INDEX

Numerics

- **802.1x port security, 352**

A

- **access auditing, enabling, 266**
- **access points, 350**
- **account lockouts, 311**
  - detecting password-cracking attacks, 307
- **account logins, logging, 309–310**
- **ACK scan, discovering firewall configuration, 321**
- **ACK scans, 100**
- **ACK storms, 137–138**
- **acting classes, developing social engineering skills, 57**
- **active host reconnaissance, 89**
  - NSLookup/Whois lookups, 89–92
  - SamSpade, 92–94
  - Visual Route, 95
- **active session hijacking, 127**
- **AD (active directory) model, 448**
- **admin account (Novell), 451**
- **AiroPeek NX, 357**
- **AirSnort, 357**
- **Allaire, J.J., 193**
- **ALOHANET, 9**
- **anomaly detection systems, 109**
- **anomaly-based IDSs, evading, 324**
- **antennas, 350**
- **antivirus scanners, 430–431**
- **Apache HTTP Servers, 11**
  - securing, 236
  - vulnerabilities, 199
- **appendixes, 44**
- **appliance firewalls, detecting DoS attacks, 490**
- **application hardening, 496**
  - DoS attacks, preventing, 497
- **APs (access points), *detecting* rogue APs, 358**
- **ARP attacks**
  - hardening switches against, 341
  - testing switches for vulnerabilities, 335
- **ASA (Adaptive Security Algorithm), 337**
- **ASP, 188–190**
- **assets**
  - threats to, identifying, 537
  - cost of protecting, identifying, 537–538
- **assigning permissions to root user, 445**
- **Atkins, Steve, 93**
- **attacks**
  - D.A.D. attacks, 7
  - DoS, 21
  - hacktivist attacks, 13
  - mutating, 324
  - on databases, protecting against, 270–271
  - stages of
    - *erasing evidence, 14*
    - *maintaining access, 14*
    - *obtaining access, 14*
    - *reconnaissance stage, 13*
    - *scanning stage, 14*
  - zero-day, 8
- **auditing passwords, 309**
- **auditing tools**
  - AiroPeek NX, 357
  - AirSnort, 357
  - DStumbler, 355
  - GPSMAP, 356
  - Kismet, 355
  - NetStumbler, 354
  - StumbVerter, 354
  - WEPCrack, 357
- **authentication, 210**
  - on Microsoft SQL Server, sysxlogins, 261–262
- **authority-based persuasion, 53**
- **authorship of security policies, 540**
- **availability of hacking tools, 10**
- **availability threats, 7**

B

- **backdoor applications, 37, 560, 562**
  - detecting, 423
  - preventing, 432–433
- **backup policies, 543**
- **bandwidth attacks, 481**
- **banner grabbing, 223**
- **basic authentication bypass attacks, 199**
- **basic HTTP authentication, 210**
- **Beast, 412**
  - client configuration, 417–419, 423
  - gaining access with, case study, 433–436
  - server settings, 412–416

- **Beastkit, 448**
- **behavioral profiling, 55**
- **behavior-based virus detection, CSA, 456**
- **Berners-Lee, Tim, 180**
- **black-box tests, 6**
- **black-hat hackers, 5**
- **Blaster worm, 375–376**
- **blind hijacking, 130–131**
- **blind spoofing, 129**
- **BO2K (Back Orifice 2000), 378–384, 388**
  - plug-ins, 380–382
- **Borghard, Peter, 27**
- **BoSniffer program, 67**
- **Boson GetPass, 302–303**
- **Boson RIP Route Generator, 330**
- **breaching internal networks, case study, 238–244**
- **Brown Orifice, 411–412**
- **Brumleve, Dan, 411**
- **brute force attacks, 209**
  - Brutus, 211
  - detecting, 212, 215
  - HTTP Brute Forcer, 211
  - on SQL servers
    - *case study, 272, 275–277*
    - *detecting, 268*
  - protecting against, 215–216
  - testing database vulnerability to, 260
- **Brutus, 211**
- **buffer overflows**
  - case study, 476–478
  - heap buffers, 464
  - Linux privilege escalation, 466–471
  - on IIS web servers, 202–203
  - preventing, 473–475
  - simple buffer overflow example, 465
  - stack smashing exploit, 446
  - stacks, 461
  - tools for attempting, 566
  - Windows privilege escalation, 471
- **BugBear virus, 372–373**
- **bypassing firewalls, 322**
  - ICMP tunneling, 323
  - Loki ICMP tunneling, 322
- **bytecode, 466**

