INDEX

Numerics

3DES, 130–131
limitations of, 132
strengths of, 131
802.11b standard, 278
APs, associating, 304
enhancing security, 311–312
hacking tools
AirSNORT, 282, 288, 297, 310, 313, 316–317
NetStumbler, 313–315
packet sniffers, 315–316
SSIDs, 303–304
WEP, 302–306
limitations of, 306
802.11g standard, 279, 282

A

AAA, 115
accounting, 117–118
authentication, 116
authorization, 116
aaa new-model command, 218
acceptable use policies, 54–55
confidential information, 57
passwords, specifying criteria for, 57–58
prohibited activities, 59–62
access control, 86
accounting, 117–118
ACLs, 89–90, 199
applying to vty ports, 227
deny statements, 94
grocery list analogy, 91–94
implicit deny statements, 196
limitations of, 95
lock and key, 199
permit statement, 205
static, 196
active reconnaissance, 17
ad-hoc WLANs, 283
AES (Advanced Encryption Standard), 128, 232
AH (Authentication Header), 250
AirSNORT, 282, 288, 297, 310, 313, 316–317
all-in-one firewalls, implementing, 171
anomaly detection, 334

antennas, 290–291
applets (Java), blocking, 201
application level firewalls, 105
application specific monitoring, 200–201
applications
attacks, 28
for performing exploitation attacks, 357
applying
crypto maps to interfaces, 268
passwords to console port, 227
APs (access points)
antennas, 290–291
associating, 304
bandwidth limitations, 285
distance limitations, 285
misconfigured, 300–302
rogue APs, 298–300
SSIDs, 289, 303–304
ARIN (American Registry for Internet Numbers), 100
ARP poisoning, 362
ARP proxy, disabling, 223
ARP spoofing attacks, 362
ASA (adaptive security algorithm), 170
assessing vulnerability, tools, 374–383
associating, 304
atomic signatures, 210
attacks
Cisco IOS IDS signatures, 211
covering tracks, 31–33
DoS, 358
on WLANs, 297–298
ping-based, 360–361
preventing, 361–362
smurf, 360
SYN flood, 361
downstream liability, 160
enumerating, Microsoft Windows, 22–25
escalating privilege, 30–31
firewalking, 366
gaining access, 26
IP spoofing, 170, 356
applications used, 357
land, 364
man-in-the-middle, 362
ARP spoofing, 362
ping of death, 365
ping pong, 365
ping-based, 360
reconnaissance, 13
active, 17
DNS, 16
DNS tools, 15–17
goals of, 13–15

scanning, 18–20
get command, 21–22
vulnerability scanning, 22
session hijacking, 356
applications used, 357
SYN flood, 365–366
preventing, 219
targeted
misconfiguration attacks, 28–29
on applications, 28
on operating systems, 27
script attacks, 29–30
teardrop, 365
U.S. as source, 34
Xmas tree, 364
authentication, 116, 134
local, TACACS+, 218
on IPSec VPNs, 246
per user, 199
RADIUS, 118–119
authenticity of data, 132
authorization, 116
per user, 199
automated attacks, 27

B

back doors, 363
applications used, 31–33
bandwidth, limitations on WLANs, 285–286
banners, configuring, 226–227
benefits of VPNs, 239–240
bit buckets, 107
black hole routes, 224
blocking Java applets, 201
brute force attacks, 41

C

capturing core dumps, 220
carrier protocol, 247
CAs (Certificate Authorities), 261
case studies
DMZs, necessity of, 176–177
firewalls
deploying with mail server in DMZ, 181–184
deploying with mail servers, 178–180
CBAC (Context-Based Access Control), 197–200
application specific monitoring, 200–201
communication session states, tracking, 199

