
- /etc/group file, 70-72
- /etc/hosts file, 22-25
- /etc/hosts.equiv file, 26-28
- /etc/inetd.conf file, 25
 - dual-homed firewalls, 335
 - editing, 427
 - TIS Firewall Toolkit, 408-411
- /etc/networks file, 23
- /etc/passwd file, 65-66
- /etc/protocols file, 24
- /etc/services file
 - dual-homed firewalls, 335
 - editing, 438
 - TIS Firewall Toolkit, 412-413
- /etc/shadow file, 67-68, 134
- Ethernet, 18
 - board setup, Filter program, 318
- Ethernet-to-Ethernet KarlBridge box, 303
- ethers file, 23
- ex0/ex1 interfaces (Gauntlet), 397-398
- exec executable keyword, netacl
 - program, 434
- exec function, 465
- exec service specification, 574
- executable pathname option (smappd), 458
- executable rule, 459
- execute permission, 85
- exit command, 441, 474
- expanded IP/ARP support (KarlBridge packet filter), 293
- extended access lists, 240-243
- extensions, Black Hole, 509
- external calculators, 193
- External Data Representation (XDR), 223
- external nameservers, Black Hole, 530



external networks
 access, restricting, 140
 packet filtering, 226-227
external users, 109, 118
extracting software (Drawbridge packet filter), 305-307

F

-f address-family option (netstat), 41
-f option
 finger, 40
 opielogin, 566
 opiesu, 567
 ping, 35
 rlogind, 576
 su command, 583
-f file option (arp utility), 46
fallback strategies, 131
FAQs (Frequently Asked Questions), 147
fault isolation, ping, 36
fc directory, Drawbridge packet filter, 306
fields
 /etc/group file, 71
 /etc/passwd file, 65-66
 password, 74
flkeyinit, 573
File Control database, 78
File Manager, DES support, 321
File menu commands (Black Hole)
 Commit, 514, 523-525
 Open, 521
 Revert, 514
file transfer protocol, *see* FTP
files
 Black Hole log files, 513
 dialup password, 68-70
 encrypting, 89-90
 entries, trusted, 80
 ftpusers, 54-55
 group, 70-72
 login, 196
 named.boot, 529
 named.hosts, 530
 .netrc, 55-57
 network access
 hosts.equiv, 26-28
 .rhosts, 26, 28
 network configuration, 22-25
 ethers, 23
 hosts, 22-23
 inetd.conf, 25
 networks, 23
 protocols, 24
 services, 24-25
 opieaccess, 566
 .opiealways, 566
 opiekeys, 566, 568
 passwd, 65-66
 permissions, 81, 84-87
 pwexp.pl, 93-95
 security, 70-72
 services, 438
 shadow, 67-68
 syslog, 435
 TCB (Trusted Computing Base), 78
 TIS Firewall Toolkit, installing, 424-426
 Unix, 84-85
-filter option, http-gw, 464
Filter Compiler
 Drawbridge packet filter, 305-307
 table generation, 308
filter directory, Drawbridge packet filter, 306



- ul style="list-style-type: none; padding-left: 0;">
- filter language, Drawbridge packet filter, 312-317
- Filter Manager, 305-307, 319-323
- filter modules, FireWall-1 Status Monitor, 372
- Filter PC, 321-322
- Filter program
 - Drawbridge packet filter, 305-307, 317-319
 - invoking, 318
- filter scripts, FireWall-1 Rules-Base Manager, 370
- FILTER.EXE, 317-319
- filtering
 - packets, 225-235, 237-281
 - access lists*, 238-243
 - address spoofing*, 244-245
 - Cisco routers*, 237-281
 - filters*, 244-245, 284-322
 - firewalls*, 325-326, 359-362
 - FTP (File Transfer Protocol)*, 248-269
 - IAP (Internet Access Provider)*, 337-338
 - ICMP (Internet Control Message Protocol)*, 273-274
 - incoming/outgoing calls*, 243-244
 - ports*, 245-248
 - RIP (Routing Information Protocol)*, 274
 - rules*, 238-243
 - screen routing examples*, 275-281
 - Telnet*, 269
 - UDP (User Datagram Protocol)*, 271-273
 - X Windows*, 248, 270
 - tables, 321
- FIN flag, 214
- FIN_WAIT_1 socket state, 44
- FIN_WAIT_2 socket state, 44
- finger utility, 39-40
- Firewall Toolkit (TIS), 421-499, 548
 - authserv (authentication server)
 - authmgr program*, 476-477
 - commands*, 477-478
 - compiling*, 468
 - configuring*, 468
 - passwords*, 475
 - protocols*, 475
 - reports*, 491-492
 - rules*, 469-470
 - users*, 468-480
 - compiling, 423-424
 - connections, testing, 436-437
 - help, 498
 - installing, 424-426
 - netacl program
 - arguments*, 433
 - configuring*, 433-435
 - keywords*, 434-435
 - testing*, 436-437
 - netperm table, 431-433
 - netscan program, 488
 - obtaining, 422-423
 - plug-gw application, 480-487
 - configuring*, 481-482
 - NNTP (Network News Transfer Protocol)*, 482-485
 - POP (Post Office Protocol)*, 485-487
 - portscan utility, 429, 487-488
 - proxies
 - FTP*, 449-453
 - HTTP*, 460-464



- rlogin*, 444-449
- sendmail*, 454-460
- Telnet (tn-gw)*, 438-444
- X Windows*, 466-467
- reports
 - reporting tools*, 489-491
 - usage*, 494-499
 - service denial reports*, 492-493
- services, disabling, 426-430
- TCP/IP, configuring, 430-431
- FireWall-1
 - architecture, 359-362
 - control modules, 360-362
 - FTP outbound connections, 375-376
 - Gopher, 376
 - information resources, 379
 - Log Viewer, 373-374
 - managers
 - Network Objects Manager*, 364-366
 - Rules-Base Manager*, 368-372
 - Services Manager*, 367
 - Mosaic, 376
 - optimizing, 376-377
 - packet filtering, 359-362
 - performance degradation, 376-377
 - Router Access List, 371-372
 - RPC-based problems, 376
 - rules
 - language*, 377-379
 - verifying*, 370
 - Status Monitor, 372
 - system requirements, 359
 - UDP applications, 375
 - WWW (World Wide Web), 376
- firewalls, 326-354
 - application-level gateways, 350-354
 - bastion hosts, 335-346
 - dual-homed hosts, 327-335
 - forums, 553
 - implementing, 355-420
 - mailing lists, 552-553
 - packet filtering, 325-326
 - screened subnets, 349-350
 - software, 552
 - Black Hole*, 501-541
 - Gauntlet*, 395-404
 - InterLock*, 379-395
 - TCP Wrapper*, 356-358
 - TIS Firewall Toolkit*, 408-499
 - system monitoring, 132
- Fisher, Hugh, 196
- Fixed option (rule entries), 516
- fixmake command, 423
- flags (TCP), 194, 212-216
- fm directory, Drawbridge packet filter, 306
- .fmrc file, Filter Manager, 322
- Follow command (Black Hole), 523
- fonorla.net site, 444
- forced entries (passwords), 74
- forums, 553
- forwarder agents, 329
- forwarding
 - multicast packets, 291
 - IP (Internet Protocol) packets, 333, 430-431
- frames, data link layer (OSI Model), 206
- Frequently Asked Questions (FAQs), 147
- FTP (File Transfer Protocol)
 - anonymous FTP, 560
 - configuring*, 180-181
 - TIS Firewall Toolkit*, 416-417
 - application layer (OSI Model), 224
 - Black Hole, 532-533



commands, 256-257, 558-559,
 568-570
 control connection, 248
 daemons, testing, 178-179
 data connection, 248
 FireWall-1 (outbound connections),
 375-376
 Gauntlet, 402-403
 InterLock proxy services, 389
 packet filtering, 248-269
 proxy, 453-454
 security, 267
 servers, 180-181
 Service flag options, 517
 sites
 Bellcore, 163, 549
 COPS (Computer Oracle and
 Password Program), 550
 Crack, 550
 LogDaemon, 184
 NRL (U. S. Naval Research
 Laboratory), 166
 portmapper, 548
 Release 6/Fix 13 (X Display
 Manager), 196
 SATAN, 551
 Swatch Logfile Monitor, 549
 TAMU Tiger, 550
 Tcpdump, 549
 tcpwrapper, 548
 TIS (Trusted Information Systems,
 Inc.), 422, 548-549
 Wietse, 166
 TCP (Transfer Control Protocol),
 259-264
 TCP ACK flag, 268
 transfers, 466
 URLs, 463

usage reports, 494
 usernames, specifying, 453
 Well-Known Port 21, 248
 ~ftp directory, 560, 571
 ftp utility, 54-56, 453, 465
 ftp-gw, 449-454
 connections, 453-454
 rules
 host access, 451-452
 program, 449-450
 verifying, 452-453
 ftp-proxy server option, http-gw, 462
 ftp-summ.sh (ftp usage report),
 491, 494
 ~ftp/bin directory, 560, 571
 ftpd, 190, 568-571
 ~ftp/etc directory, 561, 571
 ~ftp/pub directory, 561, 571
 ftpusers file, 54-55
 full associations (packet filters), 233-235
 full backups, 137-139
 full-duplex communications, 222, 231
 fwtk.tar.Z (TIS Firewall Toolkit),
 405-408

