

INDEX

References followed by an “f” are to figures; references followed by a “t” are to tables.

Numbers/Symbols

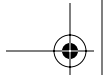
802.11 family of protocols, 72, 89. *See also*
 NetStumbler; War driving
 and ARP, 73
 and MAC, 73
 modes (independent/peer-to-peer and
 infrastructure/access-point), 74
 popular/important members, 73-74
 supported frame types, 74-75
 vulnerabilities, 72-73
 /etc/group file, 109
 /etc/passwd file, 107-109

A

Access (maintaining), 547, 623. *See also*
 Backdoors; Trojan horse backdoor
 genre; Trojan horses

Access/application and operating system
 levels, 339, 435-437
 exploits available on the Web, 339-340
 sophisticated attacker techniques,
 340-342
 trolling (script kiddies), 339-340, 341f
 Access/network level
 attacks, 439, 510
 Access point hijacking attacks, 488-490
 Account harvesting. *See* Web application
 attacks
 Achilles, 416t, 417-418, 417f
 ACK storm, 485-486, 485f
 Active Directory, 130-131, 166, 180
 change to domain controllers, 132
 protection, 167
 tree structure, 165, 165f
 Active Ports, 295

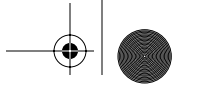




INDEX

- Active Whois Browser, 232
- ActiveX
 - controlling access to, 586, 587f
 - and use for shipping remote-control backdoors, 565-566
- Ad-Aware, and imposters, 580
- Address Resolution Protocol, 68-69, 69f
- Adore-ng rootkit, 613-615
- Advanced Intrusion Detection Engine (AIDE), 606
- AFX File Lace, 564
- AFX Windows Rootkit, 602-604, 603f
- AirDefense, 251
- AirJack toolkit, 247, 490
- AirMagnet, 251
- AirSnort tool, 243, 490
- AIX (IBM), 92
- Albitz, Paul, 221
- Aleph One, 342
- Alice (scenario cast member), 14
- American Registry for Internet Numbers (ARIN), 218
- Anatomy of attacks, 671-672
 - scenarios depicting pragmatism of attackers, 672, 708-709. *See also* Crouching Wi-Fi, Hidden Dragon scenario; Death of a Telecommuter scenario; The Manchurian Contractor scenario
- Antivirus and antispyware tools, 581-583
- Apache Web servers, 162
- Aphex, 557, 602
- Aplus.net, 220
- Application-level security for TCP/IP-based networks, 75-76, 76t
- Application-level Trojan horse backdoor tools, 554t, 555. *See also* Bots; Phishing attacks; Remote-control backdoors; Spyware; URL/obfuscation
- defenses against
 - antivirus and antispyware tools, 581-583
 - identify unusual TCP and UDP ports, 583
 - identify your software, 583-586
 - user education, 586-587
 - identifying victims, 565
- AppShield (Watchfire), 423
- Arkin, Ofir, 292
- arpspoof tool, 452-454, 453f, 486, 520-521
- The Art of Deception*, 186
- Asia Pacific Network Information Center (APNIC), 219
- Asterisk (Linux), 188
- Atkins, Steve, 230
- Attack tools. *See also* Computer attacks; Underlying technologies and platforms
 - genres of, 5
 - security information, 715
 - security information/conferences, 720
 - Black Hat Briefings, 720-721
 - DEFCON, 720
 - SANS Institute, 721
 - security information/ mailing lists, 718
 - Bugtraq, 718
 - Crypto-Gram, 720
 - U.S. Computer Emergency Readiness Team (CERT), 718-719

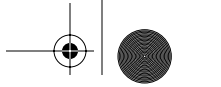




- security information/Web sites, 715
 - Counter Hack, 715-716
 - Honeynet Web site, 718
 - Information Security Magazine*, 717
 - Internet Storm Center (ISC), 368, 716
 - Metasploit Web site, 717
 - Packet Storm Security, 339, 717
 - SearchSecurity Web site (TechTarget), 717
 - Security Focus, 716
 - study of, 15, 23
 - controlled environment/lab for experimentation, 16-17, 17f
 - hidden dangers, 15, 18
 - limitations and permissions, 17-18
 - Attacker Tool Kit (ATK), 310
 - Attackers, 13, 23. *See also* “Bad guy”;
 - Computer attacks; Scenario cast members
 - categorization of
 - business competitors, 8
 - governments, 8
 - hactivists, 9
 - “hired guns,” 9
 - insider threats, 9-10
 - organized crime, 7-8
 - terrorists, 8
 - youthful offenders, 7
 - communication channels of, 4
 - contractors/temps/consultants, 10
 - “Owned” systems and backdoors, 549
 - skill level
 - elite attackers, 12
 - medium-level attackers, 11
 - script kiddies, 11
 - targets, 628
 - terminology, 12-13, 23
 - Attacks. *See* Anatomy of attacks; Phases of attacks
 - AttacPortal.net, 233
- B**
- Back Orifice, 2000, 559
 - Backdoors, 548-550, 623. *See also* Netcat/
 - as backdoor on UNIX systems;
 - Trojan horse backdoor genre
 - and “Owned” systems, 549
 - Backward compatibility, 129-130
 - “Bad guy,” 13, 23
 - Bagle, 578
 - BGP (Border Gateway Protocol), 53
 - Binders, 563-564
 - “Black hat,” 13, 14f
 - Black Hat Briefings, 720-721
 - Blacklight, 621
 - BO2K, 565
 - Bob (scenario cast member), 14
 - Bofra worm, 433
 - Bonk, 519t, 520
 - Border Gateway Protocol (BGP) attack, 522
 - Bots, 22, 568-569, 570f
 - bot-nets, 569, 628
 - IRC control, 571-573
 - distribution (worm-bot feedback loop), 575-578
 - functionality, 571, 572t
 - future communication directions, 573-574
 - history of, 569-570
 - variations, 570-571

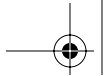
INDEX

- Brin, Sergey, 197
- Brutus, 379-381, 380f
- Buffer overflow exploits, 342-343, 435. *See also* Heap; Stack
- defenses, 371, 436
 - at software developer level, 375-377
 - at system administrator/security personnel level, 371-375
 - exploitation engines, 361-362. *See also* Metasploit
 - heap-based overflow attacks,
 - 21, 358-360
 - stack-based buffer overflow attacks,
 - 21, 347-353, 348f
 - exploit (“sploit”) structure, 358f
 - exploitation of, 353
 - smashed stack, 350-352, 351f
 - typical attack code, 352-353
 - vulnerability-identification techniques, 353-358
 - vulnerable code, 348-349, 353-354
- Bugtraq
- Archives (Security Focus), 340
 - mailing list, 718
- Bulba, 376
- C**
- Cain and Abel tools, 22, 385
- capabilities, 386-387
 - integrated sniffer (Cain), 392-394, 394f
 - password cracker functions (Cain),
 - 387-388, 391-392, 392t
 - configuration options, 390-391, 390f
 - non-Windows systems, 394-396
 - Windows, 388-390
- Caller ID spoofing, 21, 187-189
- defenses against, 190
 - and in-house voice mailboxes, 186-187
 - and Voice over IP (VoIP) services, 188
- Camophone, 188, 189f
- Canary functionality, 376-377
- CANVAS tool (Immunity), 362
- Car hacking, 3
- Cell phones, widespread use of, 2
- CERIAS wordlist collection, 384
- Certificates, 81
- Cheops-ng, 266-267, 266f, 336
- Chief Information Security Officer (CISO)/Chief Information Officer (CIO)
- and exploit frameworks, 368-369
 - and permissions to study attacks, 18
- chkconfig command, 298
- Chkrootkit tool, 619-620
- chmod command, 112
- Cisco
- defense against renegade access
 - points, 251
 - Secure IDS, 667
 - Security Agent (CSA), 334
- Claerhout, Brecht, 444
- Classless Inter-Domain Routing (CIDR)
- notation
 - and netmasks, 48. *See also* Smurf attacks
- Comer, Douglas, 25
- Competitors (in business), and computer attacks, 8
- Computer attacks. *See also* Phases of attacks
- frequency of, 1