C

- **calculating cost of protecting assets, 537–538**
- **candy networks, 49**
- **case studies**
  - buffer overflows, 476–478
  - DoS attacks, 497–499
  - gaining access with Beast, 433–436
  - internal networks, breaching, 238–244
  - password cracking, 316–318
  - port scanning, 118, 121–122
  - remotely accessing networks, 342, 345–347
  - rootkits, 456–457
  - session hijacking, 168–169, 172–173
  - SQL server brute force attacks, 272, 275–277
  - wireless network security, 363–365
- **cDc (Cult of the Dead Cow), 378**
- **CDP (Cisco Discovery Protocol)**
  - disabling on routers, 338
  - testing for vulnerabilities, 324–326
- **CERT (Computer Emergency Response Team), 8**
- **CFAA (Computer Fraud and Abuse Act), 25**
- **CFML (ColdFusion Markup Language), 193**
- **CGI (Common Gateway Interface), 191**
- **character traits of social engineers**
  - confidence, 57–58
  - patience, 56–57
  - possessing inside knowledge, 59
  - trust, 58
- **characteristics of open source software, 11**
- **Chernobyl virus, 369**
- **CIA (confidentiality, integrity and availability), 7**
- **Cisco Guard XT, 493**
- **Cisco IDS 4200 series, detecting session hijacking, 153–156, 160–164**
- **Cisco passwords, cracking, 302–303**
- **Cisco PIX Firewalls**
  - Flood Defender, 490
  - securing, 337
- **Cisco Traffic Anomaly Detector XT appliance, 493**
- **CleanIISLog, 222**
- **clear-text passwords, 280**
- **client-based Java, 194**
- **Code of Fair Information Practices, 25**
- **ColdFusion, 193**
- **commands, SQL, 249**
- **commercial vulnerability scanners, 219**
- **company websites, downloading for offline viewing, 79–80**
- **compiler-based solutions, preventing buffer overflows, 475**

compiling NMAP, 105
Computer Ethics Institute, Ten Commandments of Computer Ethics, 22–23
Computer Misuse Act of 1990 (U.K.), 24, 31
confidence as social engineer trait, 57–58
confidentiality threats, 7
configuring
Ethereal, 145
password settings, 311–312
conformity persuasion, 50
connection strings, testing vulnerability to, 259
connnections, embryonic, 140
conscientious behavior classification (D.I.S.C.), 55
cookie guessing, 205–206
cracking encrypted passwords, 281
tools, 556
creating
security policies, 544
spoofed e-mail messages, 65–67
crystal-box tests, 6
CSA (Cisco Security Agent), 455
customer impersonation, 69–70
cybercrime, 23

D

D.A.D. (disclosure, alteration, and destruction) attacks, 7
D.I.S.C. profile, 55
data dictionary, 250
database attacks
detecting, 266
tools for performing, 556
databases
Microsoft SQL Server, 252
querying, 253
structure of, 252
MySQL, 251
Oracle, 250
protecting against attacks, 270–271
RDBMSs, 249
vulnerabilities, testing, 254–260
susceptibility to attacks, 249
Datapool, 486
DAWN Security Systems, fictitious penetration test of LCN, 505
covering tracks, 524
follow-up, 530
gaining access, 512–517, 520, 523
information gathering, 504, 507–510
maintaining access, 524
planning the attack, 503
sample report, 524–529
scanning and enumeration, 510–512
DDoS (Distributed Denial of Service) attacks, 482
DDoSPing tool, 492
default SSIDs as security risk, 351
defending against social engineering attacks, 71
defining scope of testing, 6, 36
detecting
backdoor applications, 423
brute force attacks, 212, 215
database attacks, 266
directory traversals, 226–228
DoS attacks, 489
with appliance firewalls, 490
with host-based IDSs, 490
with signature-based network IDSs, 490, 492
password-cracking attacks, 305–307
from physical access, 308
within system log files, 306
scans, 109
server attacks, 452
session hijacking, 143–144
with Cisco IDS 4200 series sensors, 153–156, 160–164
with packet sniffers, 145
Trojans applications, 423
web attacks, 225
directory traversals, 226–228
Whisker attacks, 228–231
wireless network attacks
DoS attacks, 358
MAC address spoofing, 358
on unprotected WLANs, 357
rogue APs, 358
unallocated MAC addresses, 359
devices, 324, 333
routers, testing for vulnerabilities, 324–332
switches, 111–112
testing for vulnerabilities, 333–337
DHTML (Dynamic HTML), 181
DilDog, 378
dipole antennas, 350

directory traversals, detecting, 226–228
disabling unnecessary router services, 338
disaster recovery policies, 543
discovering firewall configurations
- through firewalking, 321
- with ACK scan, 321

DMZ (demilitarized zone), securing network architecture, 237
documentation
- Appendixes, 44
- Executive Summary, 40, 44
  - *sample, 41*
- Project Scope, 42
- Results Analysis, 42–43

domain model, 448
dominant behavior classification (D.I.S.C.), 55
Donald Dick, 390–393
DoS (denial of service) attacks, 21, 481
- case study, 497–499
- DDoS, 482
- detecting, 489
  - *with appliance firewalls, 490*
  - *with host-based IDSs, 490*
  - *with signature-based network IDSs, 490–492*
- detecting on wireless networks, 358
- Fraggle attacks, 485
- LAND attacks, 485
- Ping of Death, 483–484
- preventing, 493
  - *through application hardening, 497*
  - *through network hardening, 494–496*
- protocol exceptions, 481
- Smurf attacks, 484
- SYN floods, 486
- tools for executing, 486, 566–569
  - *Datapool, 486*
  - *Hgod, 489*
  - *Jolt2, 488*

downloading websites for offline viewing, 79
DSSS (Direct Sequence Spread Spectrum), 350
DStumbler, 355
DTD (Document Type Definition), 183–184
dumb scans, 101
dumpster diving, 308
- obtaining company information, 59

E

EAPOW (Extensible Authentication Protocol over Wireless), 352
e-commerce, 198
EDGAR (Electronic Data Gathering, Analysis, and Retrieval), 78, 87
educating employees about password cracking, 315–316
EIP (extended instruction pointer), 202
elements (HTML), 180
elevation techniques, 446
- for Microsoft Windows, 449
- irix-login.c exploit, 447
- rpc.statd exploit, 446–447
- stack smashing exploit, 446