G

gateway proxy services (InterLock),
 387-395
 gateways, 327
 application-level, 350-354
 circuit, 353-354
 FireWall-1, 358-379
 FTP (File Transfer Protocol)
 configuring, 449-454
 connections, 453
 rules, 449-452
 verifying, 452-453



- InterLock, 379-395
 - OSI Model, 224
 - rlogin
 - configuring*, 444-449
 - rules*, 445-449
 - verifying*, 448-449
 - screened host, 336-337
 - Gauntlet, 395-404
 - BSD Unix, 396
 - configuring, 397-401
 - ex0/ex1 interfaces, 397-398
 - rlogin, 403-404
 - telnet, 403
 - generating
 - passwords
 - LogDaemon*, 189
 - OPIE (One-Time Passwords In Everything)*, 175
 - reports, Black Hole, 537-540
 - Generic Protocol Daemon (GPD), 395
 - genkey command, 321
 - Get Permission option (Black Hole), 517
 - getenv() function, 408
 - getty program, 88
 - GID assignments, TIS Firewall Toolkit, 405
 - GID field
 - /etc/group file, 71
 - /etc/passwd file, 66
 - global routing tables, 15-16
 - globbing conventions, 570
 - gopher server option
 - http-gw, 464
 - Gopher
 - Black Hole, 533-534
 - FireWall-1, 376
 - InterLock, 394
 - URLs, 463
 - GPD (Generic Protocol Daemon), 395
 - grace periods (password aging), 74
 - granting network access, 111-115
 - Great Circle mailing list, 552
 - group file, 70-72
 - Group Membership message, 34
 - group user groupname command, 473
 - group wheel condition (skey.access file), 580
 - group wizard, 475
 - groups
 - Black Hole, 523
 - defining, 83
 - wheel, 71
 - Guardian (Black Hole), 507
 - guessing passwords, 76-77
 - gunzip utility, 305
- ## H
- h option
 - opieinfo, 565
 - opiekey, 562
 - opielogin, 566
 - opiepasswd, 563
 - hackers, *see* vandals
 - half associations (packet filters), 235
 - half-duplex communications, 222
 - halting Filter program (Drawbridge packet filter), 319
 - hardware requirements
 - Filter program (Drawbridge packet filter), 318
 - FireWall-1, 359
 - Gauntlet, 395
 - InterLock, 381
 - KarlBridge packet filter, 285



HELP command (FTP), 441, 474,
558-560, 569-570
help-msg filename option
 ftp-gw, 450
 rlogin-gw, 445
 tn-gw, 439
Hess, David K., 305
hexadecimal notation, 10
home field, /etc/passwd file, 66
HOME variable (su), 583
host access rules
 FTP proxy, 451-452
 http-gw, 463-464
 rlogin proxy, 448-449
 texnet proxy (tn-gw), 442-443
host addresses
 netmasks, 12-15
 spoofing, 580-581
host classes (Drawbridge packet filter),
 314
host denial messages, 436-437
 rlogin proxy, 447-450
host equivalency, 27-28, 80-81
host names
 assigning, 17-18
 spoofing, 581
hostname command, 17
hosts
 dual-homed, 327-335
 names, 16-18
 security, 127-128
hosts files, 22-23
hosts host-pattern [key] rule
 (authserv), 470
hosts host-pattern option
 http-gw, 464
 rlogin-gw, 446
 tn-gw, 440

hosts keyword, 464
hosts.allow/hosts.deny files (TCP
 Wrapper), 357-358
hosts.equiv file, 26-28, 80
HTTP (HyperText Transport Protocol)
 Black Hole, 534
 clients, 462-463
 InterLock, 393-394
 URLs, 463
 usage reports, 494-495
http-gw, 460-466
 clients, 462-463
 rules, 461-464
http-summ.sh (http usage report),
 491, 495
-httpd server option (http-gw), 464
Hyper Text Transport Protocol, *see*
 HTTP
hyphen (-), 84, 464

I

-i option
 finger, 40
 netstat, 41
 ping, 35
I&A (Identification and Authen-
 tication), 79
IAP (Internet Access Provider) packet
 filtering, 337-338
IC Engineering, 556
ICMP (Internet Control Message
 Protocol)
 access lists, 241
 errors, reporting, 273
 messages, 33-34, 274
 packet filtering, 273-274
 ping utility, 33-36, 274



- redirection (InterLock), 381
- routers, screening, 340
- ICMP ECHO_REQUEST
 - command, 33
- Icon Browser button (Update User window), 526
- icons, adding (Black Hole), 527
- Identification and Authentication I&A), 79
- identifying
 - security threats, 106-108, 124-130
 - users, 109-117
- IDLE command (FTP), 560, 570
- idle time, 39
- IETF (Internet Engineering Task Force), 9, 163
- ifconfig utility, 19-22, 38-39
 - command parameters, 20-21
- implementing
 - firewalls, 355-420
 - KarlBridge packet filter, 301-302
 - OTP (one-time password system), 163-165
 - packet filter rules, 238-243
- include statements, 407, 423
- incoming calls (packet filtering), 243-244
- incremental backups, 137-139
- inetd, 32
 - restarting, 427-428, 437-438
 - TIS Firewall Toolkit, 410
- inetd.conf file, 25, 427
- ingress, *see* access points
- initial password selection, 115
- initializing passwords (OTP), 194
- input ports (packet filtering), 245-248
- install option (Makefile), 172
- Install Software Upgrade option (Gauntlet), 400
- installing
 - LogDaemon, 189
 - OPIE (One-Time Passwords In Everything), 177-198
 - smap, 455
 - TIS Firewall Toolkit, 410-413, 424-426
- interfaces, 18-21
 - Black Hole, 512-514
 - configuring, 19-22
 - physical layer (OSI Model), 206
- InterLock, 379-395, 555
 - ACRB (Access Control Rule Base), 382, 385-387
 - auditing, 380
 - configuring, 383-385
 - e-mail (SMTP gateway services), 389-390
 - GPD (Generic Protocol Daemon), 395
 - ICMP redirection, 381
 - IP (Internet Protocol) forwarding, 381
 - logging, 380
 - proxy daemons, 382-383
 - rules, 382
 - services
 - NNTP (Network News Transfer Protocol), 391-393*
 - proxy application gateway, 387-395*
 - FTP proxy, 389*
 - HTTP (HyperText Transport Protocol), 393-394*
 - SMTP (Simple Mail Transfer Protocol) gateway, 389-390*



- Telnet proxy*, 387-388
- X Windows*, 390-391
- source routing, 381
- TCP/IP, 379
- internal DNS (Domain Name Service),
 - configuring, 528-536
- internal nameservers, 529
- internal network segments, 226-227
- International Organization of Standards (ISO), 204
- Internet
 - Internet Engineering Task Force (IETF), 9, 163
 - RFCs
 - RFC 1178*, 17
 - RFC 950*, 13
 - security, 122-123
 - service requests, logging, 356-358
 - see also* protocols
- Internet Control Message Protocol (ICMP), 340
 - packet filtering, 273-274
- Internet Engineering Task Force (IETF), 9, 163
- Internet Protocol, *see* IP
- Interrupt Process signals, 560
- Interval rule component (Black Hole), 516
- invoking Filter program (Drawbridge packet filter), 318
- IP (Internet Protocol)
 - addresses, 9-18
 - classes*, 10-12
 - netmasks*, 12-15
 - notations*, 10-18
 - spoofing*, 506
 - extended access lists, 241
 - forwarding, 430-431

- network layer (OSI Model), 207
- protocols, 24
- routing, KarlBridge packet filter, 289-290
- spoofing, 92, 506
- tunneling, UDP (User Datagram Protocol), 222
- IP Address Configuration option (Gauntlet), 401
- IP Hosts Setup screen (KarlBridge packet filter), 295
- ISO (International Organization of Standards), 204
- iteration values, 161, 166

J-K

- jails, 120-121
- K option (su command), 583
- Karl, Doug, 284
- KarlBridge packet filter, 284-304
 - bridging, 289-291
 - CellWave algorithm, 302
 - configuring, 286-301
 - data encryption, 289-290
 - distribution software, 286
 - Ethernet-to-Ethernet KarlBridge box, 303
 - IP (Internet Protocol) routing, 289-292
 - IP/ARP support, 293
 - learned table lockdown, 292
 - security filters, 289-290
 - SMC Elite 16 cards, 301
 - storm thresholds, 293-294
 - watchdog reboot timer, 290



KarlNet, Inc., 303-304
Karn, Phil, 162
KBCONFIG.EXE, KarlBridge
 configuration, 287
Kerberos, 146, 556
 disadvantages, 91-92
 passwords, requesting, 582
 physical security, 129
kernel module, FireWall-1 packet
 filtering, 362
key command, 189, 572
keyinfo command, 572-573
keyinit, 573-574
keyinit command, 187, 194
keys
 password, 89
 public-key encryption, 509
keywords
 hosts, 464
 netacl program, 434
kill command, 427, 469