- future directions, 20, 711-712, 721-722
 - probable merging of two scenarios, 714-715
 - security will become a priority
 - among vendors and users, 713-714
 - vulnerabilities continue to be discovered/exploited, 712-713
- Computer technology
 - dependency on, 2
 - expansion of uses, 3
 - hackability of, 2
- Consultants
 - as security researchers/defenders, 12
 - and presentation of threats, 656
 - and use of virtual machines, 574
 - as source of attack, 10, 253-254
- Controlled environment/experimentation lab, 16-17, 17f
- Cookies, 412
 - and e-commerce, 420-421
 - persistent and nonpersistent, 414-415
 - SYN cookies, 527-529, 527f
- Counter Hack Web site, 715-716
- Counterpane Internet Security, Inc., 720
- Covering tracks/hiding, 22, 627-628, 668.
 - See also* Covert channels;
 - Steganography
 - altering event logs, 628-629
 - altering event logs (defenses), 637, 668-669
 - activate logging, 637
 - encrypted log file, 640
 - log file append only (Linux and some UNIX systems), 640
 - log file on write-once media, 640-641
 - separate logging server, 638-639
 - setting permissions, 638
- event log in Windows, 629-630, 630f
 - attacks, 631-632
- hidden files/directories attack
 - technique, 641
 - defenses, 646-647
 - UNIX, 641-643
 - Windows, 643, 644f, 645-646
- system logs in Linux and UNIX, 632-634, 633f
 - altering accounting entry files, 634
 - altering shell history file, 635-636
- Covert Channel Tunneling Tool (CCTT), 652
- Covert channels, 647, 648f
 - defenses against, 665-667, 669
 - installation techniques, 648
 - and malware, 655-657
 - tools, 652. *See also* Covert_TCP; Loki; Nushu; Reverse WWW Shell tool
 - tunneling, 649-650
 - using HTTP, 652-655
 - using ICMP, 650-652, 651f
- Covert_TCP, 657
 - bounce operations, 659-662, 660f
 - benefits (attacker's viewpoint), 661-662
 - steps, 660-661
 - vulnerable header components, 658-659, 658f
- "Crackers," 13
- cron, 102-103





INDEX

Crouching Wi-Fi, Hidden Dragon
 scenario
 access point search (passive wireless monitoring), 676-677, 676f, 709
 credit card theft (attacker's goal), 673
 port scan, 677
 reconnaissance steps, 674
 scanning phase/scanning tools, 674-675, 675f
 security vulnerabilities of target, 677-680, 682, 683
 target selection criteria, 673-674
 using Metasploit, 682, 682f
 using Nmap, 677, 678f
 using Paros Proxy tool, 683, 684f
 VNC access to additional locations, 681, 681f
 VNC access of victim's server, 679-680, 679f

CrucialAds, 647
Cryptcat, 492
Crypto-Gram, 720
Cutler, David N., 129

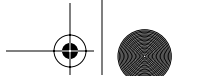
D

Da_Doc, 557
daemon9, 484, 650
Dameware, 559
Data Encryption Standard (DES), 382
Data Link Layer (2) of OSI Reference Model, 66-67. *See also* LANs and ARP, 69
Data Sentinel (Ionx), 606
Death of a Telecommuter scenario, 710
 Netcat redirector, 694

 scan for target files using cracked passwords, 695-696, 696f
 scanning for employee e-mail addresses, 687
 search for vulnerable system for hiding, 686, 687f
 stealing software (attack goal), 685
 Trojan horse backdoor program
 activation/password hashes dump and e-mailing, 693, 694f
 using e-mail addresses and sending links to custom Trojan horse backdoor tool, 688-689, 689f
 victim identification (attack target), 685-686, 686f
 victim vulnerability
 password underprotection, 695
 public newsgroups and mailing lists, 687-688
 underprotected telecommuting machines, 690-691, 691f

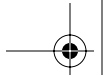
Declerk, Carl, 484
DEFCON, 720
Defenses against cyber siege, 2
Defensive techniques, reasons for, 4-5
DejaNews Web site, 208
Denial-of-service (DoS) attacks, 513-514
 categories, 514, 514f
 locally exhausting resources, 517-518, 544
 defenses, 518
 locally stopping services, 515-516, 544
 defenses, 516-517
 methods
 filling communications link, 517-518
 filling file system, 517





- filling process table, 517
 - process crashing, 515-516
 - process killing, 515
 - system reconfiguration, 515
 - remotely exhausting resources, 523,
545. *See also* Distributed Denial-
of-Service (DDoS) attacks; Smurf
attacks; SYN flood
 - remotely stopping services, 518, 519t,
520-522, 544-545
 - defenses, 522-523
 - DEP (Data Execution Prevention)/
Windows, 373-375, 374f
 - Deraison, Renaud, 310
 - DiamondCS, 295
 - Digital Equipment Corporation (DEC),
and Windows NT technology, 120
 - Digital fingerprints/signature,
584-586, 585f, 605
 - Directed broadcast attacks. *See* Smurf
attacks
 - Distributed Denial-of-Service (DDoS)
attacks, 22, 533, 543-544, 545. *See
also* Tribe Flood Network 2000
(TFN2K) tool
 - architecture, 534-535
 - defenses, 542-543
 - future directions, 541-542
 - high-profile attacks, 533-534
 - reflected DDoS attacks, 538, 539f
 - DNS and BIND, 221
 - DNS (Domain Name System),
43, 122, 220-221
 - hierarchy and root DNS servers, 221, 221f
 - other information available, 223-225,
224f
 - resolving process, 221-223, 222f
 - record types, 224t
 - split DNS technique, 228-230, 229f
 - Domains By Proxy, 220
 - Dotted-quad notation, 46-47, 47f
 - Downloading attack tools. *See also*
Controlled environment/
experimentation lab
 - risks involved in, 15-16
 - safety precautions, 18
 - Download.Ject flaw (Internet Explorer),
432-433
 - Dsniff, 442, 449-450
 - additional tools, 466, 467t, 484
 - DNS spoofing attack, 458-459, 458f
 - HTTPS and SSH sniffing capabilities,
459-466
 - confusing messages (attack alert),
463-464, 463f, 464f
 - monkey-in-the-middle attack
example, 461-462, 461f
 - protocol varieties, 450
 - sniffing methods (switched LAN)
floods, 451
 - spoofed ARP messages, 451-455, 453f
 - traffic manipulation tools, 450
 - Dumpster diving, 193-194
 - defenses against, 194-195
 - Dynamic Link Libraries (DLLs), 135
- E**
- e-commerce. *See also* Web application
attacks
 - and browser-flaws exploitations, 431-432
 - and cookies, 420-421