content-based packet inspection, 202–203
FFS security process, 204–207
dynamic filtering, 198
IDS, 207–208
intended use, 209
operational overview, 209
packet auditing process, 211–213
signatures, 208–210
Java applet blocking, 201
limitations of, 213–214
session logging, 199
CDP (Cisco Discovery Protocol), disabling, 225
CEF (Cisco Express Forwarding), enabling, 220
centralized sensor management, 328
CHAP (Challenge Handshake Authentication Protocol), 137
Chappell, Laura, 210
chargen service, disabling, 217
checksums, MD5, 135
choke points, edge routers as, 193
permissible traffic, 195
choke routers
limitations of, 196
static ACLs, 196
CIS (Center for Internet Security), 36
Cisco IOS IDS, 209
packet auditing process, 211–213
signatures, 210
Cisco IOS Software
ARP proxy, disabling, 223
configuration files, encrypted, 218
core dump facility, 220
error reporting facility, 208
facilities, 208
FFS, 190
benefits of, 198–201
content-based packet inspection, 202–207
IDS, 207–209
limitations of, 213–214
process-switched packets, 205
FFS (Firewall Feature Set), CBAC, 197–198
Firewall Feature Set, benefits of, 192
Secure IOS Template, 214
topology, 215–228
Cisco PIX Firewalls, configuring VPNs for client access, 268–272
Cisco SDM Security device manager, 215
classes of IPv4 addresses, 100
client-based filtering, 110
clock timezone command, 220
combining key IDS functions, 336

commands
aaa new-model, 218
clock timezone, 220
enable secret, 218
get, 21–22
ip accounting access-violations, 223
ip cef, 220
ip classless, 219
ip multicast boundary, 223
ip subnet-zero, 219
ip tcp intercept connection-timeout, 219
ip tcp intercept watch-timeout, 219
ip tftp source-interface, 220
ip verify unicast reverse-path, 222–224
line vty, 227
nbstat, 24
net view, 24
nslookup, 15–17
ntp authenticate, 221
service nagle, 216
service password-encryption, 217
service sequence numbers, 217
show privilege, 117
community strings (SNMP), securing access, 225
comparing
L2TP and PPTP, 140–141
SSH and Telnet, 146–149
TACACS+ and RADIUS, 121
compound signatures, 211
conduit permit statement, 165
confidential information, defining for acceptable use policies, 57
configuration files, encrypted, 218
configuring
banners, 226–227
Cisco PIX VPNs for client access, 268–272
firewalls
inbound access policy, 172–173
outbound access policy, 173
null0 interface, 221
routers as VPN peers, 264
IPSec, 264–267
ISAKMP, 260–263
congestion, Nagle algorithm, 216
connection aware technologies, 97
connection establishment phases (VPNs), 255–258
console logging, 218
console port, applying passwords, 227

content filtering, 108–109
client-based filtering, 110
limitations of, 111
server-based filtering, 111
content-based packet inspection, 202–207
control messages, 137
controlling access, 86
core dump facility, 220
Core Impact, 384–388
Corporate Security Team, 54
Counterpane Internet Security, 138–139
creating crypto maps, 266
crypto maps, applying to interfaces, 268
CVE (common vulnerabilities and exposures) database, 35, 328

D

data authenticity, 132
data classification policy, protecting sensitive information, 7
data integrity, 132
on IPSec VPNs, 246
data packets, 137
DDoS attacks, 39, 358
ping-based, 360–361
preventing, 361–362
smurf, 360
SYN flood, 361
DDoS Daemons, 359
deception systems, 347
default manufacturer SSIDs, 303–304
deny statements, 94
DES (Data Encryption Standard) encryption, 127
RSA DES Challenge web page, 128
strengths of, 128–130
detecting anomalous activity, 334
development of Intrusion Detection, 325
devices
firewalls, 158
ASA, 170
basic functions of, 167–168
DMZ, 174–177
downstream liability, 160
implementing, 170–171
inbound access policy, configuring, 172–173
inside interfaces, 169
limitations of, 184–185
need for, 159–160

outbound access policy, configuring, 173
outside interfaces, 169
rules, 161
security policies, 163–165
SPI, 166, 168
Diffie-Hellman algorithm, 257
digital signatures, 134–135
directed broadcast, 360
disabling
ARP proxy, 223
CDP, 225
chargen and echo services, 217
ICMP mask reply messages, 223
ICMP redirect messages, 222
IP directed broadcasts, 222
source routing, 223
disaster recovery, 373
displaying
MOTD banners, 226–227
user privilege level, 117
distance limitations of WLANs, 284
DMZs, 174
case study, 176–177
mail server deployment
case study, 181–184
placement of, 175–176
DNS, in passive reconnaissance, 15–17
DoS attacks, 39, 358
on WLANs, 297–298
ping-based, 360–361
preventing, 361–362
smurf, 360
SYN flood, 361
downstream liability, 34, 160
Dsniff, 357
dumpster diving, 4
dynamic ACLs, lock and key, 199
dynamic filtering, 198
dynamic NAT, 102
dynamic proxy firewalls, 106