L

-l option
 finger, 40
 netstat, 41
 opieftpd, 558
 rlgind, 576
 rlogin, 184
 rsh, 184
 ruptime, 37
 su, 583
l file type (Unix), 85
-l username option (rsh command), 51
Labeled Security Protection, 62
LAST_ACK socket state, 44

Lawrence Livermore National Laboratory (LLNL), 156
ldsocket daemon, 28-29
learned table lockdown, KarlBridge
 packet filter, 292
lengths (masks), 16
level 0/level 1 backups, 137-139
levels, security, 60-62
 Canadian Common Criteria, 62-64
 United States Department of
 Defense, 60-61
libwrap.a library, 186
line printer daemon, 29
linking STREAMS modules, 28
list command, 473-476, 559, 569
LISTEN socket state, 44
listing
 destinations, 443
 ports, 429
listings
 2.1—pwexp.pl, 93-95
 4.2—Installing the OPIE Software,
 178
 4.3—Makefile Options Section,
 180-181
 4.4—Sample opiekey Execution, 182
Livingston Enterprises, 556
LLNL (Lawrence Livermore National
 Laboratory), 156
log files
 Black Hole, 513
 syslog facility, 435
 TIS Firewall Toolkit, 489-491
Log Viewer (FireWall-1), 373-374
LogDaemon, 160, 166, 183-198
 components, 189-191
 ftpd, 190, 568-571
 key, 572



- keyinfo*, 572-573
- keyinit*, 573-574
- login*, 190
- rexecd*, 190, 574-575
- rlogind*, 190, 576-577
- rshd*, 190, 577-579
- skey.access*, 579-581
- skeysh*, 191, 582
- su*, 582-583
- telnetd*, 584
- FTP site, 184
- installing, 189
- manual pages, 568-584
- passwords, generating, 189
- platforms, 185
- programs, testing, 187-189
- source code
 - compiling*, 185-187
 - obtaining*, 184-185
- TCP Wrapper, 186
- logging
 - InterLock, 380
 - security violations, 119
 - transactions, 489-491
- login activity, monitoring, 132
- login field, /etc/passwd file, 66
- login program, 88
- login service specification, 576
- Login UID, 25
- logins
 - dual-homed hosts, 329, 331, 334-335
 - file permissions, 196
 - OPIE (One-Time Passwords In Everything), 176-177
 - remote, Log Daemon, 573
 - shells, 66
 - Unix, 79

- logout command (telnet), 53
- longname field, list [group] command, 473
- lpd (line printer) daemon, 29
- ls command, 83
- LT Auditor, 555
- LUID (Login UID), 25

M

- m option
 - netstat, 41-43
 - passwd, 69
 - su, 583
- M&T Technologies, 556
- Macintosh calculators, 192
- mail exchanger records, *see* MX
- mail handlers, DuhMail, 508
- mail usage reports, 496-497
- mailing lists
 - Bugtraq, 149-150
 - CERT (Computer Emergency Response Team), 150-151
 - Computer Underground Digest*, 150
 - firewalls, 499, 552-553
 - network security, 147-152
 - Risks forum, 148-149
 - S/Key, 197
 - signal-to-noise ratio, 147-148
 - SUN-NETS, 151-152
 - TCP/IP, 151
 - TIS, 499
 - Unix security, 148
 - VIRUS-L, 149
- Main Management Menu (Gauntlet), 399



- make command, 171, 174-175, 186, 332-334, 423
- make install command, 177, 424-426
- Makefile, 405-407
 - editing, 188, 423-424
 - OPIE (One-Time Passwords In Everything), 171-172
 - options section, 180-181
- managing user accounts, Black Hole, 521-523
- Manipulation Detection Code (MDC), 145
- manual pages
 - LogDaemon
 - ftpd*, 568-571
 - key*, 572
 - keyinfo*, 572-573
 - keyinit*, 573-574
 - rexecd*, 574-575
 - rlogind*, 576-577
 - rshd*, 577-579
 - skey.access*, 579-581
 - skeysh*, 582
 - su*, 582-583
 - telnetd*, 584
 - OPIE (One-Time Passwords In Everything)
 - opieftpd*, 558-561
 - opieinfo*, 564-565
 - opiekey*, 561-563
 - opielogin*, 566-567
 - opiepasswd*, 563-564
 - opiesu*, 567-568
- masks
 - lengths, 16
 - netmasks, 12-15
- Max_FTP_Login_Failures, 384
- Max_TELNET_Login_Failures, 384
- maxbytes value option (*smap*), 456
- maxrecip value option (*smap*), 456
- MD4 algorithm, 162
- MD5 algorithm, 163
- MDC (Manipulation Detection Code), 145
- MDTM command, 559, 569
- Media types, 18
- merging service specifications, 314
- message digests, 162-163
- messages
 - host denial, 436-437
 - rlogin proxy*, 447
 - telnet proxy*, 440
 - levels, Black Hole, 513
- metacharacters, 560, 570
- metric N option (*ifconfig* utility), 21
- mfs command, 429
- Microsafe, 556
- Microsoft Windows calculators, 193
- Milkyway Networks Corporation, 501, 556
 - address, 541
 - see also* Black Hole
- MKD command (FTP), 559, 569
- MODE command (FTP), 559, 569
- mode command, 53, 257
- Modem Security Enforcer, 556
- modems
 - dial-back modems, 131
 - Modem Security Enforcer, 556
- Modify command (Black Hole), 523
- monitoring networks, 131-133
- Mosaic, FireWall-1, 376
- multi-homed hosts
 - data sharing, 327
 - firewalls, 327-335
 - network interface boards, 327



multicast addresses, 10
 multicast packets, 291
 Multiple UDP Packets option (Black Hole), 517
 multiplexing, 209
 MX (mail exchanger) records, adding, 459-460

N

-n option
 key, 572
 netstat, 41
 opiekey, 175, 562
 opiepasswd, 563
 ping, 35
 rsh, 51
 named daemon, 31
 named pipes, 85
 named.boot file, 529
 named.hosts file, 530
 names, hosts, 16-18
 nameservers, 529-530
 NASA Ames Computer Network Security Response Team, 156-157
 National Institute of Standards and Technology (NIST), 88, 153-155
 National Science Foundation, 8
 Navigate menu commands (Black Hole)
 Follow, 523
 New, 523
 Open, 523, 525
 Top, 523
 Up, 523
 negation operator (!), 443
 netacl program
 arguments, 433
 configuring, 433-438

connections, restricting, 436, 454
 host denial messages, 436-437
 keywords, 434-435
 proxy agent, 508
 reports, 495-496
 testing, 436-437
 netacl-summ.sh, 491, 495-496
 netmask MASK option (ifconfig), 21
 netmasks
 calculating, 14-15
 defaults, 12-13
 netperm table, 431-433
 conventions, 432
 NNTP (Network News Transfer Protocol) client requests, adding, 483
 .netrc file, 55-57
 netscan program, 488
 netstat utility, 30, 40-44, 429
 command parameters, 41
 dual-homed firewalls, 335
 output, 42
 network addresses, 9, 14
 Network Information Services (NIS), 366
 network interface boards, 327
 Network Interface Tap (NIT), 319
 network interfaces
 bi-interface configuration (bastion hosts), 343-344
 promiscuous mode, 344
 network layer (OSI Reference Model), 207
 Network News Transfer Protocol (NNTP), 391-393
 Network Objects Manager, 364-366
 network permissions tables, TIS Firewall Toolkit, 413-420



- Network Policy, 97-157
- network segments (packet filtering), 226-227
- network tables, Drawbridge packet filter, 308
- networks
 - access
 - granting, 111-115*
 - points, 125-127*
 - application-level gateways, 350-354
 - ARPANET, 8
 - AUP (Acceptable Use Policy), 109-111
 - bastion hosts, 335-346
 - confidentiality, 129-130
 - connections, 139-140
 - data sharing, 327
 - dialup lines, 126-127
 - disclosure of information, 107
 - dual-homed hosts, 327-335
 - encryption, 140-146
 - equivalency
 - host, 80-81*
 - user, 82-83*
 - external, 140
 - files, 22-28
 - /etc/ethers, 23*
 - /etc/ftpusers, 54-55*
 - /etc/hosts, 22-23*
 - /etc/hosts.equiv, 26-28*
 - /etc/inetd.conf, 25*
 - /etc/networks, 23*
 - /etc/protocols, 24*
 - /etc/services, 24-25*
 - .rhosts, 26, 28*
 - host names, 16-18
 - interfaces, 18-22
 - jails, 120-121
 - Kerberos, 146
 - mailing lists, 147-152
 - managing, 134-136
 - monitoring, 131-133
 - newsgroups, 152
 - NSFNet, 8
 - passwords, 115
 - physical security, 128-129
 - recovery procedures (security), 136-139
 - reporting procedures, 134-139
 - resource identification (security), 106
 - risk analysis (security), 102-106
 - routing, CIDR (Classless Inter-Domain Routing), 15-16
 - security, 109-117, 146-147
 - planning, 98*
 - policies, 99-100, 118-123, 123-124*
 - response teams, 153-157*
 - threats, identifying, 106-108, 124-130*
 - servers, 127
 - subnets
 - netmasks, 12-15*
 - screened subnets, 349-350*
 - VPNs (Virtual Private Networks), 502
 - see also* firewalls; hardware; protocols; software
- networks file, 23
- New command (Black Hole), 523
- newgrp command, 71
- newkey command, 321
- news server software, 484
- newsgroups, network security, 152
- NFS (Network File System), 222