INDEX

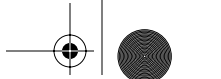
e-mail

- mass (distribution mechanism for malicious code), 563
- mass-mailing worm with a bot, 577-578, 577f
- precautions/education about, 587
- protocols, 33, 121
- Egg*, 358, 358f
- Elite-level attack skills, dual purposes, 12
- EliteWrap, 564
- Encryption, of passwords, 382-383
- Engarde Systems, 484
- Entercept (McAfee), 334
- enum, 161
- ESSID-Jack, 247, 248f
- EtherARP test, 469
- Ethereal, 445, 446f
- Ethernet, 67, 89
 - ARP, 68-69, 69f
 - hubs, 70, 70f
 - vulnerability to attack, 72. *See also* Sniffing/passive
 - MAC address, 67-68
 - switches, 70-71, 70f, 71f
 - types, 67
- Etherping test, 469
- Ettercap, 22
 - monkey-in-the-middle attack, 466
 - port stealing, 455-457, 456f
 - session hijacking tool, 484, 486-487
- Eve (scenario cast member), 14
- Execution redirection, 610-611
- Exploit frameworks, 362-363. *See also* Metasploit
 - advantages for attackers, 367-368
 - as defensive tools, 368-371

F

- FIN scan, 274-275
- Firefox (Mozilla), 463, 463f
- Firewalk, 301-302
 - defenses, 306-307
 - input and phases, 302-304, 303f, 304f
 - output uses, 306
 - packet filters focus, 304-305
 - use against layered filtering, 305
- Firewalls, 56, 57f, 88. *See also* Firewalk;
Intrusion Prevention Systems (IPSS);
Packet filters (stateful); Packet filters
(traditional); Proxy-based firewalls
approach
technology selection criteria, 65-66, 66f
usage, 56
- Flawfinder, 375
- Floods, 451
- Foundstone (McAfee), 204, 295
 - Foundscan, 310
- Fport, 295
- Fraggle, 531-532
- Fragments
 - use of in attacks at network level, 322-323
 - case example, 323-326, 324f, 325f
- FragRouter and FragRoute, 326-328, 326t-327t, 327f, 453
- FreeBSD (Berkeley Software Distribution), 92
- French Security Incident Response Team (Fr-SIRT), 339
- FTP (file transfer protocol), 120
 - Bounce scans, 278-279, 279f
 - and TCP, 33
 - port, 35





FU rootkit, 615

Function calls. *See* Stack/and function calls

Fyodor, 269

G

Gast, Matthew S., 26

“Get Out of Jail Free Card” (GOOJFC), 18

Gnu Privacy Guard (GnuPG), 76t, 193

Golden Age of Hacking, 2-3, 23, 721-722

and Golden Age of Information Security, 722

Google

attack use for, 21, 196, 236

example, 201-202

target document harvesting, 202-204

-bombing, 197

elements

Google API, 197-198

Google bots, 196

Google cache, 197

Google index, 197

Hacking DataBase (GHDB), 204, 206

markers for removing data (defensive technique), 210-211

search directives, 198, 199t-201t

search scraping, 207

search tips, 198

search tools, 204-206, 205f

useful searches, 206-207, 206f

Governments, as cyber attackers, 8

Gray World Net Team, 652

“Grey hats,” 13

Guide to Building Secure Web Applications and Web Services, 431

H

Hacker Defender, 599-602, 600f, 601f
“Hackers,” 12-13

The Hacker’s Choice group, 255

Hactivists, 9

Heap, 358-360, 360f. *See also* Buffer overflow exploits

vulnerable program example, 359, 359f

Helix, 622-623

Heyne, Frank, 647

“Hired guns,” as computer attackers, 9

Hobbit, 492

“holy father,” 599

Honeynet Project Web site, 718

Honeypot, 508-509, 617

Hping2 tool, 471

HP-UX (Hewlett Packard), 92

HTTP (Hypertext Transfer Protocol),
121. *See also* Dsniff; Reverse WWW Shell tool

floods, 540-541, 545

TCP port, 35

Huegen, Craig A., 532

Hunt, 484, 488

hxdef. *See* Hacker Defender

Hypertext Transfer Protocol (HTTP), and
TCP, 33

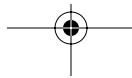
I

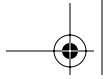
“I hack stuff” guy, 207

IBM, IDS, 251

Idle scans, 280-284, 281f, 282f

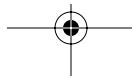
IDS (Intrusion Detection System),
319-321



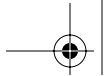


INDEX

- IDS and IPS evasion, 319-320. *See also*
Fragments; FragRouter and
FragRoute; Nikto; Whisker
defenses against, 333-335, 334f
detection-avoidance techniques,
321-322
application level, 328-333
network level, 322-328
tools (operation of), 320-321, 321f
- IDTR (Interrupt Descriptor Table
Register), and the Red Pill, 575
- IFRAME flaw (Internet Explorer), 433
- ifstatus tool, 469
- IMPACT tool (Core Security
Technologies), 362
- inetd, 100-101
- iNetTools, 232
- Information Security Magazine*, 717
- init, 99
- Insider threats/attackers, 9
business partners, 10
customers, 9
employees (disgruntled/clueless), 9
suppliers, 9
vendors, 9-10
- Intellectual property, misleading
abbreviation, 45
- Interactive TCP Relay, 416t
- Interconnections: Bridges, Routers,
Switches, and Internetworking
Protocols*, 25
- InterDo (Kavado), 423
- International Organization for
Standardization (ISO), and Open
System Interconnection (OSI)
Reference Model, 26-28
- Internet, 46. *See also* DNS (Domain Name
System)
and NAT, 56
as source of hacking information, 4
exploit trolling sites, 339-340
Web-based reconnaissance tools,
233-234, 234f, 237
widespread use of, 2
- Internet Assigned Numbers Authority
(IANA), and port numbers, 35
- Internet Control Message Protocol
(ICMP), 51, 88
message types, 52t
- Internet Corporation for Assigned Names
and Numbers (ICANN), 212
- Internet Explorer
vulnerabilities, 432-433
warning messages, 463-464, 464f
- Internet Network Information Center
(InterNIC), 213-214, 213f, 214f
- Internet Protocol (IP), 88. *See also* LANs;
Routers
addresses, 46-47. *See also* Network
mapping
header, 44-45, 45f. *See also*
Tracerouting
Destination IP Address, 50
Flags, 50
Fragment Offset, 50
Header Checksum, 50
host address, 47
IHL/Internet Header Length
field, 49-50
IP identification field, 49
network address, 47
Options, 50