Elkern virus, 373
e-mail impersonation, 64–68
- malware attachments, 67

e-mail policies, 541
embryonic connections, 140
employees
- impersonating, 60
- tech support, impersonating, 61–62
- telecommuter phone numbers, obtaining, 61

enabling access auditing, 266
encrypted passwords, 281
end-user impersonation, 69
enforcing standards for wireless networks, 362
EPHI (electronic public health information), 29
erasing
- evidence stage of attacks, 14
- passwords, 280

ESP (extended stack pointer) registers, 462
Ethereal
- configuring, 145
- monitoring session hijacking attacks, 147, 151–153

ethical hackers, 5
European Council Convention on Cybercrime, 23
evading IDSs, 323
example penetration test, LCN, 501–517, 520, 523–530
examples
- of buffer overflows
  - *Linux privilege escalation, 466–471*
  - *Windows privilege escalation, 471*
- of scan detection, 112
  - *FIN scans, 115*

NULL scans, 115
OS guessing scans, 117–118
SYN scans, 114
TCP Connect() scans, 113
Xmas tree scans, 115
of simple buffer overflows, 465
execiis-win32.exe, 221
executing DoS attacks, 486
Datapool, 486
Hgod, 489
Jolt2, 488
Executive Summary, 40–41, 44
expanding number of security threats, reasons for
administrator trust, 13
availability of hacking tools, 10–11
business partnerships, 13
complexity of networks, 10
frequency of software updates, 10
hacktivism, 13
industry regulations, 12
marketing demands, 12
nature of open source, 11
proliferation of viruses and worms, 9
reliance on Internet, 11
unmonitored telecommuters and mobile users, 12
WLANs, 9
expiration dates of passwords, modifying, 312
exploits
hidden fields, 207–209
zero-day, 8
extended stored procedures, 258, 272
external JavaScript, 185
extra fun tab (SubSeven), 411

F

fictitious penetration test of LCN, 503, 505
covering tracks, 524
follow-up, 530
gaining access, 512–517, 520, 523
information gathering, 504, 507–510
maintaining access, 524
planning the attack, 503
sample report, 524–529
scanning and enumeration, 510, 512
file extensions for web languages, 178
file permissions, UNIX, 445
FIN scans, 100
fingerprinting, 106
firewalking, discovering firewall configuration, 321
firewalls
bypassing, 322
ICMP tunneling, 323
Loki ICMP tunneling, 322
discovering configuration through firewalking, 321
securing, 337
FISMA (Federal Information Security Management Act), 30
Flood Defender, 490
footprinting, 108, 501
form-based authentication, 216
form-based HTTP authentication, 210
four-factor security, 279
fport, 428
Fraggle attacks, 485
fun manager tab (SubSeven), 411
FuX0red, 398
fuzzy matching, 107

G

general-purpose registers, 462
GetPass, 302–303
GLB (Graham-Leach-Bliley) act of 1999, 29
GNU (GNUs not UNIX), 11
Google.com as hacking tool, 224
Gosling, James, 193
GPSMAP, 356
grading passwords with L0phtcrack, 295
gratuitous ARPs, 138
gray-box testing, 6, 31
guest accounts (Microsoft SQL Server), 264

H

hacking, 5
laws. *See* legislation
non-U.S. laws pertaining to, 31
Novell NetWare, 451
script-kiddies, 11
tools, availability of, 10
hacktivism, 13
hardening switches
against ARP attacks, 341
against MAC table flooding attacks, 341

against STP attacks, 341
against VLAN hopping, 341
against VTP attacks, 342
hashing algorithms, 281
Hassell, Riley, 202
heap buffers, 464
Hedley, David, 447
Herzog, Peter, 37
Hgod, 489
hidden field exploit, 207–209
Hide Server, 266
high-gain omni-directional antennas, 350
highly directional antennas, 350
HIPAA (Health Insurance Portability and Accountability Act), 12
history of passwords, modifying, 313
history of wireless networking, 349–350
HK exploit, 449
hoaxes, BugBear virus hoax, 373
honeypots, 17
host reconnaissance, tools, 547, 550–553
host-based IDSs, 110
detecting DoS attacks, 490
HTML, 179
HTTP
basic authentication, 210
form-based authentication, 210
tunneling, 323
web server vulnerabilities
Apache, 199
IIS, 199–203
HTTP Brute Forcer, 211
HTTP service
disabling on routers, 338
testing for vulnerabilities, 326
human psychology, behavioral profiling, 55
human-based social engineering, 50
customers, impersonating, 69–70
defending against, 71
e-mail impersonation, 64–68
employees, impersonating, 60
tech support, 61–62
end-users, impersonating, 69
persuasion, types of
authority-based, 53
conformity-based, 50
information-based, 54–55
logic-based, 51–52
need-based, 52
reciprocation-based, 53–54
similarity-based, 54
RSE, 70
third parties, impersonating, 62–64
traits of social engineers
confidence, 57–58
patience, 56–57
possessing inside knowledge, 59
trust, 58
wetware, 50
Hunt, 134–135
hijacking Telnet sessions, 135
HyperText PreProcessor, 192
Hypnopædia, 299