NIS (Network Information Services), 366
 NIST (National Institute of Standards and Technology), 88, 153, 155
 NIT (Network Interface Tap), 319
 NRL (U. S. Naval Research Laboratory), 160
 URL, 166
 NLST command (FTP), 559, 569
 NNT, Black Hole, 535-537
 NNTP (Network News Transfer Protocol)
 clients, configuring, 483
 InterLock, 391-393
 news protocol, 482-485
 NNTP Forwarder Configuration option (Gauntlet), 401
 NNTP Post_Header_Mapping, 384
 NNTP Post_Use_Mailmaps, 385
 NNTP_Private, 384
 NNTP_Public, 384
 nobogus true rule (authserv), 470
 node-to-node connections, 207
 NOLUID parameter, 25
 non-proxy-aware clients, 462-463
 NOOP command (FTP), 257, 559, 569
 Nortel (Northern Telecom), 509
 notating bastion host configurations, 336
 npasswd program, 551
 NRL, OPIE (One-Time Passwords In Everything), 168-177
 platforms, 169
 source code, 168-169
 NSFNet, 8
 nslookup command, 31, 460

O

objects, FireWall-1 packet filtering, 362
 obtaining
 LogDaemon, 184-185
 OPIE (One-Time Passwords In Everything), 168-169
 TIS Firewall Toolkit, 422-423
 octets, 10, 13
 One-Time Passwords In Everything,
 see OPIE
 one-rotor encryption, 90
 one-time password system, *see* OTP
 one-way encryption algorithm, 88
 one-way hash functions, 145
 Open command (Black Hole)
 File menu, 521
 Navigate menu, 523, 525
 telnet, 53
 open connection packets, 214
 OpenLook X11R5 GUI, FireWall-1
 Control Module, 363
 operation user id telnet-gw host rule (authserv), 471
 OPIE (One-Time Passwords In Everything), 168-177
 calculators, 191-193
 external, 193
 Macintosh, 192
 Microsoft Windows (WinKey), 193
 Unix programs, 191-192
 components
 opieftpd, 180-181, 558-561
 opieinfo, 181, 564-565
 opiekey, 182, 561-563
 opielogin, 182-183, 566-567
 opiepasswd, 183, 563-564
 opiesu, 183, 567-568



- FTP server, 179
- installing, 177-198
- logins, testing, 176-177
- Makefile, 171-172
- manual pages, 558-568
- passwords
 - password echo feature, 176*
 - setting, 173*
- platforms, 169
- programs, testing, 172-177
- seeds, verifying, 176
- source code
 - compiling, 170-172*
 - obtaining, 168-169*
- Telnet, testing, 179
- troubleshooting, 174
- see also* OTP
- opie-des, *see* opiekey
- opie-md4, *see* opiekey
- opie-md5, *see* opiekey
- opieaccess file, 566
- .opiealways file, 566
- opieftpd, 180-181
 - bugs, 561
 - command parameters, 558
 - security, 560-561
 - users, authenticating, 560
- opieinfo, 181, 564-568
 - command parameters, 565
- opieinfo command, 176
- opiekey, 174-175, 182, 561
 - bugs, 562
 - command parameters, 561-562
- opiekeys file, 566, 568
- opielogin, 176, 182-183, 566-567
- opiepasswd, 173, 183, 195, 563-564
 - command parameters, 563
- opiesu, 175, 183, 567-568
 - command parameters, 567
- Oracle (Black Hole), 507
- Orange Book security standards, 60
- origin authentication, 143
- OSI (Open Systems Interconnection) Reference Model, 203-204
 - application layer, 223-224
 - data link layer, 206
 - network layer, 207
 - physical layer, 206
 - presentation layer, 223
 - session layer, 222-223
 - transport layer, 207-222
- OTP (one-time password authentication system), 159-198
 - calculators
 - external, 193*
 - Macintosh, 192*
 - Microsoft Windows, 193*
 - Unix programs, 191-192*
 - database, testing, 187
 - implementing, 163-165
 - LogDaemon, 183-198
 - components, 189-191*
 - installing, 189*
 - testing, 187-189*
 - mailing lists, 197
 - passwords, initializing, 194
 - S/Key, 166-167
 - source code, 184-185
 - users, configuring, 194-196
 - versions, 165
 - X Windows, 196-198
 - see also* OPIE
- otp-md4, *see* opiekey
- otp-md5, *see* opiekey
- outgoing calls (packet filtering), 243-244
- output ports (packet filtering), 245-248



P

- p option
 - finger, 40
 - opielogin, 566
 - ping, 35
 - rcp, 50
- p file type (Unix), 85
- p protocol-name option (netstat), 41
- packet filter gateways/routers, *see* screening routers
- packet filter modules (FireWall-1), 360-362
- packet filtering, 225-235, 237-281
 - access lists
 - defining*, 238-239
 - extended*, 240-243
 - standard*, 239-240
 - address spoofing, 244-245
 - Cisco routers, 237-281
 - firewalls, 325-326, 359-362
 - IAP (Internet Access Provider), 337-338
 - incoming/outgoing calls, 243-244
 - input and output ports, 245-248
 - network segments, 226-227
 - packet filters, 230-235
 - configuring*, 227-229
 - designing*, 229-233
 - Drawbridge packet filter*, 304-322
 - KarlBridge packet filter*, 284-304
 - PCs (personal computers), 284-322
 - placement, 244-245
 - protocols, 248-274
 - FTP (File Transfer Protocol)*, 248-269
 - ICMP (Internet Control Message Protocol)*, 273-274
 - RIP (Routing Information Protocol)*, 274
 - Telnet*, 269
 - UDP (User Datagram Protocol)*, 271-273
 - X Windows*, 270
 - X11 protocol*, 248
 - rules, 238-243
 - screen routing, 202, 216, 275-281
- Packet Too Big message, 33
- packets, 214-216
 - routing, 207
- Paralon Technologies, 556
- Parameter message, 33
- parameters
 - arp, 46
 - finger, 40
 - kernal, changing, 431
 - netstat, 41
 - ping, 35-36
 - runtime, 37
- partitions, dual-homed firewalls, 335
- PASS command (FTP), 254, 559, 569
- pass phrases, 163, 167
 - OPIE (One-Time Passwords In Everything), 174
 - OTP (one-time password system), 162
- passing packets, KarlBridge packet filter, 292
- passok option
 - ftp-gw, 451
 - host access rules, 443
- passthrough telnet services, 438
- passwd command, 69
- passwd+ program, 551
- password [username] text command, 473
- Password button (Update User window), 526



- password control table, 579
- password echo feature (OPIE), 176
- password field, 74
 - /etc/group file, 71
 - /etc/passwd file, 65
- password key, 89
- Password rule component (Black Hole), 516
- password-cracking software, Crack, 550
- passwords
 - aging, 72-75, 115
 - authserv (authentication server), 468, 475
 - dialup, adding, 69
 - encrypting, 87-89
 - files
 - dialup password*, 68-70
 - password*, 65-67
 - shadow password*, 67-68
 - initial password selection, 115
 - lifetimes, 74
 - LogDaemon, generating, 189
 - OTPs (one-time password system), 160-198
 - initializing*, 194
 - OPIE (One-Time Passwords In Everything)*, 168-177
 - S/Key*, 166-167
 - Protected Password Database, 76
- Paste button (Black Hole), 522
- PASV command (FTP), 257, 268-269, 559, 569
- Path Key, 556
- PATH variable (su), 583
- PCs (personal computers), packet filtering, 284-322
- PEM (Privacy Enhanced Mail), 142
- PERL (Practical Extraction and Report Language), 75
- permissions, 81, 84-87
 - granting, 111-115
 - login file, 196
 - root, 87
 - write, 86
- permit option, http-gw, 464
- permit-host rules, 465
- permit-hosts keyword (netacl program), 434
- permit-hosts option (http-gw), 464
- Phrack*, 135
- physical layer (OSI Reference Model), 206
- physical security, 128-129
- PIDs (process identifiers), procuring, 428
- ping utility, 33-36
 - Filter Manager, 322
 - ICMP (Internet Control Message Protocol), 274
 - netscan program, 488
- plaintext passwords, 418
- plug-to host, plug-gw, 481
- Plug To option (Black Hole), 517
- plug-gw application, 480-487
 - configuring, 481-482
 - multiple hosts, configuring, 483
 - NNTP (Network News Transfer Protocol), 482-485
 - POP (Post Office Protocol), configuring, 485-487
 - rules, 481
- plus function, 465
- policies (security), 65, 99-100, 123-124
 - Black Hole*, 512
 - violations*, 118-123