- Padding, 50
 - Protocol, 50
 - Source IP Address, 50
 - Time-to-Live/TTL field, 50
 - Total Length field, 50
 - Type of Service field, 50
 - Version field, 49
 - netmasks, 47-48, 48f
 - packet fragmentation, 48-49
 - Internet Scanner (IIS), 310
 - Internet Storm Center/ISC (SANS Institute), 368, 716
 - Internet surfing, safety precautions, 17-18
 - Internetworking with TCP/IP*, 25
 - Intrusion Prevention Systems (IPSs). *See also* Firewalls
 - network-based, 65
 - IP address spoofing, 470, 511
 - attacking predictable TCP sequence numbers, 473-477, 473f, 474f, 475f
 - changing IP address, 470-472, 472f
 - defenses, 479-482
 - difficult-to-predict sequence numbers, 479
 - install antispoof packet filters, 480f, 480-481
 - no source-routed packets through network gateways, 481
 - replace r-commands, 479
 - spoofing with source routing, 477-479, 478f
 - IP. *See* Internet Protocol (IP)
 - IP Watcher, 484
 - ipconfig /displaydns, 223
 - IPS (Intrusion Prevention System), 319-321. *See also* IDS and IPS evasion
 - IPSec, 33, 75, 82-83, 89
 - Authentication Header (AH), 83, 83f, 84f
 - Encapsulating Security Payload (ESP), 84-85, 84f, 85f
 - future capabilities, 85-86
 - IRIX (sgi), 92
 - Island-hopping attacks, 441, 441f
 - ITS4, 375
- J**
- John the Ripper, 385
 - configuration, 397-400
 - operation modes, 401
 - password cracking, 396-397
 - retrieving encrypted UNIX password, 397
 - Jolt2, 519t
 - Juggernaut, 484
- K**
- Kernel-mode rootkits, 608-610, 609f, 624-625
 - defending against
 - antivirus tools, 622
 - automated checkers, 619-621
 - control kernel access, 617-618
 - dangers of preemption, 616
 - file integrity checkers, 621
 - hand checking, 618-619
 - incident handling/forensics CD, 622-623
 - prevent attackers from gaining superuser access, 616-617



INDEX

Kernel-mode rootkits (*Continued*)

- examples, 613-615
- execution redirection, 610-611
- file hiding, 611-612
- network hiding, 612-613
- process hiding, 612
- Kernel mode/Windows, 139-141
 - Executive subsystems, 139. *See also* Security Reference Monitor
 - Hardware Abstraction Layer (HAL), 140-141
 - Object Manager, 139-140

Kershaw, Mike, 246

Kil3r, 376

kill command, 106

Kim, Gene, 606

Kismet, 246-247

Knoppix-STD, 622-623

Kra, 484

L

L0phtCrack, 385

LADS (List Alternate Data Streams)
tool, 647

Land, 519t, 520

LANguard Network Security Scanner
(GFI), 310

LANguard System Integrity Monitor
(GFI), 606

LANs, 45-46, 46f. *See also* 802.11 family of protocols; Ethernet and Data Link and Physical Layers of protocol stack, 66-627

Latierra, 519t

Latin American and Caribbean Internet
Address Registry (LACNIC), 219

LC5, 385

Linux, 93

- distribution (“distro”), 93
- kernel, 93

Linux Administration Handbook, 94

Linux and UNIX (common) network services, 119-123. *See also* Domain name services; E-mail protocols; FTP (file transfer protocol); HTTP; Network File System (NFS); r-commands; Secure Shell (SSH) tool; Telnet; X Window System/X11

Linux and UNIX operating systems, 91, 124

- command-line orientation, 94
- sources of information about, 94-95

Linux and UNIX operating systems

- accounts and groups, 107, 125
- /etc/group file, 109
- /etc/psswd file, 107-109
- root (“god”/super-user) account, 110

Linux and UNIX operating systems

- architecture, 98f
- automatically starting up processes, 99, 102, 103f
- cron, 102-103
- inetd, 100-101
- init, 99
- xinetd, 100

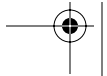
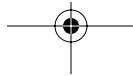
file system structure, 95-97, 95f

- directories, 96t, 97

interacting with processes, 105-107

- kill command, 106
- lsof command, 105-106
- ps command, 105
- TERM signal, 106

kernel and processes, 97-99, 124



- manually starting processes, 103-104
 - dangers of using current working directory, 104
 - Linux and UNIX operating systems
 - permissions, 110-112, 111f, 112f, 113t, 125
 - chmod command, 112
 - octal formats, 112, 113t
 - SetUID programs, 113-115
 - vulnerability of, 115
 - Linux and UNIX trust relationships, 115-117
 - logs and auditing, 117-118, 126
 - scenario example, 115-116, 116f
 - Liu, Cricket, 221
 - Local Security Authority Subsystem Service (LSASS), 135-137
 - Logic bomb, 516
 - Logs and auditing. *See also* Covering tracks/hiding
 - in Linux and UNIX, 117-118, 126, 632-634
 - Loki, 650-652, 651f
 - Long, Johnny, 204
 - lrk6 (Linux RootKit 6), 595
 - lsuf command, 105-106, 296-297, 297f
 - Lynn, Mike, 247
- M**
- MAC (Media Access Control) address, 67-68
 - MacOS (Apple Computer), 92
 - Mac OS X, 188
 - Malware, and covert channels, 655-657
 - The Manchurian Contractor scenario, 710
 - DDoS diversion, 707
 - file modification, 702-703
 - malicious company insider attacker, 697-698, 698f
 - malicious intent (attack goal), 699
 - Metasploit for control of victim's machine, 705, 705f
 - Nessus tool to look for system vulnerabilities, 701-702, 701f
 - track covering, 707-708, 708f
 - use of bots (diversionary tactics), 703-704
 - use of Cain tool, 699-700, 699f
 - using Nessus, 705
 - vulnerability of company
 - easy to crack passwords, 700, 700f
 - incorrectly assigned permissions, 702
 - omitting encryption on critical data, 707
 - MasterRat, 557
 - The Matrix Reloaded*, 269, 575, 619
 - example of execution redirection, 611
 - Megasecurity Web site, 557-558, 558f
 - Mendex, 475
 - Message Digest, 4, 382
 - Message Digest 5 (MD5) algorithm, 584-585, 585f, 596, 605
 - Metasploit, 21, 340, 435-436
 - advantages to attackers, 367-368
 - benefits to security professionals, 368-371
 - components, 363-364, 363f
 - customization tools, 367
 - payloads, 364-365
 - user interface options, 365-367, 366f
 - Web site, 717