I

“I Love You” worm, 370
ICMP
Ping of Death attacks, 483–484
Smurf attacks, 484
tunneling, 322–323
identifying threats to assets, 537
IDSs (intrusion detection systems), 109, 431
evading, 323
IEV (IDS Event Viewer), viewing session hijacking, 164–165
IIS Lock Down, 235
IIS web servers
securing, 234–236
vulnerabilities, 199–200
buffer overflows, 202–203
privilege escalation, 201
showcode.asp, 200–201
IIS Xploit, 221
impersonating
company employees, 60
tech support personnel, 61–62
customers, 69–70
end-users, 69
third parties, 62–64
implementing
employee education on password cracking, 315–316
physical protection, 313–314
improvisation, developing social engineering skills, 57

industry regulations as cause for expanding number of security threats, 12
influential behavior classification (D.I.S.C.), 55
INFORMATION_SCHEMA views, 251
information-based persuasion, 54–55
inside knowledge, importance of possessing, 59
integrity threats, 7
IntelliTamper, 222
internal networks, breaching, case study, 238–244
Internet policies, 541
interpreted languages, Perl, 187
IPSec, deploying on wireless networks, 353
IPv6 URI parsing heap overflows, 199
irix-login.c exploit, 447
ISS (Internet Security Scanner), 444
Ivgi, Rafel, 208
I-worm, 373

J

Java, 193
client-based, 194
server-based, 194–195
JavaScript, 185–186
John the Ripper, 285–287
johnny.ihackstuff.com, 224
Jolt2, 488
JScript, 186
Juggernaut, 131–133

K-L

key logging, 308
Kismet, 355
Klez worm, 373
Kouznetsov, Pavel, 194
Krauz, Pavel, 134
Kwyjibo, 371

L0phtcrack, 289–290, 294, 298
LAND attack, 482
LANMAN hashing, 283
LCN (Little Company Network), example penetration test, 501–505
covering tracks, 524
follow-up, 530
gaining access, 512–523
information gathering, 504, 507–510
maintaining access, 524
planning the attack, 503
sample report, 524–529
scanning and enumeration, 510–512
legislation
CFAA, 25
Code of Fair Information Practices, 25
Computer Misuse Act (U.K.), 24
FISMA, 30
Graham-Leach-Bliley act of 1999, 29
non-U.S., 31
Sarbanes-Oxley Act, 30
USA PATRIOT Act, 30
length of passwords, modifying, 312
Lerdorf, Rasmus, 192
library tools, preventing buffer overflows, 475
Linux
DoS attacks, executing
Spendor Datapool, 486
elevation techniques
irix-login.c exploit, 447
rpc.statd exploit, 446–447
stack smashing exploit, 446
MACOF, 129
privilege escalation, example of, 466–471
rootkits, 447
Litchfield, David, 260
LiveScript, 185
Local System account (SQL Server), 263
locking out user accounts, 311
logging
account logins, 309–310
actions during penetration testing, 31–32
logic attacks, 482
logic persuasion, 51–52
Loki ICMP tunneling, 322
Long, Johnny, 224

M

MAC address spoofing, detecting on wireless networks, 358
MAC filtering on wireless networks, 352
MAC table flooding attacks
hardening switches against, 341
testing switches for vulnerabilities, 335

MACOF, 129
maintaining access stage of attacks, 14
malware, 67, 368
markup languages
  CFML, 193
  DHTML, 181
  HTML, 181
  XHTML, 184
  XML, 183–184
master database, 252
MBSA (Microsoft Baseline Security Analyzer), 270
MD5 checksums, 424
Melissa virus, 371
memory, buffers
  heap buffers, 464
  stacks, 461
memory consumption DoS attacks, 199
Microsoft
  AD model, 448
  domain model, 448
  password hashing, 282
    LANMAN hashing, 283
    Windows hashing, 282
  SQL Server, 252
    authentication, sysxlogins, 261–262
    guest accounts, 264
    network libraries, 264–265
    ports, 265
    Public role, 263
    querying, 253
    sample databases, 264
    service accounts, 263
    structure of, 252
  Windows
    elevation techniques, 449
    rootkits, 450
mirror technique for gaining employee trust, 58
misuse detection systems, 109
MITM (man-in-the-middle) attacks, 128
  preventing on wireless networks, 361
  session hijacking
    blind spoofing, 129
    case study, 168–169, 172–173
    nonblind spoofing, 128
    TCP sequence prediction, 130–131
Mitnick, Kevin, 71, 139–140
  session hijacking of Tsutomu Shimomura's computer, 139–140, 143
modifying password settings, 311–312
monitoring
  ports, 424–426, 429
  session hijacking with packet sniffer, 145
morphing attacks, 324
mutating attacks, 324
MyDoom worm, 373
MySQL, 251
  databases structure, 251
  INFORMATION_SCHEMA views, 251
  structure of, 251

N

NASL (Nessus Attack Scripting Language), 440
NAT (Network Address Translation), configuring, 347
NDS (Novell Directory Services), 450
need for penetration testing, 8–9
need-based persuasion, 52
Nessus, 440
NetCat, 217–218
  shoveling remote shells, 395–397
  surreptitious installation of, 74
NetRecon, 445
Netstat, 426–427
NetStumbler, 354
network architecture, securing, 237
network attacks, tools for performing, 557
network hardening, preventing DoS attacks, 494–496
network libraries, 264–265
network-based IDSs, 110
networks, remote access, case study, 342, 345–347
newsgroups, 87
NICNAME, 91
NMAP, 22, 102
  compiling, 105
  switches, 103–105
nonblind spoofing, 128
non-executable stack, preventing buffer overflows, 475
non-U.S. laws pertaining to hacking, 31
NOPs (No Operation) commands, 464
NovelFFS (Novel Fake File Server), 451
Novell NetWare, 450
  hacking, 451
  NDS, 450
  rights, 450–451