- policy database (Black Hole)
 - copying, 515
 - rules, 514-516
 - resolving*, 519-520
- POP (Post Office Protocol)
 - Black Hole, 531-532
 - plug-gw, configuring, 485-487
 - telnet sessions, 485-486
 - workstations, configuring, 486
- port 5555 connections, 247
- PORT command (FTP), 256, 257, 376, 559, 569
- port portid, plug-gw, 481
- port portid hostpattern [options] rule, plug-gw, 481
- port ttya condition (skey.access file), 580
- portmapper, 548
- ports
 - connecting, 53
 - listing, 429
 - numbers
 - TCP (Transmission Control Protocol)*, 210-211
 - UDP (User Datagram Protocol)*, 219-221
- portscan tool, TIS Firewall Toolkit, 409
- portscan utility, 429, 487-488
- pound symbol (#), 23, 432
- Practical Extraction and Report Language (PERL), 75
- preference values, 460
- prefixes (CIDR), 16
- presentation layer (OSI Reference Model), 223
- printing, Filter Manager, 320
- priority and challenge phase (Black Hole), 520
- Privacy Enhanced Mail (PEM), 142
- privacy policies, 116
- private key cryptosystems, 143
- private keys (Black Hole), 509
- Private Network Number Addressing, 528
- Private_Address, 384
- privileged accounts, 135
- privport, plug-gw, 481
- probing, 111
- Problem message, 33
- process identifiers (PIDs), procuring, 428
- process tables, TIS Firewall Toolkit, 428-429
- programs, *see* software
- Project Athena, 90
- promiscuous mode, 344
- prompt string option
 - rlogin-gw, 445
 - tn-gw, 439
- Protect and Proceed strategy (security policy violations), 119-122
- Protected Password database, 76, 78
- Protected Subsystem database, 78
- proto user protoname command, 474
- protocol independence, FireWall-1
 - packet filtering, 362
- protocols, 216
 - authserv (authentication server), 475
 - connectionless, 221
 - packet filtering, 248-274
- protocols file, 24
- proxies
 - application-level gateways, 352-354
 - custom clients, 352
 - daemons, 382-383



- FTP (File Transfer Protocol),
 - 449-454, 532-533
 - connections*, 453
 - rules*, 449-452
 - verifying*, 452-453
 - gateway services (InterLock), 387-395
 - Gopher, 533-534
 - HTTP (HyperText Transport Protocol), 460-466, 534
 - clients*, 462-463
 - rules*, 461-464
 - NNT, 535-537
 - POP (Post Office Protocol), 531-532
 - rlogin
 - configuring*, 444-449
 - rules*, 445-449
 - verifying*, 448-449
 - sendmail, 454-460
 - SMTP (Simple Mail Transfer Protocol), 537
 - Telnet, 438-444
 - X Windows, 466-467
 - proxy-aware clients, 463-464
 - proxy calls, socks library, 353
 - ps command, 426, 429, 506
 - PSH flag, 213-215
 - public-key encryption, 143, 509
 - Public_Address, 384
 - Public_Interface, 384
 - publicizing security policies, 123-124
 - Pursue and Prosecute strategy (security policy violations), 119-122
 - Put Permission option (Black Hole), 517
 - pwconv command, 68
 - PWD command (FTP), 559, 569
 - pwexp.pl code listing, 93-95
- Q**
 - q option
 - finger, 40
 - ping, 35
 - query command, 322
 - querying interfaces, 38-39
 - quit command, 53, 257, 264, 441, 474, 559, 569
 - quote command, 480
 - R**
 - R option (ping utility), 35
 - r option
 - netstat, 41
 - opielogin, 566
 - ping, 35
 - rcp, 49
 - ruptime, 37
 - netstat, 30
 - r permission, 85
 - Raptor Systems, 556
 - rarpd (Reverse Address Resolution Protocol daemon), 23, 29
 - rcmd command, 51-52, 190
 - rcp utility, 49-50
 - read function, 465
 - read permission, 85
 - real-time display (KarlBridge packet filter), 290
 - realms (Kerberos), 91
 - reboot command (Filter Manager), 322
 - recovery procedures, 136-139
 - redirect messages (ICMP), 274
 - reject command, 314
 - reject tables, Drawbridge packet filter, 309



- Release 6/Fix 13 (XDM), 196
- reliable protocols, 216
- remote bridging, 289-290
- remote copy (rcp) utility, 49-50
- remote execution, 574-575
- remote logins, LogDaemon, 573
- Remote Procedure Calls, *see* RPCs
- remote sessions, X Windows, 512
- remsh command, 50
- report generators, Black Hole, 508-509, 537
- Report window, 538
- reporting errors, 134-139
 - Gauntlet, 400
 - ICMP (Internet Control Message Protocol), 273
 - TIS Firewall Toolkit, 489-492
- reports
 - authentication server, 491-492
 - Black Hole, 537-540
 - Bytes Per Port*, 540
 - Connections Per Host*, 539-540
 - Top 10 Destinations*, 540
 - Transactions Per Hour*, 538-539
 - TIS Firewall Toolkit
 - FTP (File Transfer Protocol) usage*, 494
 - HTTP (HyperText Transport Protocol) usage*, 494-495
 - mail usage*, 496-497
 - netacl*, 495-496
 - service denial*, 492-493
 - Telnet/rlogin usage*, 498-499
- Reports command (xbh menu), 537
- representing data (OSI Model), 223
- requesting passwords (Kerberos), 582
- requests, FTP, 568-570
- reserved addresses, 11-12
- reset command (Filter Manager), 322
- resolving rules, Black Hole, 519-520
- response teams, 153-157
- responsibilities
 - system administrators, 117
 - users, 116
- REST command (FTP), 559
- restarting inetd, 427-428, 437-438
- restricting connections, FTP, 454-499
- RETR command (FTP), 257, 559, 569
- Reverse Address Resolution Protocol
 - daemon (rarpd), 23, 29
- Revert command (Black Hole), 514
- reviewing network configuration files, 22-25
- rexecd, 184, 190, 574-575
 - diagnostics, 575
- RFCs (Requests for Comments)
 - RFC 950, 13
 - RFC 951, 30
 - RFC 959-560
 - RFC 1048, 30
 - RFC 1178, 17
 - RFC 1244, 99, 106
 - RFC 1320, 162
 - RFC 1704, 168
 - RFC 1760, 162
- .rhosts file, 26, 28
- RIP (Routing Information Protocol)
 - packet filtering, 274
- risk analysis, 102-106
- Risks forum, 148-149
- Rivest Shamir Adleman (RSA) system, 143
- rlogin, 48-49
 - daemon (rlogind), 184, 190, 576-577
 - bugs*, 577
 - diagnostics*, 577



- Gauntlet, 403-404
- proxy agent
 - configuring*, 444-448
 - rules*, 445-449
 - verifying*, 448-449
- TIS Firewall Toolkit, 413, 416
 - rlogin usage reports*, 498-499
- RMD command (FTP), 559, 569
- RNFR command (FTP), 559, 569
- RNTO command (FTP), 559, 569
- The Root Group, 556
- root access, FTP, 55-57
- root equivalency, 81
- root users, permissions, 87
- route utility, 342
 - daemon, 30
- route flapping, 16
- Router Access List (FireWall-1), 371-372
- routers, 327
 - Cisco, 237-281
 - configuring
 - screened host gateways*, 339-343
 - TIS Firewall Toolkit*, 430-499
 - disabling, 332-334
 - network layer (OSI Model), 207
 - screening, 201-235
 - packets, 207
 - tables, 15-16
- Routing Information Protocol (RIP)
 - packet filtering, 274
- RPCs (Remote Procedure Calls), 223
 - FireWall-1, 360, 376
- RSA (Rivest Shamir Adleman) system, 143
- rsh utility, 50-51
 - daemon (rshd), 184, 190, 577-579
- RST flag, 213-215
- rule tables (Black Hole), 515-516, 519-520
- rulebases, ACRB (Access Control Rule Base), 386
- rules
 - ACRB (Access Control Rule Base), 385-387
 - authserv (authentication server), 469-470
 - Black Hole, 515-516
 - resolving*, 519-520
 - user rules*, 527
 - executable, 459
 - InterLock, 382
 - matching, 432
 - modifying, 523
 - permit-host functions, 465
 - priorities, 520
 - TIS Firewall Toolkit, 432
 - FTP proxy (ftp-gw)*, 449-450
 - HTTP proxy (http-gw)*, 461-462
 - rlogin proxy*, 445-446
 - smap*, 455-458
 - Telnet proxy (tn-gw)*, 438-439, 442-443
 - plug-gw*, 481
 - verifying, 436-437
- Rules button (Black Hole), 522, 526
- Rules command (Black Hole), 523
- rules language (FireWall-1), 377-379
- Rules-Base Manager (FireWall-1), 368-372
- ruptime utility, 36-37
- rwho utility, 37
 - daemon, 32