INDEX

- Microsoft. *See also* ActiveX; Internet Explorer vulnerabilities; Windows *versions/features*
as attack target, 127-128, 177, 556
upgrades and fixes, 141-142
“Black Tuesdays,” 142
hotfixes, 141
patches, 141-142
Service Packs (SPs), 141
- Microsoft Baseline Security Analyzer (MBSA) tool, 168
- Milner, Marius, 243
- MiniStumbler, 243
- mIRC bot family, 571
- mitm (Monkey in the Middle) attack, 460
- Mitnick, Kevin, 186, 475
- Mixer, 520, 534
- Moby wordlist, 384
- Modem policy, as war dialing defense, 258-261, 336
- Montoro, Massimiliano, 385
- Moore, H. D., 362
- Morris Worm, 713
- Moser, Max, 245
- MSNShell tool, 652
- MyDoom, 578
- N**
- Nemesis, 471
- Nessus, 310, 337
advantages, 310-311
architecture, 313-314, 313f
configuration via GUI, 314
and Nmap, 312
plug-ins, 311-312
“dangerous plug-ins,” 317-318, 317f
and user-written features, 314
results reporting tool, 315-316, 315f
uses for, 316
vulnerability scanning risk of detection, 447-448
- Netcat, 491-493, 511-512
actively push a backdoor command shell, 499-500, 500f
as backdoor on UNIX systems, 550-551, 551t, 552f, 552-553
client and listening modes, 493f
connecting to open ports, 496-497
defenses, 509-501
file transfer use, 493-495, 494f, 495f
passive backdoor command-shell creation, 498-499
persistent listeners/“listen harder,” 506-508
and honeypot, 508-509
port scanning, 495-496
traffic relaying, 501-506, 501f, 503f, 505f
vulnerability scanning, 497-498
- NetDude, 471
- Netmasks, 47-48, 48f
and Classless Inter-Domain Routing (CIDR) notation, 48
- NetScan Tools Pro, 232
- Netsky, 578
- netstat command, 36, 37f
netstat -na, 294
- NetStumbler, 242-244, 244f
- Network Address Translation (NAT), 54-56, 55f, 88
gateway function, 55-56



- Network File System (NFS), 122-123, 126
 danger, 123
- Network Layer (3) of OSI Reference
 Model, 28-31, 30f, 32f, 44
- Network mapping, 261-262, 336
 defenses, 267-268
 and IP addresses, 47
 sweeping, 262
 tools, 266-267, 266f
 tracerouting, 262-267, 263f, 264f, 265f
- Network Solutions, Inc.
 registration proxy service, 220
 whois lookup, 215, 216f
- Networking. *See also* TCP/IP
 (Transmission Control Protocol/
 Internet Protocol)
 basic functions, 25
 LANs, 45-46, 46f
 other network-level functions/issues.
 See also Firewalls
 Network Address Translation (NAT),
 54-55
 network-based intrusion prevention
 systems (IPS), 65
 routing packets, 53-54
 protocols (other than TCP/IP), 26
 SS7, 26
 X.25, 26
 research resources, 25-26
 routers, 46, 46f
- Nevo tool (Tenable Network Security),
 448
- Newsgroups, 207-208
- Newtear, 519t
- Nikto, 329-333, 337
 IDS and IPS evasion tactics, 331t-332t
- Nmap, 269, 270f, 336. *See also* Nessus
 fragmentation support, 294
 inserting spoofed decoy source
 addresses in scans, 289-290
 in *The Matrix Reloaded*, 269
 operating system fingerprinting,
 290-292
 scan types supported, 270t-271t
 FTP Bounce scans, 278-279, 279f
 Idle scans, 280-284, 281f, 282f
 Ping scan, 286
 RPC programs scans, 286-287, 287f
 scans violating protocol spec, 275-276
 TCP ACK scans, 275-278, 276f, 277f
 TCP Connect, 273
 TCP SYN scans, 273-274
 UDP scans, 284-285
 Version-scan feature, 285-286
 scanning option, 21
 setting source ports for scanning,
 287-289, 288f, 289f
 timing options, 293
- No Operation (NOP) instructions/NOP
 sled, 356-358, 358f
- Novell Netware, 385
- nslookup command, 225, 236-237
- Null scan, 275
- Nushu, 22, 662-665, 663f, 664f
-
- Object Manager (Windows), 139-140
- Olphart, 475
- Open-Ports, 295
- Open Web Application Security Project
 (OWASP), 431

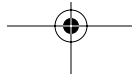


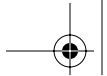
INDEX

- OpenBSD (Berkeley Software Distribution), 92, 188
- Organized crime attackers, 7-8
- Ornaghi, Alberto, 455
- OSI (Open System Interconnection)
 - Reference Model, 26-28
 - layers of, 28, 29
 - Network (Layer 3) and Transport (Layer 4) and TCP/IP, 28-31, 30f, 32f
 - protocol layering, 26-27, 26f
- Osiris, 606
- OSPF (Open Shortest Path First) protocol, 53

- P**
- P0f2, 447-448
- Packet-capture tool, multiple purposes of, 15
- Packet filters (stateful)
 - and Application-Specific Integrated Circuit (ASIC) chips, 62
 - dynamic state table, 61, 61t
 - function of, 61-62
 - security implications of, 62, 300
- Packet filters (traditional), 57-58
 - Access Control Lists (ACLs)/rules, 59-60, 59t
 - information sources for decision-making, 58-59
 - limitations of, 60
- Packet Storm Security, 339, 717
- Page, Lawrence, 197
- Pandora, 385
- Papasmurf, 532

- Paros Proxy, 416t, 418-419, 419f
- Passive operating system
 - fingerprinting, 22
- Passive vulnerability scanning. *See* Sniffing
- Password attacks, 377-378, 436
 - guessing default passwords, 378, 379f
 - limitations of, 381-382
 - via login attacks, 378-381, 380f
 - password-cracking defenses, 401-402, 436
 - additional authentication tools, 405
 - file protection for encrypted and hashed password files, 405-406
 - password-cracking tests, 405
 - password filtering software, 404
 - password policy, 402-403
 - user awareness, 403-404
- password-cracking tools, 383-385, 383f.
See also Cain and Abel tools; John the Ripper
- password storage (and encryption), 382-383
- Password Guardian, 404
- Perlman, Radia, 25
- Personal Video Recorders (PVRs), 3
- PFW (Personal Firewall Software), 656
- Phases of attacks, 6, 20. *See also* Access (maintaining); Access/application and operating system levels; Access/network level; Covering tracks/hiding; Denial-of-service (DoS) attacks; Reconnaissance (“recon”); Scanning
- phatbot family, 571, 574