NSLookup, 89–92
NT/2000 Rootkit, 395
NULL scans, 99–100
Nutcracker, 298–299

O

O'Keefe, Brett, 27
Oak, 193
obtaining access stage of attacks, 14
obtaining telecommuter phone numbers, 61
OECD (Organization for Economic Co-Operation and Development), 24
offline viewing of websites, 79
omni-directional antennas, 350
one factor authentication, 279
opcode, 466
open source software characteristics, 11
OpenBSD systems, inadvertant DoS attacks on, 22
open-source vulnerability scanners, 219
operating systems
  fingerprinting, 106
  securing, 232–234
  stack fingerprinting, 106
  UNIX, salts, 282
Oracle databases, 250
Orphan pages, 79
OSSTMM (Open-Source Security Testing Methodology Manual), 35–39, 503
out-of-sequence packets, 130

P

packet sniffers, 281
  detecting session hijacking, 145
  Ethereal, monitoring session hijacking attacks, 147, 151–153
packets, out-of-sequence, 130
Pandora, 451
Passive reconnaissance, 78
passive scanners, Kismet, 356
passive session hijacking, 127
password cracking
  attacks, detecting, 305–308
  brute force attacks
    Brutus, 211
    detecting, 212, 215
    HTTP Brute Forcer, 211
    protecting against, 215–216
  case study, 316–318
  employee education, implementing, 315–316
  protecting against, 309–314
  salts, 282
  utilities, 556
    Boson GetPass, 302–303
    Hypnopædia, 299
    John the Ripper, 285–287
    L0phtcrack, 289–290, 294, 298
    Nutcracker, 298–299
    pwdump, 277
    pwdump3, 287–288
    RainbowCrack, 303–304
    Snadboy Revelation, 300
password hashing, 280
  on Microsoft systems, 282–283
  on UNIX systems, 284
password policies, 542
passwords. See also *password cracking*
  brute force attacks, 209
    detecting on SQL servers, 268
  encrypted, 281
  erasing, 280
  hidden field exploit, 207, 209
  securing on routers, 338–340
  testing for vulnerabilities, 328
patience as social engineer trait, 56–57
penetration tests
  preparing for, 16–17
  vendors, selecting, 14–16
Perl (Practical Extraction and Report Language), 187–188
permissions, UNIX, 445
  assigning to root user, 445
  elevation techniques, 446–447
persuasion
  authority-based persuasion, 53
  conformity persuasion, 50
  information-based persuasion, 54–55
  logic persuasion, 51–52
  need-based persuasion, 52
  reciprocation-based persuasion, 53–54
  similarity-based persuasion, 54
phishing, 67, 203–205
phone numbers of telecommuters, obtaining, 61

PHP (Hypertext Preprocessor), 251
PHP (Personal Home Page), 192
***Phrack Magazine*, 131**
physical access policies, 543
physical protection, implementing, 313–314
PictureClock.class, 194
Ping of Death attacks, 483–484
PipeUpAdmin, 449
plain-text passwords, 280
plug-ins, BO2K, 380–382
port scanning, 96–97
  ACK scans, 100
  case study, 118–122
  dumb scans, 101
  FIN scans, 100
  inadvertant DoS attacks, 22
  NMAP, 102
  NULL scans, 99–100
  SYN scans, 99
  TCP connect() port scans, 98
  Xmas-Tree scans, 101
ports
  monitoring, 424–426, 429
  on Microsoft SQL Server, 265
preparing
  for penetration testing, 16–17
  security policies, 544
preventing
  attacks on wireless networks, 359, 362
    MITM attacks, 361
  backdoor applications, 432–433
  buffer overflows, 473–475
  DoS attacks, 493
    through application hardening, 497
    through network hardening, 494–496
  server attacks, 452–455
  Trojan horse applications, 432–433
privilege escalation on IIS web servers, 201
privileged exec mode, 302
Project Scope, 42
protecting
  against brute force attacks, 215–216
  against database attacks, 270–271
  against password-cracking attacks, 309–312
  against session hijacking, 167
  against social engineering attacks, 71
protocol exceptions, 481
PS/SQL (Procedural Language/Structured Query Language), 250
Public Role (Microsoft SQL Server), 263
pwdump, 277
pwdump3, 287–288