S

- S option (ftpd), 568
- s flag, 194
- s option
 - finger, 40
 - keyinit, 574
 - netstat, 41
 - opiepasswd, 563
- s host address option (arp), 46
- s packet size option (ping), 36
- S-B1-B2 configuration, 346
- S-B1-S configuration, 349
- S-B1-S-B1 configuration, 346
- S-B2 configuration, 343-344
- S-B2-B1 configuration, 346
- S-B2-B2 configuration, 344-346
- Safe-Word, 524
- Safford, David R., 305
- salt, 88-89
- SAP (Service Access Point), 209
- SATAN (Security Administrator's Tool for Analyzing Networks), 551
- SCC (Security Coordination Center), 154
- Schales, Douglas Lee, 305
- SCO
 - files, 25
 - systems, 21
- screened host gateways, 336-337
 - ARP cache table, 341
 - routing configurations, 339-343
- screened subnets, 349-350
- screening routers, 201-235
 - bi-bastion host configuration, 344-346
 - Gauntlet, 398
- ICMP (Internet Control Message Protocol), 340
- KarlBridge packet filter, 297-300
- OSI (Open Systems Interconnection) Reference Model, 203-204
- packet filtering, 202, 216, 225-235
- screened host gateways, 336-337
- security perimeters, 202
- static routing, 341
- TCP/IP-capable networks, 202-203
- Telnet access, disabling, 341
- scripts, syslog, 491
- SecurID, 524
- security
 - access
 - granting, 111-115*
 - points, 125-127*
 - account management, 134-135
 - CERT (Computer Emergency Response Team), 153-154
 - CIAC (Computer Incident Advisory Capability), 156
 - CNSRT (Computer Network Security Response Team), 156-157
 - computers, 59-95
 - IP (Internet Protocol) spoofing, 92*
 - security levels, 60-64*
 - confidentiality, 129-130
 - configuration management, 135-136
 - CSRC (Computer Security Resource and Response Center), 155
 - dialup lines, 126-127
 - encryption, 87-90, 140-146
 - DES (Data Encryption Standard), 141*
 - files
 - /bin/login, 196-198*
 - group, 70-72*
 - .netrc, 56*



- filters, 289-290
- firewalls, 326-354
 - application-level*, 350-354
 - Black Hole*, 501-541
 - dual-homed*, 334-335
 - FireWall-1 Control Module*, 363
 - TIS Firewall Toolkit*, 421-499
- FTP (File Transfer Protocol), 267
- hosts
 - bastion hosts*, 335-346
 - dual-homed hosts*, 327-335
 - host equivalence (Trusted Host Access)*, 27-28, 80-81
- improperly configured systems, 127-128
- insider threats, 128
- Internet, 122-123
- IP (Internet Protocol) spoofing, 92
- jails, 120-121
- Kerberos, 90-92, 146
- levels
 - Canadian Common Criteria*, 62-64
 - United States Department of Defense*, 60-62
- logging violations, 119
- mailing lists, 147-152
- monitoring, 131-133
- network equivalency, 80-83
- newsgroups, 152
- NIST (National Institute of Standards and Technology), 155
- packet filtering, 225-235
- passwords, 115
 - aging*, 72-75
 - files*, 65-72
 - vandals*, 75-77
- permissions, 84-87
- physical security, 128-129
- planning, 98
- policies, 65, 119-122, 130-131
 - AUP (Acceptable Use Policy)*, 109-111
 - designing*, 99-100
 - interpreting*, 123-124
 - privacy*, 116
 - publicizing*, 123-124
 - violations*, 118-123
- port 5555 connections, 247
- probing, 111
- recovery procedures, 136-139
- response teams, 153-157
- risk analysis, 102-106
- screened subnets, 349-350
- screening routers, 201-235
- software bugs, 128
- system administrator responsibilities, 117, 139
- terminal servers, 127
- threat identification, 106-108
- unauthorized access, 107, 131
- Unix, 78-80
- updates, 146-147
- users
 - equivalency*, 82-83
 - identifying*, 109-117
 - responsibilities*, 116
- Security Coordination Center (SCC), 154
- Security Domains level, 62
- seeds
 - OPIE (One-Time Passwords In Everything), 176
 - OTP (one-time password system), 161
 - S/Key, 167



- selecting passwords, 115
- Semaphore Communications, 556
- Semaphore Network Security System, 556
- send command (telnet), 53
- sendmail, 9, 508
- sendmail pathname option (smapd), 458
- sequenced packet delivery, 216
- server option (Makefile), 172
- server-install option (Makefile), 172
- servers
 - authserv (authentication server)
 - passwords*, 475
 - protocols*, 475
 - rules*, 469-470
 - TIS Firewall Toolkit*, 467-480
 - users*, 472-476
 - telnetd, 584
 - ticket-granting, 91
- Service Access Point (SAP), 209
- service denial reports, 492-493
- Service Flag, 516-517
- Service Networks, 511
- Service rule component (Black Hole), 516
- service specifications
 - cmd, 577
 - Drawbridge packet filter, 309-317
 - exec, 574
 - login, 576
 - merging, 314
- Service table (Black Hole), 515
- services, denying, 108
- services file, 24-25
 - editing, 438
- Services Manager (Firewall-1), 367
- Services window, 531
- session keys (Black Hole), 509

- session layer (OSI Reference Model), 222-223
- sessions
 - authmgr, 476-477
 - telnet, 584
- set command (telnet utility), 53
- Set Group ID (SGID), 87
- set target command (Filter Manager), 320
- Set User ID (SUID), 87
- setenv() function, 408
- SGID (Set Group ID), 87
- shadow password files, 134
- sharing data, multi-homed hosts, 327
- shell field, /etc/passwd file, 66
- shells, S/Key login, 582
- Sherwood Data Systems, Ltd., 303-304
- SIGHUP signal, 437
- signal-to-noise ratios, 147-148
- Simple Network Management (SNMP), 366
- SITE command (FTP), 559, 569
- site security (networks), 98-99
- sites
 - FTP (File Transfer Protocol)
 - Bellcore S/Key*, 163, 549
 - COPS (Computer Oracle and Password Program)*, 550
 - Crack*, 550
 - LogDaemon*, 184
 - NRL (U. S. Naval Research Laboratory)*, 166
 - portmapper*, 548
 - Release 6/Fix 13*, 196
 - SATAN*, 551
 - Swatch Logfile Monitor*, 549
 - TAMU Tiger*, 550
 - Tcpdump*, 549



- tcpwrapper*, 548
- TIS Firewall Toolkit*, 422, 548-549
- Venema, Wietse*, 166
- WWW (World Wide Web),
 - CIDR (Classless Inter-Domain Routing), 16
- SIZE command (FTP), 559, 569
- S/Key, 162-163, 166-167, 401, 549
 - calculators, 191-193
 - external*, 193
 - Macintosh*, 192
 - Microsoft Windows (winkey)*, 193
 - Unix programs*, 191-192
 - mailing lists, 197
 - password control table, 579
 - Version 1.0, 160, 165
 - see also* OTP
- skey command, 194
- skey.access, 579-581
- skeysh, 191, 582
- slash (/), 24, 49
- slc command (telnet), 53
- slink daemon, 28
- smail, 459
- smap application, 432, 454
 - configuring, 455-457
 - daemon, 454
 - configuring*, 457-459
 - installing*, 457
 - rules*, 458
 - DNS (Domain Name Service) files, 459-460
 - installing, 455
 - mail usage report (smap-summ.sh), 491, 496-497
 - rules, 455-456
- smart cards, 146
- SMC Elite 16 cards, 301
- SMTP (Simple Mail Transfer Protocol)
 - application layer (OSI Model), 224
 - Black Hole, 537
 - InterLock gateway services, 389-390
- sniffers, 160
- SNMP (Simple Network Management Protocol), 224
 - daemon, 29
 - FireWall-1 Network Objects Manager, 366
 - UDP (User Datagram Protocol), 222
- SNMP Setup screen, KarlBridge packet filter, 295-297
- socket status reports, 44
- socks library, 353
- software
 - Borderware, 555
 - copying, 110
 - COPS (Computer Oracle and Password Program), 550
 - Crack, 550
 - extracting, 305-307
 - Firewall-1 requirements, 359
 - Gauntlet requirements, 395
 - Interlock, 555
 - ACRB (Access Control Rule Base)*, 382, 385-387
 - auditing*, 380
 - configuring*, 383-385
 - e-mail (SMTP gateway services)*, 389-390
 - GPD (Generic Protocol Daemon)*, 395
 - ICMP (Internet Control Message Protocol) redirection*, 381
 - IP (Internet Protocol) forwarding*, 381
 - logging*, 380