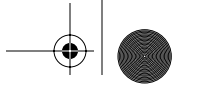


- Phenoelit hacking group, default
passwords database, 378, 379f
- Phishing attacks, 566-568
education about, 587
- Phrack, 56, 376
- Physical break-in, 190-191
defenses against, 191-193
- Physical Layer (1) of OSI Reference
Model, 66-67. *See also* LANs
- PID, 105
- Ping, 51
scan, 286
- Ping of Death, 519t, 520
- Pluggable authentication module
(PAM), 404
- Port scanning, 268, 336
defenses
find openings before attackers, 299
stateful packet filters or proxies,
300-301
system hardening, 294-299, 295f, 297f
tools, 268-269. *See also* Firewall;
Nmap; Xprobe2
potential for crashing target systems,
299-300
- Ports. *See also* Netcat; TCP port numbers
open/closed, 34
port stealing, 22
stealing, 455-457, 456f
well-known numbers, 35
- Post Office Protocol (POP), and TCP, 33
- Postel, John, 32
- Pretty Good Privacy (PGP), 76t
- PromiscDetect, 469
- Promqry/PrimaryUI (Microsoft tools),
469-470
- Protocol layering, 27, 27f
in OSI Reference model, 28
in TCP/IP (scenario example),
29-31, 30f, 32f
- Provos, Niels, 666
- Proxy-based firewalls approach,
63-65, 64f
- ps command, 105
- PUPs (Potentially Unwanted
Programs), 582
- Q**
- QualysGuard, 310
- R**
- r-commands, 116, 121. *See also* SSH
(Secure Shell) tool
in IP address spoofing attack, 473-477
- Rain Forest Puppy, 328
- RainbowCrack, 391
- RATS (Rough Auditing Tool for
Security), 375
- Rbone tool, 475
- Real Data Player (Audio/Video), UDP
port, 43
- RealSecure (ISS), 667
- Reconnaissance (“recon”), 183-184, 235
of DNS servers (zone transfers),
225-227, 236
defense from, 227-230, 229f
low-technology, 184, 235. *See also*
Caller ID spoofing; Dumpster
diving; Physical break-in; Social
engineering



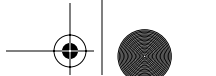
INDEX

- Reconnaissance (“recon”) (*Continued*)
- search engine and Web-based, 195-196, 236. *See also* Google; Newsgroups; Web site searching (of organization being attacked)
 - defenses against, 209-211
 - Excel and Microsoft PowerPoint files, 202
 - long-term caches, 202
 - tools (general purpose), 230, 232. *See also* Sam Spade
 - tools (Web-based), 233-234, 234f
 - whois databases, 212
 - defense against whois searches, 219-220
 - other sources of target information, 218-219
 - researching .com/.net/.org/.edu domain names, 212-214, 213f, 214f
 - researching other top-level domains, 215
 - utilizing registrar data, 215-218
- Red Pill, 575
- Remote-control backdoors. *See also* Application-level Trojan horse backdoor tools
- architecture, 556, 557f
 - functionality, 559, 559t-561t, 561
 - goals of, 555-556
 - installation approaches, 562-564
 - mass e-mailing, 563
 - wrappers and binders, 563-564
 - shipping via the Web, 565-566
 - similarities to legitimate commercial tools, 561-562
 - tools, 556-559
 - victim identification, 565
- Request for Comments (RFCs) documents (TCP/IP), 32
- Réseaux IP Européens Network Coordination Centre (RIPE NCC), 219
- RESET (spoofed packet attack), 521
- Reverse WWW Shell tool, 652-655, 653f
- Rhoades, David, 233
- RIP (Routing Information Protocol), 53
- Ritter, Jordan, 161
- Roamer, 249
- Roesch, Martin, 443
- Rootkit Hunter, 620
- Rootkit Revealer, 621
- Rootkit tools, 22. *See also* Adore-ng; FU; Hacker Defender; Kernel-mode rootkits; User-mode rootkits
- Rose, 519t, 520
- Routers, 46, 46f, 53. *See also* Packet filters (traditional)
- Routing, 53, 88
 - dynamic, 53
 - protocols, 53
 - source, 53-54
 - static, 53
- Rowland, Craig H., 657
- RPC programs scans, 286-287, 287f
- Rutkowska, Joanna, 575
- S**
- SAM database, 135-137, 178
 - NT hash, 136
 - Sam Spade, 230, 231f, 237



- capabilities, 230-232
- SANS Institute, 721
- SaranWrap, 564
- Scanning, 21, 239, 335-337. *See also* IDS
 - and IPS evasion; Network mapping;
 - Port scanning; Vulnerability-scanning tools; War dialing; War driving
 - attacker-knowledge and tools, 307t
- Scenarios. *See also* Anatomy of attacks
 - cast members, 14, 23
- Schneier, Bruce, 720
- Script kiddies, 11
 - trolling, 339-340
- sdbot family, 571
- Search scraping, 207
- SearchSecurity Web site, 717
- Secure Hash Algorithm 1 (SHA-1), 584, 605
- Secure/Multipurpose Internet Mail
 - Extensions (S/MIME), 76t, 89
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS), 75, 77-82, 77f.
 - See also* Web application attacks and authenticated/encrypted communication, 78-79, 79f, 89
 - certificates, 75, 81
 - usage, 81-82
- Security Focus Web site, 716
- Security information. *See* Attack tools
- Security Reference Monitor, 139, 178
- Segerdahl, Olle, 397
- Sentinel tool, 469
- Session hijacking, 482, 511. *See also* Ettercap/session hijacking tool; Hunt across the network example, 482-483, 483f
 - defenses, 491
 - host-based, 483-484
 - tools, 484
 - limitations of, 485
 - wireless access point attacks, 488-490
- Session IDs, 411-412
- Session tracking attacks. *See* Web application attacks
- SetUID programs, 113-115, 125
 - vulnerability of, 115
- Shiple, Peter, 240
- shv4 rootkit, 595
- Silk Rope, 564
- Simple Mail Transfer Protocol (SMTP), and TCP, 33
- Simple Network Management Protocol (SNMP), UDP port, 43
- Simple Nomad, 385
- SirMACsAlot tool, 249
- SiteDigger, 204, 205f
- “Smashing the Stack for Fun and Profit,” 342
- SMTP, TCP port, 35
- Smurf amplifier, 530
- Smurf attacks, 529-532, 531f, 545
 - defenses, 532-533
 - and netmasks, 48
- Sniffer, 439. *See also* Cain and Abel tools; Packet-capture tool
 - interfaces, 442
 - and island-hopping attacks, 441, 441f
- Sniffing, 439-440, 510
 - active (through a switch), 449, 449f, 510. *See also* Dsniff; Ettercap
 - data vulnerable to capture, 440
 - promiscuous/nonpromiscuous mode, 440



INDEX

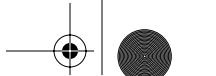
Sniffing (*Continued*)