Q-R

querying
  Microsoft SQL Servers, 253
  Oracle databases, 250

rainbow tables, 303
RainbowCrack, 303–304
RAT tools, Tini, 389
RDBMSs (Relational Database Management Systems), 249
  Microsoft SQL Server, 252
    authentication, 261–262
    guest accounts, 264
    network libraries, 264–265
    ports, 265
    Public Role, 263
    querying, 253
    sample databases, 264
    Service Accounts, 263
    structure of, 252
  MySQL, 251
  Oracle, 250
  vulnerabilities, testing, 254
    brute force attacks, 260
    connection strings, 259
    SQL injection, 256
    system stored procedures, 257
reassessment principle, 24
reciprocation-based persuasion, 53–54
reconnaissance attacks, 13
  active host reconnaissance
    NSLookup/Whois lookups, 89–92
    SamSpade, 92–94
    Visual Route, 95
  footprinting, 108
registers, 462
  ESP registers, 462
  general-purpose, 462
  special-purpose application, 464
regression testing, 7
regulatory laws, 28
remote access to networks, case study, 342, 345–347

remote administration Trojans, Beast, 412
client configuration, 417–419, 423
server settings, 412–416
remote port monitoring, 429
remote shell utilities
NetCat, 217–218
shoveling, 395–397
remote-access policies, 542
remote-access Trojans, Donald Dick, 390, 393
remote-administration trojans, detecting, 423
required topics in security policies, 538
Results Analysis, 42–43
Revelation, 300
rights (Novell NetWare), 450–451
RIP Route Generator, 330
risk analysis, 12
risk assessment, performing, 536
company acceptance, gaining, 538
cost of protecting assets, calculating, 537–538
threats to assets, identifying, 537
rogue APs, detecting on wireless networks, 358
root access, obtaining on Linux-based machines
irix-login.c exploit, 447
rpc.statd exploit, 446–447
stack-smashing exploit, 446
root user permissions, assigning, 445
rootkits, 395, 447
case study, 456–457
for Microsoft Windows, 450
routers, 324
CDP
disabling, 338
testing for vulnerabilities, 324–326
HTTP service
disabling, 338
testing for vulnerabilities, 326
passwords
securing, 338–340
testing for vulnerabilities, 328
routing protocols, testing for vulnerabilities, 329–332
securing, 338
routing protocols, testing for vulnerabilities, 329–332
rpc.statd exploit, 446–447
RSE (reverse social engineering), 70
Russinvoch, Mark, 429

S

SAINT (Security Administrators Integrated Network Tool), 441
salts, 282
SAM file, 276
sample databases on Microsoft SQL Server, 264
sample Executive Summary, 41
sample penetration test report, 524–529
SamSpade, 92–94
Sanfilippo, Salvatore, 101
Sapphire worm, 376–377
SARA (Security Auditor's Research Assistant), 442–443
Sarbanes-Oxley Act, 30
Sasser worm, 9, 377
scan detecting, 109
examples, 112
FIN scans, 115
NULL scans, 115
OS guessing scans, 117–118
SYN scans, 114
TCP Connect() scans, 113
Xmas tree scans, 115
scanners, 430–431
scanning stage of attacks, 14
scope of testing, defining, 6, 36
scripting languages
ASP, 188–190
JavaScript, 185–186
JScript, 186
Perl, 187–188
PHP, 192
VBScript, 186–187
script-kiddies, 11
securing
firewalls, 337
network architecture, 237
operating system, 232–234
routers, 338–340
web server applications
Apache, 236
IIS, 234–236
website design, 236
security policies, 7
authorship, 540
backup policies, 543
cost of protecting assets, calculating, 537–538

creating, 544
disaster recovery policies, 543
e-mail policies, 541
gaining company acceptance, 538
Internet policies, 541
password policies, 542
physical access policies, 543
remote access policies, 542
required topics, 538
threats to assets, identifying, 537
trust model, 540
types of, 541
selecting penetration testing vendor, 14–16
semi-directional antennas, 350
server attacks
detecting, 452
preventing, 452–455
server penetration, tools for performing, 562–565
server-based Java, 194–195
servers, honeypots, 17
service accounts, on Microsoft SQL Server, 263
session hijacking, 36, 127
ACK storms, 137–138
blind spoofing, 129
case study, 168–169, 172–173
detecting, 143–145
with packet sniffers, 145
detecting with Cisco IDS, 153–156, 162–164
Kevin Mitnick's attack on Tsutomu Shimomura's computer, 139–140, 143
monitoring with Ethereal, 147, 151–153
nonblind spoofing, 128
protecting against, 167
TCP sequence prediction, 130–131
utilities, 553
Hunt, 134–135
Juggernaut, 131–133
T-Sight, 136
watching, 164–165
TTY-Watcher, 136
session replays versus session hijacking, 128
Shimomura, Tsutomu, 139
shoveling remote shells, 395–397
showcode.asp, 200–201
signature-based IDSs, evading, 323
detecting DoS attacks, 490–492
signatures, detecting session hijacking, 155–156, 160, 164
similarity-based persuasion, 54
Simon, William, 71
simplex connection hijacking, 132
single-server e-commerce architecture, 198
Site Security Handbook, 535
Slammer worm, 376–377
SMBdie, 498
Smith, David, 27
Smurf amplifiers, 485
Smurf attacks, 484–485
Snadboy Revelation, 300
social engineering, 6, 36, 308
behavioral profiling, 55
case study, 72–75
defending against, 71
e-mail impersonation, 64–68
employees, impersonating,60
tech support, 61–62
end-users, impersonating, 69
human-based, 50
customers, impersonating, 69–70
persuasion, types of
authority-based persuasion, 53
conformity persuasion, 50
information-based persuasion, 54–55
logic persuasion, 51–52
need-based persuasion, 52
reciprocation-based persuasion, 53–54
similarity-based persuasion, 54
RSE, 70
technology-based, 49
third parties, impersonating, 62–64
traits necessary for
confidence, 57–58
patience, 56–57
possessing inside knowledge, 59
trust, 58
user group meetings, 88
web page spoofing, 203–205
wetware, 50
witness consultants as coaches, 58
sockets, 196
software, open source
characteristics of, 11
SOX (Sarbanes-Oxley) Act, 30
spacefiller viruses, 369
SPAN (Switched Port Analyzer), 129
special-purpose application registers, 464
Spendor Datapool, 486
spoofed e-mail messages, 64