E

EAP (Extensible Authentication Protocol), 307
EAP-Cisco Wireless, 309
EAP-MD5, 308–309
EAP-TLS, 310
EAP-TTLS, 311
eavesdropping on WLANs, 295–297
echo service, disabling, 217
edge routers, 190
as network choke point, 192–193
limitations of, 196
permissible traffic, 195
static ACLs, 196

as packet inspector, 197–198
versus firewalls, 191
eliminating false positives, 328
enable secret command, 218
enable secret passwords, 218
enabling
CEF, 220
logging, 217
RADIUS, 119
SSH, 228
encrypted configuration files, 218
encryption, 126
3DES, 130–131
limitations of, 132
strength of, 131
DES, 127
RSA DES Challenge web page, 128
strength of, 128–130
passwords, 217
SSH, 145–146
authentication ciphers, 150
limitatations of, 152–153
operation, 149–151
port forwarding, 151
SecureCRT client, 151
versus Telnet, 146–148
encryption modes (VPNs)
transport mode, 249
tunnel mode, 248
enhancing wireless security, 311–312
enterprise firewalls, implementing, 171
enumerating Microsoft Windows, 22–25
error reporting facility on Cisco IOS Software, 208
escalating privilege, 30–31
ESP (Encapsulated Security Protocol), 250
ESP (Encapsulating Security Payload), 140
establishing IPSec SAs, 251
Ethereal, 296
ettercap, 146, 357
event correlation, 327
examples of security policies, 81–82
explicit permit access model, 203
exploits, 356
applications attacks, 28
code, 31
DoS, 359
misconfiguration attacks, 28–29
operating system attacks, 27
script attacks, 29–30
tools for accomplishing, 357
extended ACLs, 199
extended IP ACLs, 90
extended TACACS, 119–120

external network security assessments, performing, 369–370
extranet connection policies, 74–77
extranet VPNs, 233, 238

F

facilities, 208
core dump, 220
false positives, eliminating, 328
FFS (Firewall Feature Set), 197
benefits of, 198–200
application specific monitoring, 201
Java applet blocking, 201
VPNs, 201
CBAC, 197–198
application specific monitoring, 200
communication states, tracking, 199
dynamic filtering, 198
session logging, 199
content-based packet inspection, 202–207
IDS, 207–208
intended use, 209
operational overview, 209
packet auditing process, 211–213
signatures, 208–210
limitations of, 213–214
process-switched packets, 205
security process, 203–205
firewalking, 366
firewalls, 158, 191. *See also* FFS (Firewall Feature Set)
all-in-one, implementing, 171
application level, 105
ASA, 170
basic functions of, 167–168
DMZs, 174
case study, 176–177
placement of, 175–176
downstream liability, 160
dynamic proxy firewalls, 106
enterprise, implementing, 171
implementing, 170
inbound access policy, configuring, 172–173
inside interfaces, 169
limitations of, 184–185
need for, 159–160
outbound access policy, configuring, 173
outside interfaces, 169
personal, implementing, 170
proxy firewalls, limitations of, 107–108

routerwalls, 197
rules, 161
security policies, 163–164
and firewall configuration, 165
conduit permit statements, 165
SPI, 166–168
standard proxy firewalls, 105
versus edge routers, 191
footprinting, 13–15

G

Gartner Dataquest, 232
get command, 21–22
goals
of reconnaissance, 13–15
of VPNs, 239–240
GRE (Generic Routing Encapsulation), 136

H

hackers
escalating privilege, 30–31
intelligence preparation operations, 13
script kiddies, 9
hacking tools
AirSNORT, 282, 288, 297, 310, 313, 316–317
NetStumbler, 313–315
wireless packet sniffers, 315–316
half-open attacks, 365–366
half-open sessions, 207
half-open sockets, 219
Hammersley, Ben, 286
hash checks, 135
hash values, 133
Haystack Project, 325
helix antennas, 290–291
HIDS (host-based intrusion detection sensors), 327, 332
Honeypots, 345–347
design strategies, 348–349
host-based IDSs, 327

I

IANA (Internet Assigned Numbers Authority), 100
IBSS (Independent Basic Service Set), 283
ICAT metabase, 38