- defenses, 467-470, 511
 - hub elimination, 468
 - secure protocols, 467-468
 - sniffer-detection tools, 468-470
- passive (through a hub), 442, 443f. *See also* *Ethereal*; *Sniffit*; *Snort*
- passive vulnerability scanning, 446-448. *See also* *Nevo* tool; *P0f2*
- tools, 441-442
- Sniffit*, 442, 444-445, 444f
- Snort*, 442-443
- Sobig*, 578
- Social engineering, 184-185
 - defenses against, 190
 - pretexts (common), 185-186
- Solar Designer*, 385, 396, 404
- Solaris* (Sun Microsystems), 92
- Song, Dug*, 326, 449, 460
- Sourcefire*, 443
 - Intrusion Sensors*, 667
- Spafford, Gene*, 606
- Spencer, Mark*, 188
- Spike*, 520
- SPIProxy/WebInspect*, 416t
- Spitzner, Lance*, 718
- Spl0it*, 358, 358f
- Spoofting. *See* IP address spoofing
- Spyware, 22, 578
 - functionality, 579f
 - installation methods, 579-581
 - bundling, 580-581
 - and Web browser vulnerabilities, 581
- SQL injection attacks. *See* Web application attacks
- SS7*, 26
- SSH (Secure Shell) tool, 76t. *See also* *Dsniff*
 - and TCP, 33
 - port, 35
 - to replace r-commands, 116-117
- sshmitm* (SSH Monkey in the Middle) attack, 460, 465, 484
- Stack*, 345, 346f. *See also* Buffer overflow exploits
 - and function calls, 344-347, 345f
 - nonexecutable (defensive technique), 372-373
- Stack Shield*, 376
- StackGuard*, 376
- Star38*, 187-188
- STAT Scanner* (Harris), 310
- Stearns, Bill*, 447
- Steganography*, 666, 669
- Stevens, W. Richard*, 25
- STFW (Search the Fine Web) strategy, 195-196
- Strongpass*, 404
- SubSeven*, 559, 565
- Sullo*, 329
- Sweeping, 262
- SYN flood,
 - 523-523, 523f, 526, 540, 545
 - defenses, 526-529
 - queue/bandwidth sizes and redundant paths, 526-527
 - SYN cookies, 527-529, 527f
 - traffic shaping tools, 529
 - filling communications link, 525-526
 - filling connection queue, 524-525
- Syndrop*, 519t



T

- Targa (Mixer), 520, 534
- TCP ACK scans, 275-278, 276f, 277f
- TCP Connect scans, 273
- TCP control bits (flags), 37f, 87
 - ACK (Acknowledgment) field, 38
 - CWR (Congested Window Reduced) field, 38
 - ECE (Explicit Congestion Notification Echo) field, 38
 - FIN field, 38
 - PSH (Push) function, 38
 - RST (Reset) function, 38
 - SYN (Synchronize) sequence number function, 38
 - URG (Urgent) bit, 38
 - uses, 37
 - session-initiation scenario example, 38-40
- TCP port numbers, 36f. *See also* netstat command; Nmap
 - destination port, 34
 - open port/closed port, 34, 36
 - port zero, 34
 - source port, 34
 - TCP Port 21 (FTP), 35
 - TCP Port 22 (SSH), 35
 - TCP Port 23 (Telnet), 35
 - TCP Port 25 (SMTP), 35
 - TCP Port 80 (HTTP), 35
 - TCP Port 6000 (X Window System/X11), 35
- TCP Reset attacks, 22
- TCP SYN scans, 273-274
- TCP/CP, 649
- TCP/IP Illustrated*, 25
- TCP/IP (Transmission Control Protocol/Internet Protocol), 26, 87-89
 - development of, 33
 - family of protocols, 32, 32f, 87. *See also* Internet Control Message Protocol (ICMP); Internet Protocol (IP); Transmission Control Protocol (TCP); User Datagram Protocol (UDP) and Network Layer (3) and Transport Layer (4) of OSI Reference Model, 28-31, 30f, 32f, 44
 - Request for Comments (RFCs) documents, 32
 - resources, 25
 - security capabilities, 33, 86-87. *See also* Application-level security for TCP/IP-based networks; IPsec; Secure Sockets Layer (SSL)/Transport Layer Security (TLS)
- TCPView, 295, 295f
- Teardrop, 519t, 520
- Telespoof, 187-188
- Telnet, 119
 - TCP port, 35
- Tenable Network Security, 310. *See also* Nessus
- TERM signal, 106
- Terrorists, and cyber attacks, 8
- TFN2K. *See* Tribe Flood Network 2000 (TFN2K) tool
- THC-Scan, 652
- Three-way handshake, 87-88, 272, 272f, 471
 - scenario example of TCP session initiation, 38-40
- Timmingh, Roelof, 204



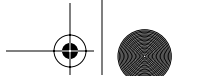
INDEX

Toast (Gridmark), 520
Torvalds, Linus, 93
Tracerouting, 262-265, 263f, 264f, 265
Traffic relaying,
 501-506, 501f, 503f, 505f
Transmission Control Protocol (TCP)
 applications, 33
 header, 34, 34f. *See also* TCP control
 bits (flags); TCP port numbers
 session-initiation/three-way handshake
 (scenario example), 38-40
Transport Layer (4) of OSI Reference
 Model, 28-31, 30f, 32f, 44
Tribe Flood Network 2000 (TFN2K) tool,
 534-537
 attack types, 534
 client-zombie communication
 mechanism, 534-537
 DDoS attack model, 535f
 simultaneous single arbitrary
 command feature, 537
Tripwire, 516-517, 607
Trivial File Transfer Protocol (TFTP),
 UDP port, 43
Trojan horse backdoor genre, 553-554,
 554t, 624. *See also* Application-level
 Trojan horse backdoor tools;
 Kernel-mode rootkits; User-mode
 rootkits
Trojan horses, 547-548, 623
Trojan Man, 564
Tsutomu Shimomura, 475
TTL field (IP header), 50
TTYSnoop, 484
TTYWatcher, 484
Tunneling, 649-650. *See also* Loki

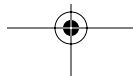
U

UDP. *See* User Datagram Protocol (UDP)
Underlying technologies and platforms,
 19. *See also* Linux and UNIX
 operating systems; Networking;
 Windows
UNIX, 92. *See also* Linux and UNIX
 operating systems
 / (“slash”) directory, 124
 main lines, 93
 tools, r-commands, 116
 variants, 92-93
URL
 obfuscation, 567-568
 session tracking, 411-412, 411f
U.S. Computer Emergency Readiness
 Team (CERT), 718-719
User Datagram Protocol (UDP), 41-43, 88
 header, 43, 43f
 ports, 43
 Port 53/DNS, 43
 Port 69/TFTP, 69
 Port 161/SNMP, 69
 Port 7070/Real Player Data, 69
 scans, 284-285
 security, 43-44
User-mode rootkits, 587-588, 588f, 624
 defending against
 file integrity checkers, 605-607
 preventing installation, 604-605
 functions, 589
 history of, 588-589
 Linux/UNIX user-mode rootkits, 589
 additional hiding techniques,
 593-594, 594t
 backdoors, 589-592