SQL (Structured Query Language), 247
- brute force server attacks, case study, 272, 275–277
- commands, 249
- master database, 252
- servers
  - *brute force attacks, detecting, 268*
  - *system stored procedures, 269*

SQL injection, 236, 270
- testing vulnerability to, 256

SQL Slammer worm, 265, 376–377
SQLPing2, 256
SSIDs (service set identifiers), 351
SSL infinite loops, 199
stack fingerprinting, 106
stack smashing exploit, 446
stacks, 461
- non-executable, preventing buffer overflows, 475

stages of attacks
- erasing evidence, 14
- maintaining access, 14
- obtaining access, 14
- reconnaissance, 13
- scanning, 14

standards for wireless networks, enforcing, 362
stored procedures, 257, 269
- extended, 272

STP (Spanning Tree Protocol)
- hardening switches against attacks, 341
- testing switches for vulnerabilities, 334

structure
- of Microsoft SQL Servers, 252
- of MySQL databases, 251
- of Oracle databases, 250

StumbVerter, 354
SubSeven, 398, 401–403, 406, 409–410
superusers, assigning permissions to, 445
susceptibility of databases to attack, 249
switches, 111–112
- ARP attacks, hardening against, 341
- MAC table flooding attacks, hardening against, 341
- NMAP, 103–105
- STP attacks, hardening against, 341
- testing for vulnerabilities, 333
  - *via ARP attacks, 335*
  - *via MAC table flooding, 335*
  - *via STP, 334*
  - *via VLAN hopping, 333–334*
  - *via VTP attacks, 336–337*
- VLAN hopping, 341
- VTP attacks, hardening against, 342

symptoms of session hijacking, 143–145
SYN floods, 481, 486
SYN scans, 99
system log files, detecting password-cracking attacks, 306
system stored procedures, 257–258
system tablespace, 250
sysxlogins, 261–262

T

tablespaces, 250
TCP
- embryonic connections, 140
- sequence prediction, 130–131
- session hijacking, 36

TCP Connect() scans, 98
TCPView, 429
tech support personnel, impersonating, 61–62
technology-based social engineering, 49
telecommuters, remote access policy, 542
Teleport Pro, 81
Telnet sessions, hijacking example, 135
temporal response analysis, 107
Ten Commandments of Computer Ethics, 22–23
testing
- RDBMS for vulnerabilities, 254
  - *brute force attacks, 260*
  - *connection strings, 259*
  - *SQL injection, 256*
  - *system stored procedures, 257*
- routers for vulnerabilities, 324
  - *CDP, 324–326*
  - *HTTP service, 326*
  - *passwords, 328*
  - *routing protocols, 329–332*
- switches for vulnerabilities, 333
  - *via ARP attacks, 335*
  - *via MAC table flooding, 335*
  - *via STP, 334*
  - *via VLAN hopping, 333–334*
  - *via VTP attacks, 336–337*

testing reports
- Appendixes, 44

Executive Summary section, 41, 44
Project Scope section, 42
Results Analysis section, 42–43
tests
black-box tests, 6
crystal-box, 6
gray-box, 6
white-box tests, 6
third-party impersonation, 62–64
threats, 7
availability threats, 7
confidentiality threats, 7
integrity threats, 7
tiered e-commerce architecture, 198
tiger teams, 5
time bomb viruses, 369
Tini, 389
Titanic syndrome, 8
TMRC (Tech Model Railroad Club), 5
TOE (target-of-evaluation), 6
tools
backdoor applications, 560–562
for attempting buffer overflows, 566
for attempting DoS attacks, 566–569
Datapool, 486
Hgod, 489
Jolt2, 488
for performing database attacks, 556
for performing network attacks, 557
for performing server penetration, 562–565
for performing web server attacks, 554–555
for wireless network penetration, 559
hacking tools, availability of, 10
host reconnaissance, 547, 550–553
password cracking, 556
session hijacking, 553
vulnerability scanners
ISS, 444
Nessus, 440
NetRecon, 445
SAINT, 441
SARA, 442–443
traits of social engineers
confidence, 57–58
patience, 56–57
possessing inside knowledge, 59
trust, 58
Trojan applications, 37, 67, 367, 560–562
Beast, 412
client configuration, 417–419, 423
gaining access with, case study, 433–436
server settings, 412–416
BO2K, 378–388
plug-ins, 380–382
Brown Orifice, 411–412
detecting, 423
Donald Dick, 390, 393
scanner software, 430–431
SubSeven, 398–403, 406, 409–410
trust as social engineer trait, 58
trust model, 540
T-Sight, 136
T-SQL (Transact-SQL), 253
TTY Watcher, 136
tunneling
ICMP tunneling, 323
Loki ICMP tunneling, 322
two-factor security, 279
Type-1 wireless, 353