ICMP (Internet Control Message Protocol)
connection tracking on CBAC, 199
flooding, 42
mask reply message, disabling, 223
messages, 42
ping-based attacks, 360–361
redirect messages, disabling, 222
smurf attacks, 360
IDSs, 321–323
anomaly detection, 334
communication stream reassembly, 333
development of, 326
HIDS, 332
host-based, 327
in-line intrusion detection, 207
key functions, 327–329, 336
log analysis, 336
network-based, 327
NIDS, 330–331
on FFS, 207–208
intended use, 209
operational overview, 209
packet auditing process, 211–213
signatures, 208–210
protocol analysis, 333
signature/pattern matching, 334–335
standards-based implementation, 328
tweaking, 323
IEEE 802.11b standard, 278
IEEE 802.11g standard, 279, 282
IKE, 251–253
phases of VPN creation, 255–258
implementing
firewalls, 170
all-in-one firewalls, 171
enterprise firewalls, 171
personal firewalls, 170
with mail server in DMZ, case study, 181–184
with mail servers, case study, 178–180
VPNs, 240–242
implicit deny statements, 196
inbound access policy, firewall configuration, 172–173
information handling security assessments, 373
infrastructure WLANs, 283
in-line intrusion detection, 207, 210
inline wiretaps, 330
INRGI website, 214
inside interfaces, 169
inspecting packets. *See* SPI
intelligence preparation operations, 13
intended use of FFS IDS, 209
internal network security assessments, performing, 367–369

Internet, extranet connection policies, 74–77
Internet Storm Center, 37
intrusion detection, development of, 325
intrusion prevention, 329
ip accounting access-violations command, 223
ip cef command, 220
ip classless command, 219
IP directed broadcasts, disabling, 222
ip multicast boundary command, 223
IP spoofing, 40, 356
applications used, 357
IP Spoofing attacks, 170
ip subnet-zero command, 219
ip tcp intercept connection-timeout command, 219
ip tcp intercept watch-timeout command, 219
ip tftp source-interface command, 220
ip verify unicast reverse-path command, 222–224
IPSs (Intrusion Prevention Systems)
limitations of, 342–45
responses and actions, 337–338
Snort, 339, 342
IPSec, 139
ESP, 140
router configuration, 264–267
SAs, 251
VPNs, 243–245
AH, 250
authentication, 246
connection establishment phases, 255–258
data integrity, 246
ESP, 250
IKE, 252–253
ISAKMP, 250, 254
SAs, 250–251
transport mode, 249
tunnel mode, 248
IPv6, 100
ISAKMP (Internet Security Association Key Management Protocol), 250, 254
router configuration, 260–263
island analogy of VPNs, 233–235
ISO17799 standard, 79

J-K

Java applet blocking, 201
Jones, Matt, 28

keepalives (TCP), enabling, 216
key IDS functions, 327–329

L

L2F (Layer 2 Forwarding), 140
L2TP (Layer 2 Tunneling Protocol), 139
benefits of, 141
LAC, 142
network architecture, 142
operation, 142–143
versus PPTP, 140–141
L2TP Network Server (L2TP Network Server), 140
LAC (L2TP Access Concentrator), 140–142
land Attack, 40
land attacks, 364
layered security, 86
LEAP, 309
legality of WarDriving, 292
liability, downstream, 34
limitations
of ACLs, 95
of choke routers, 196
of content filtering, 111
of FFS, 213–214
of firewalls, 184–185
of IPS, 342–343, 345
of NAT, 103–104
of PKI, 114–115
of proxy firewalls, 107–108
of PPTP, 138–139
of SSH, 152–153
of WEP, 306
line vty command, 227
local authentication, TACACS+, 218
lock and key dynamic ACLs, 199
log analysis, 336
log messages, time stamping, 216
logging
console logging, 218
enabling, 217
NetFlow, 225
Syslog, 225
login sessions, SSH, 145
authentication ciphers, 150
limitations of, 152–153
operation, 149–151
port forwarding, 151
versus Telnet, 146–149

loopback interfaces, configuring as log message source, 221
loose source routing, 41
Lucifer algorithm, 127