- proxy daemons*, 382-383
- rules*, 382
- services*, 387-395
- source routing*, 381
- TCP/IP*, 379
- LogDaemon, 184, 187-189
 - components*, 189-191
 - installing*, 189
 - manual pages*, 568-584
 - passwords, generating*, 189
 - platforms*, 185
 - programs, testing*, 187-189
 - source code*, 184-187
- netacl, 433-438
 - arguments*, 433
 - configuring*, 433-438
 - connections, restricting*, 436, 454
 - host denial messages*, 436-437
 - keywords*, 434-435
 - proxy agent*, 508
 - reports*, 495-496
 - testing*, 436-437
- KarlBridge packet filter requirements, 284-304
- Kerberos, 91-92, 146, 556
 - passwords, requesting*, 582
 - physical security*, 129
- LT Auditor, 555
- Microsafe, 556
- Modem Security Enforcer, 556
- npasswd, 551
- OPIE (One-Time Passwords In Everything), 168-177
 - calculators*, 191-193
 - components*, 180-183, 558-568
 - FTP Server*, 179
 - installing*, 177-198
 - logins, testing*, 176-177
- Makefile*, 171-172
- man pages*, 558-568
- passwords*, 173, 176
- platforms*, 169
- programs, testing*, 172-177
- seeds, verifying*, 176
- source code*, 168-172
- troubleshooting*, 174
- passwd+, 551
- password crackers, 76-77
- Path Key, 556
- SATAN (Security Administrator's Tool for Analyzing Networks), 551
- security risk analysis, 106
- Semaphore Network Security System, 556
- S/Key (Bellcore), 162-163, 166-167, 401, 549
 - calculators*, 191-193
 - mailing lists*, 197
 - password control table*, 579
 - Version 1.0*, 160, 165
- sniffers, 160
- Swatch Logfile Monitor, 549
- TAMU Tiger, 550
- Tcpdump, 549
- tcpwrapper, 548
- TIS Firewall Toolkit, 421-499, 548-549
 - authserv (authentication server)*, 475-492
 - compiling*, 423-424
 - connections, testing*, 436-437
 - help*, 498
 - installing*, 424-426
 - obtaining*, 422-423
 - plug-gw application*, 480-487
 - portscan utility*, 429, 487-488



- proxies*, 449-467
 - reports*, 489-499
 - usage*, 494-499
 - services, disabling*, 426-430
 - TCP/IP, configuring*, 430-431
- Tools, 548
- Tripwire, 551
- Unicenter, 556
- upgrading, 135
- vendors, 552, 555-556
- Software Engineering Institute at Carnegie Mellon University, 153
- Something You Know (SYK), 163
- source code
 - LogDaemon
 - compiling*, 185-187
 - obtaining*, 184-185
 - OPIE (One-Time Passwords In Everything), 168-169
 - compiling*, 170-172
 - obtaining*, 168-169
- Source Firewall option (Black Hole), 517
- source port filtering, 308
- source routing
 - InterLock, 381
 - RIP (Routing Information Protocol), 274
- Source rule component (Black Hole), 516
- SPARC systems, 504
- specifying usernames, FTP connections, 453
- spoofing
 - DNS (Domain Name Service), 433
 - IP (Internet Protocol), 92, 506
- spool area handlers, 29
- spool directory, 455
- standard access lists, 239-240
- StartX_timeout_minutes, 384
- STAT command (FTP), 559, 569
- statements, include, 423
- static routing
 - BSD Unix, 342
 - Gauntlet, 398
 - screened host gateways, 341
 - screening routers, 341
- status command (telnet), 53
- status field
 - authserv database, 476
 - list [group] command, 473
- Status Monitor (FireWall-1), 372
- status reporting (FireWall-1), 362
- Stoll, Cliff, 128
- STOR command (FTP), 257, 479, 559, 569
- storm thresholds, 293-294
- STOU command (FTP), 559, 569
- STREAMS modules, 28
- strings command, 333
- STRU command (FTP), 257, 559, 569
- Structured Protection, 62
- su command, 582-583
- subnet masks, *see* netmasks
- subnets, 12-18
 - netmasks, 12-15
 - screened subnets, 349-350
- Sudo, 556
- SUID (Set User ID), 87
 - dual-homed firewalls, 335
 - root setting, 319
- SUN-NETS mailing list, 151-152
- SunOS systems
 - ifconfig utility, 21
 - kernal parameters, changing, 431
 - TIS Toolkit
 - compiling*, 423
 - installing*, 424-426



supernetting, *see* CIDR (Classless Inter-Domain Routing)
 superwiz user command, 474
 superwiz wizards, 475
 swatch, 513
 Swatch Logfile Monitor, 549
 SYK (Something You Know), 163
 symbolic links, 85
 SYN flag, 214-215
 SYN_RECEIVED socket state, 44
 SYN_SENT socket state, 44
 Synch signals, 560
 SynOptics, 555
 sys_errlist, defining, 424
 syslog, 435, 490-491
 daemon (syslogd), 31
 SYST command (FTP), 559, 569
 System Access Configuration option (Gauntlet), 400
 System Backup option (Gauntlet), 399
 System Defaults database, 78
 System Event/Reporting Configuration option (Gauntlet), 400
 System Integrity Checks option (Gauntlet), 399
 system logger daemon, 31
 system monitoring, 131-132
 System V, STREAMS TCP/IP
 Berkeley interface, 28

T

-T option (opieftpd), 558
 -t option
 netstat, 41
 opieftpd, 558
 uptime, 37

tables
 Drawbridge packet filter, 308
 Filter Manager, 321
 netperm, 431-433
 password control, 579
 routing, 15-16
 route daemon, 30
 rule tables (Black Hole), 515-516
 TAMU Tiger, 550
 tar utility, 305
 target (FireWall-1 Rules-Base Manager), 370
 target options
 Makefile, 172
 TCP Wrapper, 186
 TCB (Trusted Computing Base), 67, 78-80
 TCP (Transmission Control Protocol)
 access lists, 241
 files, 78
 filtering, Drawbridge packet filter, 308-309
 flags, 212-216
 ACK, 212, 268
 FIN, 214
 PSH, 213-215
 RST, 213-215
 SYN, 214
 URG, 212
 FTP (File Transfer Protocol), 259-264
 ports
 connecting, 53
 numbers, 209-211
 sockets, 44
 virtual circuits, 271
 TCP Wrapper, 356-358
 ALL keyword, 358
 compiling, 186-187



- downloading, 184
- files, 357-358
- libwrap.a library, 186
- target options, 186
- TCP/IP (Transmission Control Protocol/
Internet Protocol), 7-57
 - daemons, 28-32
 - bootpd*, 30
 - inetd*, 32
 - ldsocket*, 28-29
 - lpd* (line printer), 29
 - named*, 31
 - narpd*, 29
 - routed*, 30
 - rwohd*, 32
 - slink*, 28
 - snmpd*, 29
 - syslogd*, 31
 - history, 8-9
 - host names, 16-18
 - InterLock, 379
 - mailing lists, 151
 - routing
 - CIDR* (Classless Inter-Domain
Routing), 15-16
 - TIS Firewall Toolkit*, 430-499
 - security perimeters, 202-203
 - subnets, 12-15
 - utilities, 32-56
 - arp*, 45-47
 - Berkeley r*, 48-52
 - dig*, 47-48
 - finger*, 39-40
 - ftp*, 54-56
 - ipconfig*, 38-39
 - netstat*, 40-44
 - ping*, 33-36
 - ruptime*, 36-37
 - rwbo*, 37
 - telnet*, 52-53
 - traceroute*, 44-45
- tcpd file, 356
- Tcpdump, 549
- tcpwrapper, 548
- Telnet, 224
 - daemon (telnetd), 584
 - disabling, 341
 - Gauntlet, 403
 - packet filtering, 269
 - passthrough services, 438
 - proxy agents
 - Black Hole*, 526
 - connections*, 441-442
 - host access rules*, 442-443
 - InterLock*, 387-388
 - testing, 179
- Telnet hostname [port] command, 441
- Telnet proxy gateway service (TIS
Firewall Toolkit), 411-412
- Telnet usage reports (TIS Firewall
Toolkit), 498-499
- Telnet utility, 52-53, 352
- Telnet_Inactivity_Timeout_minutes, 384
- Telnet_Inactivity_Warning_minutes, 384
- TERM variable (su), 583
- Terminal Control database, 78
- terminal servers, 127
- terminal types, 49
- testing
 - applications
 - LogDaemon*, 187-189
 - OPIE* (One-Time Passwords In
Everything), 172-177
 - telnet*, 179
 - TIS Firewall Toolkit*, 436-437,
443-444