U

unallocated MAC addresses, detecting on wireless networks, 359
unethical practices, free penetration testing, 32
UNIX
elevation techniques, 446
irix-login.c, 447
rpc.statd exploit, 446–447
stack smashing exploit, 446
password-cracking utilities, Nutcracker, 298–299
password hashing, 284
permissions, 445
assigning to root user, 445
rootkits, 447
salts, 282
UrlScan, 235–236
USA PATRIOT act, 30
USENET newsgroups, 87
user accounts, locking out, 311
user exec mode, 302
user group meetings, 88
utilities

backdoor applications, 560, 562
CleanIISLog, 222
execiis-win32.exe, 221
for attempting buffer overflows, 566
for attempting DoS attacks, 566–569
for attempting network attacks, 557
for server penetration, 562–565
for wireless network penetration, 559
fport, 428
host reconnaissance, 547, 550–553
IIS Xploit, 221
IntelliTamper, 222
NetCat, 217–218
Netstat, 426–427
packet sniffers, 281
password-cracking
Boson GetPass, 302–303
Hypnopædia, 299
John the Ripper, 285–287
L0phtcrack, 289–290, 294, 298
Nutcracker, 298–299
Pwdump3, 287–288
RainbowCrack, 303–304
Snadboy Revelation, 300
session hijacking, 553
TCPView, 429
vulnerability scanners, 218
commercial, 219
open-source, 219
Xprobe2, 107

V

VBScript, 186–187
vendors of penetration testing, selecting, 14–16

views (MySQL), INFORMATION_SCHEMA, 251
viruses, 9, 368. *See also* worms
BugBear, 372–373
Chernobyl, 369
construction kits, 369
Melissa, 371
Sasser virus, 9
scanner software, 430–431
Visual Route, 95
VLAN hopping
hardening switches against, 341
testing switches for vulnerabilities, 333–334
VTP attacks
hardening switches against, 342
testing switches for vulnerabilities, 336–337
vulnerabilities, 7
of Apache HTTP Web Servers, 199
of databases to attack, 249
of IIS web servers, 199–200
buffer overflows, 202–203
privilege escalation, 201
showcode.asp, 200–201
of RDBMSs, testing, 254–260
vulnerability scanners, 218, 439
commercial, 219
ISS, 444
Nessus, 440
NetRecon, 445
open-source, 219
SAINT, 441
SARA, 442–443
tests performed, 440
Whisker attacks, detecting, 228–231

W

W32.CIH.Spacefiller, 369
W32.Slammer worm, 376–377
W32/BugBear virus, 372–373
W32/Klez worm, 373, 375
war dialing, 86
war driving, 353
war flying, 353
war pedaling, 353
war sailing, 353
war walking, 353
web attacks
detecting, 225
directory traversals, detecting, 226–228
web languages
ASP, 188–190
CGI, 191
ColdFusion, 193
DHTML, 181
file extensions, 178
HTML, 179

- Java, 193
  - *client-based, 194*
  - *server-based, 194–195*
- JavaScript, 185–186
- JScript, 186
- Perl, 187–188
- PHP, 192
- VBScript, 186–187
- XHTML, 184
- XML, 183–184

web pages
- hidden fields, exploiting, 207–209
- spoofing, 203–205
- tools for performing, 554–555

web servers
- Apache, 11
  - ***applications, securing**, 236*
  - *vulnerabilities, 199*
- attacks on, tools for performing, 197, 554–555
- IIS
  - ***applications, securing**, 234–236*
  - *vulnerabilities, 199–203*

web-based authentication attacks, 197

websites, 196–197
- configuring NAT, 347
- downloading for offline viewing, 79
- Google.com as hacking tool, 224
- OECD, 24
- orphan pages, 79
- securing, 236
- sockets, 196

WEP (Wired Equivalency Protocol), 9, 352

WEPCrack, 357

wetware, 50

Wget, 79

Whisker attacks, detecting, 228–231

white-box tests, 6

white-hat hackers, 5

Whois lookups, 89–92

Windows
- elevation techniques, 449
  - *HK exploit, 449*
  - *PipeUpAdmin, 449*
- hashing, 282
- password-cracking utilities, Hypnopædia, 299
- privilege escalation, example of, 471
- rootkits, 450

wireless networks
- 802.1x port security, 352
- access points, 350
- attacks
  - *detecting, 357*
  - *preventing, 359–362*
- DoS attacks, detecting, 358
- DSSS, 350
- history of, 349–350
- IPSec, 353
- MAC address spoofing, detecting, 358
- MAC filtering, 352
- penetration testing tools, 559
  - *AiroPeek NX, 357*
  - *AirSnort, 357*
  - *DStumbler, 355*
  - *GPSMAP, 356*
  - *Kismet, 355*
  - *NetStumbler, 354*
  - *StumbVerter, 354*
  - *WEPCrack, 357*
- rogue APs, detecting, 358
- security, 351
  - *case study, 363–365*
- SSIDs, 351
- standards, enforcing, 362
- Type-1, 353
- unallocated MAC addresses, detecting, 359
- war driving, 353
- WEP, 352

witness consultants as social engineering coaches, 58

WLANs (wireless LANs), 9

worms, 9, 368
- "I Love You," 370
- Blaster, 375–376
- MyDoom, 373
- Sasser, 377
- W32/Klex, 373–375

X-Y-Z

XHTML, 184

Xmas-Tree scans, 101

XML, 183–184

Xprobe2, 107

zero-day exploits, 8

zones, 90