M

MAC address filtering, 307
mail servers
deploying in DMZ, case study, 181–184
deploying with firewalls, case study, 178–180
manageability of VPNs, 241
man-in-the middle attacks, 362
mask reply messages (ICMP), disabling, 223
MD5 (Message Digest 5), 132–135
digital signatures, 134
hash values, 133
message logging
enabling, 217
loopback interfaces, configuring as message source, 221
Microsoft Windows, enumerating, 23–25
misconfiguration attacks, 28–29
misconfigured APs as threat to WLAN security, 300–302
monitoring, 87
MOTD banners, configuring, 226–227
multicast filtering, applying to interfaces, 223
multi-deception systems, 348

N

Nagle congestion control algorithm, 216
NAT (Network Address Translation), 99, 101–102, 172
dynamic NAT, 102
limitations of, 103–104
overloading, 102
static NAT, 102
NBAR (Network Based Application Recognition), 196
nbtstat command, 24
necessity of DMZs, 176–177
necessity of firewalls, 159–160
Nessus, 376–379
net view command, 24
NetFlow, 225
NetStumbler, 313–315
NIDS (Network-Based Intrusion Detection Systems), 327–331

NIST (National Institute of Standards and Technology), 127
NSA (National Security Agency), 127
nslookup command, 15–17
NTP (Network Time Protocol), 221
ntp authenticate command, 221
null0 interface, configuring, 221

O

one-way hash algorithms
MD5, 133–135
operating systems
attacks, 27
Windows, enumerating, 23–25
operational overview of FFS IDS, 209–210
organizations
CERT, 36
CIS, 36
ICAT metabase, 38
Internet Storm Center, 37
SANS, 36
SCORE, 37
OSPF (Open Shortest Path First), 125
outbound access policy, firewall configuration, 173
outside interfaces, 169
overloading, 102

P

packet auditing process on Cisco IDS, 211–213
packet filtering
ACLs, 89–90
deny statements, 94
grocery list analogy, 91–94
limitations of, 95
dynamic, 198
packet inspection
application specific monitoring, 200
CBAC, 197–200
application specific monitoring, 201
Java applet blocking, 201
limitations of, 213–214
VPNs, 201
content-based, 202–203
FFS security process, 204–207
on edge routers, 197
SPI, 166–168
packet sniffers, 296, 358

packets
communication stream reassembly on IDSs, 333
source routing, 223
SPI, 97–98
PAP (Password Authentication Protocol), 137
passenger protocol, 247
passive reconnaissance, DNS, 16
password policies, 63–65
password construction guidelines, 66–68
password protection standards, 68–69
passwords
applying to console port, 227
enable secret, 218
encrypting, 217
specifying criteria for acceptable use policies, 57–58
SSIDs, 302–304
PAT (Port Address Translation), 172
patching, 87
pattern matching, 334–335
patterns of trust, 357
penetration testing, 366–370
tools, 383–390
per user authentication, 199
performing
security assessments, 366
external vulnerability and penetration assessment, 369–370
internal vulnerability and penetration assessment, 367–369
physical security, 371
procedural risk assessments, 373
service providers, 374
vulnerability assessments, tools, 374–383
permissible traffic on choke routers, 195
permit statements, 205
personal firewalls, implementing, 170
physical security, assessing, 371
Ping of Death, 39
ping of death attacks, 365
ping pong attacks, 365
ping scans, 40
ping-based attacks, 360
PKI (Public Key Infrastructure), 112–115
placement
of NIDS, 331
of DMZs, 175–176

policies, 163–164
acceptable use, 54–55
confidential information, 57
passwords, 57–58
prohibited activities, 59–62
comparing with firewall configuration, 165
examples of, 81–82
extranet connection policies, 74–77
ISO17799 standard, 79
levels of trust, 51–53
on firewalls, conduit permit statement, 165
password policies, 63–65
password construction guidelines, 66–68
password protection standards, 68–69
review team, 54
types of, 48–50
VPN security policies, 70–74
port forwarding, SSH, 151
port mirroring, 330
port monitors, 347
port scan attacks, 39
PPP (Point-to-Point Protocol), L2TP, 139
benefits of, 141
LAC, 142
network architecture, 142
operation, 142–143
versus PPTP, 140–141
PPTP (Point-to-Point Tunneling Protocol), 135–137
GRE, 136
limitations of, 138–139
versus L2TP, 140–141
preventing
DoS attacks, 361–362
exploitation attacks, 358
SYN-flood attacks, 219
Private IP Addresses, 100
privilege levels, 116
escalating, 30–31
procedural risk assessments, 373
process-switched packets, 205
production Honeypots, 347
protocol analysis, 333
proxies, 105
proxy firewalls
dynamic proxy firewalls, 106
limitations of, 107–108
standard proxy firewalls, 105
Public IP Addresses, 100–101
public-key algorithms, 258