- FTP (File Transfer Protocol)
 - daemons*, 178-179
 - proxy (ftp-gw)*, 452-453
- TFTP (Trivial File Transfer Protocol), 222
- threats (security), identifying, 106-108
- three-tuple, 91
- tickets (Kerberos), 91
- Time Exceeded messages, 33
- Time table (Black Hole), 515
- TIME_WAIT socket state, 44
- timeout seconds option
 - rlogin-gw, 445
 - tn-gw, 439
- timeout seconds rule (plug-gw), 481
- timeout secondsvalue option
 - ftp-gw, 450
 - http-gw, 461
- timeout value option (smap), 456
- TIS (Trusted Information Systems, Inc.)
 - URL, 422, 548-549
 - see also* Firewall Toolkit (TIS); Gauntlet
- TIS.COM firewall mailing list, 553
- tn-gw (Telnet proxy)
 - commands, 441
 - configuring, 438-441
 - connections, 441-442
 - host denial messages, 440
 - rules
 - clauses*, 438-439
 - host access*, 442-443
 - verifying, 443-444
- tn-gw-summ.sh (Telnet/rlogin usage report), 491, 498-499
- token management, session layer (OSI Model), 222-223
- Toolkit, *see* Firewall Toolkit (TIS)
- tools, *see* software
- Top 10 Destinations report, 540
- Top button (Black Hole), 522
- Top command (Navigate menu), 523
- Total Bytes In reports, 539
- Total Bytes Out reports, 539
- traceroute utility, 44-45
- track (FireWall-1 Rules-Base Manager), 370
- traffic, analyzing, 508
- trailers option (ifconfig utility), 20
- Transactions Per Hour report, 538-539
- Transfer rule component (Black Hole), 516
- Transmission Control Protocol, *see* TCP
- Transmission Control Protocol/Internet Protocol, *see* TCP/IP
- Transparent mode (Black Hole), 518
- transparent operations, 503
- Transparent Promote option (Black Hole), 517
- transport addresses, 209
- transport layer (OSI Reference Model), 207-222
- Tripwire tools, 551
- Trojan-horse programs, 129
- troubleshooting
 - OPIE (One-Time Passwords in Everything), 174
 - user equivalency, 83
- trusted access, 80-81
- Trusted Computer Standards Evaluation Criteria, 60
- Trusted Computing Base (TCB), 67, 78-80
- trusted entries, 80
- Trusted Host Access, 27-28



Trusted Information Systems, Inc.,
 see TIS
Trusted Network Configuration option
 (Gauntlet), 400
trusted user access, 82-83
twisted-pair cable, 18
TYPE command (FTP), 257, 559, 569

U

-u option (ruptime), 37
U.S. Department of Defense security
 standard levels, 60-62
UDP (User Datagram Protocol),
 216-222
 broadcast data, 221
 DNS, 273
 extended access lists, 241
 FireWall-1, 360, 375
 packet filtering, 271-273
 port numbers, 219-221
 robustness of, 216
 Service flag options, 517
UDP Relay proxy agent, 508
UID assignments (TIS Firewall Toolkit),
 405
UID field, /etc/passwd file, 66
UMASK command (FTP), 560, 570
unauthorized access, 107, 436
Unicenter, 556
United States Naval Research Laboratory
 (NRL), 160, 166
Unix
 BSD Unix
 Gauntlet, 396
 routing, 332-334, 342
 calculators, 191-192
 dual-homed firewalls, 331
 encryption methods, crypt(3), 88-89
 file types, 84-85
 security
 I&A (Identification and Authentication), 79
 mailing lists, 148
 TCB (Trusted Computing Base),
 78-80
 time, tracking, 80
Unix-like Password, 524
unlearned packets, passing, 292
Unreachable message, 33
unreliable protocols, 216
unset command (Telnet utility), 53
Up button (Black Hole), 522
Up command (Black Hole), 523
up option (ifconfig utility), 20
Update Group window, 524
Update User window, 525-526
upgrading software, configuration
 management, 135
upload command (Filter PC), 321
URG flag, 212
URLs (Uniform Resource Locators)
 Bellcore S/Key, 163, 549
 CIDR (Classless Inter-Domain
 Routing), 16
 COPS (Computer Oracle and
 Password Program), 550
 Crack, 550
 LogDaemon, 184
 NRL (U. S. Naval Research Laboratory), 166
 portmapper, 548
 Release 6/Fix 13, 196
 SATAN, 551
 Swatch Logfile Monitor, 549
 TAMU Tiger, 550



- Tcpdump, 549
- tcpwrapper, 548
- TIS Firewall Toolkit, 422, 548-549
- Venema, Wietse, 166
- Use privileged port option (Black Hole), 517
- user access, granting, 111-115
- User Authentication Management
 - option (Gauntlet), 400
- USER command (FTP), 252, 257, 559, 570
- user commands, 48-57
 - Berkeley r, 48-52
 - rcmd*, 51-52
 - rcp*, 49-50
 - rlogin*, 48-49
 - rsh*, 50-51
 - ftp, 54-56
 - telnet, 52-53
- User Datagram Protocol (UDP), 216-222
- user equivalency, 82-83
 - configuring, 28
 - troubleshooting, 83
- user field, list [group] command, 473
- User Icon window, 526
- User rule component (Black Hole), 516
- User table (Black Hole), 515
- user userid keyword (netacl), 435
- user uucp (skey.access file), 580
- USER variable (su), 583
- user-management commands (Black Hole), 523
- user_name option (opiesu), 567
- userid name option
 - smap, 456
 - smapd, 458
- userid name rule (authserv), 470
- userid user option
 - ftp-gw, 450
 - http-gw, 461
 - rlogin-gw, 445
 - tn-gw, 439
- userlist field, /etc/group file, 71
- <user_name> option (opieinfo), 565
- username argument, 573
- username field, /etc/passwd file, 65
- usernames, specifying, 453
- users
 - identifying, 109-117
 - responsibilities, 116
 - authserv (authentication server),
 - adding, 472-476
 - Black Hole, 521-527
 - accounts*, 521-523
 - authenticating*, 524-526
 - creating*, 523-5245
 - rules*, 527
 - User icon*, 526-527
 - defining, 83
 - OTP (one-time password authentication system), configuring, 194-196
- Users icon (Black Hole), 521
- /usr/src/sys, 333
- /usr/sys/conf, 333
- utilities, 32-57
 - arp, 45-47
 - Berkeley r, 48-52
 - rcmd*, 51-52
 - rcp*, 49-50
 - rlogin*, 48-49
 - rsh*, 50-51
 - dig, 47-48
 - finger, 39-40
 - ftp, 54-56
 - ifconfig, 38-39



- netstat, 30, 40-44
- ping, 33-36
- portscan, 429
- ruptime, 36-37
- rwho, 37
- telnet, 52-53
- traceroute, 44-45
- uuencode command, 142

V

- v option
 - netscan, 488
 - opieinfo, 565
 - opiekey, 562
 - opiepasswd, 563
 - ping utility, 36
- values
 - maxbytes, 456
 - password aging, 72-74
- vandals, 75-77
- vendors (software), 552, 555-556
- Venema, Wietse, 160
 - URL, 166
 - see also* LogDaemon
- verbose mode (netscan), 488
- verification (FireWall-1 Rules-Base Manager), 370
- Verified Design level, 62
- verifying
 - proxies, TIS Firewall Toolkit
 - FTP proxy*, 452-453
 - rlogin proxy*, 448-449
 - Telnet proxy (tn-gw)*, 443-444
 - rules, netacl program*, 436-437
 - seeds, OPIE (One-Time Passwords In Everything), 176

- viewing passwords, OPIE (One-Time Passwords In Everything), 176
- virtual circuits, 212-216, 271
- Virtual Private Networks (VPNs), 502
- VIRUS-L mailing list, 149
- VPNs (Virtual Private Networks), 502

W

- w option (finger), 40
- w permission, 85
- wais function, 465
- wakeup value option (sampd), 458
- warn message level (Black Hole), 513
- watchdog reboot timer (KarlBridge packet filter), 290
- weekly-report.sh, 491
- welcome-msg filename option
 - ftp-gw, 450
 - rlogin-gw, 445
 - tn-gw, 439
- Well Known Services (WKS), 209
- Well-Known Port 21 (FTP), 248
- Well-Known Services (WKS), 272
- wheel group, 71
- White Hole, 511
- Windows, WinKey calculator, 193
- windows
 - Report, 538
 - Services, 531
 - Update Group, 524
 - Update User, 525-526
 - User Icon, 526
- WinKey calculator, 188, 193
- wiz user command, 474
- wizards, 475
- WKS (Well Known Services), 209, 272
- Worm incident, 108



write function, 465
 write permission, 85-86
 WWW (World Wide Web)
 clients
 non-proxy-aware, 462-463
 proxy-aware, 463
 FireWall-1, 376
 sites, CIDR (Classless Inter-Domain Routing), 16

X

X Display Manager, *see* XDM
 x permission, 85
 X Windows, 224
 Black Hole, 512-514
 InterLock, 390-391
 OTP (one-time password system),
 196-198
 packet filtering, 270
 proxy (TIS Firewall Toolkit), 466-467
 compiling, 423
 remote sessions, 512
 x[-gw] [display/hostname] command,
 441
 X_Inactive_timeout_minutes, 384
 X11 protocol, 248
 xbh menu commands, Reports, 537
 XCUP command (FTP), 559, 570
 XCWD command (FTP), 559, 570
 XDM (X Display Manager), 512
 Release 6/Fix 13, 196
 XDR (External Data Representation),
 223
 XMKD command (FTP), 559, 570
 XPWD command (FTP), 559, 570
 XRMD command (FTP), 559, 570

Z

z command (telnet), 53
 zmailer, 459
 zones of risk
 dual-homed firewalls, 329
 screening routers, 202