- examples, 595-596
- and hiding sniffer, 592-593
- and password sniffing, 592
- track covering, 594
- recovery from attack, 607-608
- Windows, 596
 - API hooking, 597-598, 598t
 - examples, 599-604
 - hiding strategies, 597-599
 - implementation, 599
 - tactics, 596-597
- User mode/Windows, 134
 - and APIs (Application Program Interfaces), 134
 - Environment services, 135
 - Integral subsystems, 135
 - security-related functions in, 135-137
 - LM password representation, 136
 - NT hash, 137
 - password derivation, 137-139
- Uwhois Web site, 215
- V**
 - Vacuum, 161
 - Valleri, Marco, 455
 - van Hauser, 255, 652
 - Vandalism, archive of, 627
 - Version-scan feature, 285-286
 - Vidstrom, Arne, 632
 - Virtual machines
 - and Red Pill, 576
 - as research tools, and
 - vulnerabilities of, 574
 - Virtual Network Computing (VNC)
 - tool, 559
 - VoIP (Voice over IP) services, and
 - spoofing caller ID, 188
 - von Braun Consultants, 558
 - VPN (Virtual Private Network), 250-251
 - Vulnerability-scanning tools, 15, 362-363.
 - See also* Nessus; Netcat
 - commercially available scanners, 310
 - defenses
 - closed ports and system
 - patches, 316
 - use tools against your network,
 - 316-318
 - limitations of, 318-319
 - operation of, 308-309, 309f
- W**
 - War dialing, 252-253
 - defenses, modem policy, 258-261
 - modems/remote access products/naive users, 253-254
 - nudging function, 257-258
 - phone numbers (requirement), 254
 - sources, 254-255
 - tools, THC-Scan, 255-257, 255f, 256t
 - War driving, 240-241. *See also* 802.11
 - family of protocols
 - antennas, 241
 - defenses, 248
 - configuring access points/using wireless security protocols,
 - 249-250
 - deploying a VPN, 250-251
 - detection, 251
 - physical protection, 252
 - setting ESSID, 248



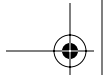


INDEX

- War driving (*Continued*)
 - ESSID (Extended Service Set Identifier) determination, 241
 - Methods. *See also* ESSID-Jack; Kismet; NetStumbler; Wellenreiter
 - active scanning, 242-244
 - forcing deauthentication, 247, 248f
 - passive scanning, 245-247
 - tools, 242
- War Games, 252
- Watson, Paul, 522
- Wayback Machine, 202, 211
 - session tracking attacks, defenses, 421-423
- Web application attacks, 406-407, 436-437
 - account harvesting, 407-410, 408f, 409f
 - defenses, 410
 - browser-flaws exploitation, 431-434, 437
 - attack examples, 432-433
 - defenses, 434
 - manipulation proxies, 416t, 417-420
 - session tracking attacks, 412-421. *See also* Session IDs
 - detection difficulties, 413
 - nonpersistent, 414f, 415, 416f
 - persistent cookies, 414-415
 - session ID manipulation, 413-414
 - SQL injection attacks, 423-428, 425f, 426f, 427f, 437
 - defenses against, 428-431. *See also* WebGoat
 - SSL limitations, 407
- Web site searching (of organization being attacked), 208-209
- Web Sleuth, 416t
- WebGoat, 22
 - SQL injection attack example, 424-428, 425f, 426f, 427f
- WebScarab, 416t
- Wellenreiter, 245-247, 246f
- Wheeler, Dave, 375
- Whisker, 328, 337. *See also* Nikto
- “White hat,” 13
 - and presentations of threats, 656
- Widner, Michael R., 475
- Wikto, 204
- Windows accounts, 142, 178
 - default, 142-144
 - Administrator, 143
 - Guest, 143-144
 - security issues, 144-145
 - other, 144
- Windows auditing, 154-155, 155f
- Windows fundamental concepts. *See also* Windows underlying operating system architecture
 - domain, 131-132, 177
 - Primary Domain Controller (PDC), 132
 - domains, *workgroups*, 132
 - shares, 133
- Windows groups, 142, 145-146, 178
 - default, 146-147, 146t
 - other, 147
- Windows network security, 160, 179
 - limitations/basic network protocols and APIs, 160, 180
 - Common Internet File System (CIFS), 161
 - Microsoft’s Internet Information Service (IIS), 161-162



- NetBEUI (Network Basic Extended User Interface), 161
- NetBIOS (Network Basic Input/Output System), 161
- Service Message Block (SMB), 161
- Windows NT, 162, 178
 - history of, 128-130, 156
- Windows object access control and permissions, 156
 - File Allocation Table (FAT), 156
 - NTFS and permissions, 156-157
 - EVERYONE group limits, 158
 - Full Control permissions/dangers and limits, 157
 - Take Ownership right/dangers and limits, 157-158
 - ownership, 156
 - Share permissions, 158
 - weak default permissions and guides for hardening, 159-160
- Windows policies, 149
 - Account Policy, 149-151, 150f
 - Account Lockout, 150-151
 - User Properties settings, 151-152
- Windows privilege control, 147-148
 - rights and abilities*, 147, 149f
- Windows trust, 152-154
- Windows 2000, 130-131, 162-163, 180. *See also* Active Directory
 - accounts and groups, 169
 - architecture (and refinements over NT), 168-169
 - auditing, 175, 181
 - event logging (EventLog), 629-630, 630f
 - altering, 631-632
 - new features, 163
 - domains deemphasis, 164-166, 180
 - native vs. mixed mode, 164, 180
 - and new security features, 163-164
- object access control
 - EFS (Encrypting File System), 176-177, 181, 193
 - NTFS-5, 175-176, 181
- organizational units (OUs), 169-170, 170f, 180-181
- physical security considerations, 167-168
- policies, 174
 - Group Policy Objects (GPOs), 173-174, 173f
- privilege control (changes), 170
 - rights, 170-171, 171f, 181
 - RunAs, 172, 172f
- Security Configuration Tools (templates and wizards), 168
- security considerations, 166, 180
 - Active Directory protection, 167
- stack, 373-375
- trust, 174-175
 - Kerberos-based, 181
- Windows underlying operating system
 - architecture, 133, 134f. *See also* Windows accounts; Windows auditing; Windows fundamental concepts; Windows groups; Windows network security; Windows object access control and permissions; Windows policies; Windows privilege control; Windows trust



INDEX

- Windows underlying operating system
 - architecture (*Continued*)
 - modes, 134. *See also* Kernel mode/
Windows; User mode/Windows
 - security implications, 133, 156
 - Windows XP, 130
 - WinFingerprint, 161
 - Winnuke, 519t, 520
 - WinZapper tool, 632, 668
 - Wireless Intrusion Detection Systems
(IDSs), 2561
 - Wireless Local Area Networks (WLANs),
240. *See also* 802.11 family of
protocols; War driving
rfmon/monitor mode, 245
 - Wireless Networks: The Definitive Guide*, 26
 - World Wide Web (WWW). *See also* Web
application attacks
source for information for attacker,
235-236
 - Worm-bot feedback loop, 575-578, 577f
 - Worms, 576-577
 - Morris Worm, 713
 - Wrappers, 563-564, 564f
 - Writing Secure Code*, 2, 375
- X**
- X.25, 26
 - X Window System/X11, 123
 - TCP port, 35
 - xinetd, 100, 515
 - Xmas Tree scan, 275
 - Xprobe2, 292-293
- Y**
- Yarochkin, Fyodor, 292
 - ywindump, 441
- Z**
- Zalewski, Michael, 447
 - Zeus Web servers, 162
 - Zhu Shuanglei, 391
 - Zombie software, 534
 - Zombies
 - avoiding, 542
 - pulsing, 538, 540
 - Zone-H Web site, 627
 - Zone transfers, 225-227, 237
 - limiting, 227-228