R

RADIUS (Remote Authentication Dial-In User Service), 118
enabling, 119
versus TACACAS+, 121
rate limiting traffic, 222
read/write mode (SNMP), 225
reassembling packets via IDSs, 333
reconnaissance, 13
active, 17
DNS, 16
DNS tools, 15–17
goals of, 13–15
recorded routes, 41
redirect message (ICMP), disabling, 222
reliability of VPNs, 242
remote access VPNs, 233, 237
split tunneling, 242
remote login sessions, SSH, 145
authentication ciphers, 150
limitations of, 152–153
operation, 149–151
port forwarding, 151
versus Telnet, 146–149
research Honeypots, 347
response teams, 88
Retina, 379–383
risk assessment
external, performing, 369–370
internal, performing, 367–369
physical security, performing, 371
procedural risk assessments, performing, 373
service providers, 374
tools
Nessus, 376–379
Retina, 379–383
vulnerability scanners, 374–376
role specific security, 87
routers
configuring as VPN peers, 264
IPSec, 264–267
ISAKMP, 260–263
edge routers, 190
as network choke point, 192– 196
as packet inspector, 197–198
versus firewalls, 191
routerwalls, 197
routing protocols, 125
RPF (Reverse Path Forwarding), 224
RSA DES Challenge web page, 128

S

SANS (SysAdmin, Audit, Network, Security) Institute, 36
SAs (security associations), 250–251
IPSec, establishing, 251
ISAKMP, 254
scalability of VPNs, 236, 242
scanning, 18–20
get command, 21–22
NMAP, accuracy of, 19
vulnerability scanning, 22
Schneier, Bruce, 138
SCORE, 37
script attacks, 29–30
script kiddies, 9, 196
Secure IOS Template, 214
topology, 215—228
SecureCRT, 151
security policies, 47–48, 163–165
on firewalls, conduit permit statement, 165
types of, 48–50
security protocols, 125
security through obscurity, 8
sequence number tracking, 199
server-based filtering, 111
service nagle command, 216
service password-encryption command, 217
service sequence-numbers command, 217
session hijacking, 356
applications used, 357
session logging, 199
sh run command, 147
Shipley, Peter, 291
show privilege command, 117
shunning, 337
signatures, 210
Cisco IDS packet auditing process, 211–213
pattern matching, 334–335
IDS responses to, 208
site-to-site VPNs, 233, 237, 248
router configuration, 264
IPSec, 264–267
ISAKMP, 260–263
smurf attack, 41, 360
sniffers, 43, 358
WLAN-capable, 295–297, 315–316
sniping, 337
SNMP (Simple Network Management Protocol), 225
Snort, 339, 342
social engineering, 5–7
source routing, 41, 223
spam, WarSpamming, 292–293

SPI (Stateful Packet Inspection), 95–96, 166–168
application specific monitoring, 201
limitations of, 99
packet flow, 97–98
Spitzner, Lance, 346
split tunneling, 242
spoofing attacks, 40, 170
SSH (Secure Shell), 145
authentication ciphers, 150
enabling, 228
limitations of, 152–153
operation, 149–151
port forwarding, 151
SecureCRT client, 151
versus Telnet, 146–149
SSIDs (Service Set Identifiers), 289, 303–304
SSL (Secure Socket Layer), 112
standard ACLs, 199
standard IP ACLs, 90
standard proxy firewalls, 105
standards-based IDS implementation, 328
static ACLs, 196
static NAT, 102
Stevens, Richard, 361
strength
of 3DES encryption, 131
sof DES encryption, 128–130
strict source routing, 41
STS (Station-to-Station) protocol, 251
symmetric key algorithms, 258
SYN flood attacks, 39, 361, 365–366
preventing, 219
syslog (System Message Logging), 208, 225

T

TACACS+, 119–121
for local authentication, 218
targeted attacks, 27
applications attacks, 28
misconfiguration attacks, 28–29
operating system attacks, 27
script attacks, 29–30
targeted business sectors, 34
targets of choice, 10
assessing vulnerability, 10–12
targets of opportunity, 7
assessing vulnerability, 9–10
Security Through Obscurity, 8
versus targets of choice, 10
TCP (Transmission Control Protocol)
keepalives, enabling, 216
Nagle algorithm, 216
sequence number tracking, 199

TCP Intercept, black hole routes, 224
TCP/IP model, 96
tear drop attacks, 40
teardrop attacks, 365
Telnet
ettercap, 148
Nagle congestion control algorithm, 216
versus SSH, 146–149
TFTP, 220
third party agreements, 76
time stamping log messages, 216
time synchronization, NTP, 221
time zones, standardizing on routers, 220
tools
for hacking
AirSNORT, 282, 288, 297, 310, 313, 316–317
NetStumbler, 313–315
wireless packet sniffers, 315–316
NMAP, 19
topology of Secure IOS Template, 215–228
traffic, rate limiting, 222
transport mode, 249
trust, 51–54
TTL (Time-To-Live) field, role in firewalking attacks, 366
tunnel mode (IPSec), 248
tunneling
IPSec, 139
L2TP, 139
benefits of, 141
LAC, 142
network architecture, 142
operation, 142–143
PPTP, 136–137
GRE, 136
limitations of, 138–139
versus L2TP, 140–141
VPNs, 247
tweaking IDSs, 323

U

UDP (User Datagram Protocol)
connection tracking on CBAC, 199
flooding, 39
unauthorized access, preventing on WLANs, 301

V

VPNs, 201, 231, 236
AES, 232
configuring Cisco PIX Firewall for client access, 268–272
connection establishment phases, 255–258
encryption modes, 248
extranet, 238
goals of, 239–240
growth in marketplace, 232
implementation strategies, 240–242
IPSec, 243–245
AH, 250
authentication, 246
data integrity, 246
ESP, 250
IKE, 252–253
ISAKMP, 250
transport mode, 249
tunnel mode, 248
ISAKMP, 254
island analogy, 233–235
manageability, 241
reliability, 242
remote access, 233, 237
SAs, 250–251
scalability, 236, 242
security policies, 70–71, 73–74
site-to-site, 237
encapsulating protocol, 248
router configuration, 260–267
site-to-site VPNs, 233
split tunneling, 242
tunneling, 247
vty ports, applying ACLs, 227
vulnerabilities
external, assessing, 369–370
internal, assessing, 367–369
of WANs
abuses by authorized users, 302
DoS attacks, 297–298
misconfigured APs, 300–302
rogue APs, 298–300
sniffing, 295, 297
WarChalkers, 287
WarDriving, 288–292
WarFlying, 292
WarSpamming, 292–293
WarSpying, 294
physical security, assessing, 371
procedural risk assessments, performing, 373
risk assessments, service providers, 374
vulnerability scanners, 22, 374–376

W

WapChalking, 288
WAPs (wireless access points), 281
WarChalking, 286–287
WarDialing, 286
WarDriving, 288–292
WarFlying, 292
WarSpamming, 292–293
WarSpying, 294
wave guide antennas, 290–291
websites
INRGI, 214
sample security policies, 81–82
WEP (Wireless Encryption Protocol), 302–306
WEPcrack, 317
WhatRoute, 17
Wi-Fi, 279
WinNuke, 40
wireless networking, 282
wireless packet sniffers, 315–316
WLANs, 277
ad-hoc, 283
antennas, 290–291
APs, associating, 304
bandwidth limitations, 285–286
benefits of, 280–281
distance limitations, 284
EAP, 307
EAP-Cisco Wireless, 309
EAP-MD5, 308–309
EAP-TLS, 310
EAP-TTLS, 311
enhancing security, 311–312
hacking tools
AirSNORT, 282, 288, 297, 310, 313, 316–317
NetStumbler, 313–315
packet sniffers, 315–316
IEEE 802.11b standard, 278
IEEE 802.11g standard, 279
infrastructure, 283
MAC address filtering, 307
SSIDs, 289, 303–304
vulnerabilities of
abuses by authorized users, 302
DoS attacks, 297–298
misconfigured APs, 300–302
rogue APs, 298–300
sniffing, 295, 297
WarChalkers, 287
WarDriving, 288–292
WarFlying, 292
WarSpamming, 292–293
WarSpying, 294
WAPs, 281
WEP, 302–306
Wi-Fi, 279

X-Y-Z

Xmas tree attacks, 364

zombie computers, 359