

# INDEX

## Symbols

802.1X

applying, 272-282  
enforcement, 298

## A

acceptable use policy  
(AUP), 122

access

anonymous restrictions,  
369-372

controls (physical  
security), 165-168

GUIs, 60

LUA (least user  
access), 398

masks, 503

remote, 198-200

restrictions, 253-257, 264  
rogue

applying 802.1X,  
272-282

enabling IPsec,  
283-294

layer 2/3 protection,  
269-271

network quarantine  
systems, 296-300

preventing, 267  
sniffing, 267-268

Web, 198-199

access control lists.

*See* ACLs

accounts

administrative security,  
218-222

IDS, 52

lockout, 385

logon events, 384

passwords, 344

services, 421

ASR (attack surface  
reduction), 418-420

dependencies, 222

mitigating, 223-228

securing, 427-434

SRPs (software  
restriction policies),  
366-367

ACKnowledge packets, 38

ACLs (access control lists),  
353, 493

best practices, 509-513

layers, 507-509

security descriptors,  
495-506

ACS (Audit Collection  
Services), 458

active administrative  
dependency, 218

active attacks, 7

active-automated attacks, 8

active-manual attacks, 9

AdAware, 412

Address Resolution  
Protocol (ARP)  
attacks, 270-271

addresses

ranges, 34-36

spoofing, 190-191

administration

attachments, 408-410

Help, 151-152

passwords, 225-228, 307

applying, 317-325

attacks, 326-332

configuring, 536-539

passgen tool, 529-539

storage, 307-316

patches

advanced techniques,  
97-100

as risk management,  
83-84

AU/WSUS, 94

automatic updates, 94

building test bed,  
88-90

definition of, 81, 83

EMS (enterprise  
management system),  
95-96

MBSA (Microsoft  
Baseline Security  
Analyzer), 93

**552** INDEX

- need for, 79-80
- security update tools, 91-93
- selection of, 96
- slipstreaming, 101-108
- testing security updates, 85-87
- penetration testing, 28-31
- rights systems, 513-517
- risk, 113, 118-119
- security, 135-136
  - administrator responsibilities, 18
  - dependencies, 218-222
  - mitigating services, 223-228
  - receiving feedback, 14-20
  - usability, 16-18
  - vendor design tradeoffs, 19-20
  - system administration, 135-136
- administrator password policy (APP), 122
- administrators, 220
  - passwords, 536-539
  - responsibilities, 18
- ADS (Automated Deployment Services), 101
- Advanced Encryption Standard (AES), 176
- adware, 450
- AES (Advanced Encryption Standard), 176
- agent-based enumeration, 92
- agent recovery, 176
- AH (Authentication Header), 286
- ALE (annualized loss expectancy), 119
- Alerter service, 418
- algorithms, troubleshoot- ing, 485
- analysis
  - environments, 415-416
  - Exchange Server Best Practices Analyzer Tool, 454
  - existing systems, 512
  - hacking, 72-73
  - MBSA (Microsoft Baseline Security Analyzer), 93
  - penetration testing, 24, 28-31
  - security needs, 118-128
  - threats, 244, 246, 248
- annualized loss expectancy (ALE), 119
- anonymous connections (null sessions), 50
- anonymous restrictions, 369-372, 384
- anti-malware, 379
- anti-spyware software, 450
- antivirus policy (AVP), 123
- antivirus software, 450
- API (application programming interface), 55
- APP (administrator password policy), 122
- application-filtering firewalls, 194-195
- applications
  - analyzing, 415-416
  - ASR (attack surface reduction), 418
  - blocking unnecessary interfaces, 420
  - disabling unnecessary features, 419
  - uninstalling unnecessary components, 418-419
- data-protection mechanisms, 517-518
- exposed (on hosts), 39
- functionality
  - restricting browser, 402-407
  - turning off, 400-402
- hiding, 357
- LUA (least user access), 398
- patches, 41, 395-398
- security
  - baselining systems, 469-470
  - evaluating, 467
  - reviewing, 471-474, 477-487
- servers, 417
- services, 421-426
- small businesses
  - applying anti-spyware/ antivirus software, 450
  - configuring firewalls, 451-453
  - controlling automatic updating, 449
  - updating, 448-449
- spyware, 411

- states, 41
  - structure of, 42
  - updates, 96
  - version information, 40
  - Web, 441
  - applying
    - 802.1X, 272-282
    - anti-spyware/antivirus software, 450
    - firewalls, 192-198
    - IPsec, 283-294
    - passwords, 317-325
    - security guides, 362
  - ARP (Address Resolution Protocol) attacks, 270-271
  - ASR (attack surface reduction), 418-420
  - assessment of penetration tests, 24
  - associations (security), 283
  - attachment management, 408-410
  - attack surface reduction (ASR), 418-420
  - attackers, Warez, 47
  - attacks
    - ARP (Address Resolution Protocol), 270-271
    - cached credentials, 331
    - casual attackers, 5
    - cross-site scripting, 479
    - damage (types of), 10, 13
    - DDoS (Distributed DoS), 188
    - detecting, 150
    - DoS (denial-of-service), 188, 243
    - elevation-of-privilege, 243
    - hacking
      - analyzing, 72-73
      - cleaning attackers, 74-76
      - detecting initial compromise of, 43-45
      - elevating privileges, 46-50
      - footprinting networks, 34-43
      - null sessions, 50-57
      - taking over, 59-71
    - passwords, 326-332
    - penetration testing, 28-31
    - reflection, 230
    - spoofing, 190-191
    - target networks, 32
    - types of, 7, 9-10
  - AU (Automatic Update), 94, 449
  - Audit Collection Services (ACS), 458
  - auditing, 377
    - CrashOnAuditFail, 386
    - enabling, 384-385
    - full privilege, 386
  - AUP (acceptable use policy), 122
  - authentication, 283
    - challenge-response transactions, 229-234
    - LAN Manager, 375, 383
    - mutual, 279
    - passwords, 303-305
      - applying, 317-325
      - attacks, 326-332
      - best practices, 334-344
      - management, 307-316
    - multifactor authentication, 346-348
      - overview of, 305-307
      - policies, 345
    - physical security, 168
    - SQL Servers
      - customizing, 435
    - IIS (Internet Information Services), 441
      - troubleshooting, 482
  - Authentication Header (AH), 286
  - authenticity, 187
  - authorization, 283
  - automated attacks, 7
  - Automated Deployment Services (ADS), 101
  - Automatic Update. *See* AU; updates
  - availability, 187-189, 519
  - avoiding
    - hacking, 521
    - viruses, 13
  - AVP (antivirus policy), 123
  - awareness of security, 128-129, 149-150
- B**
- back-end servers, structure of, 42
  - baselining
    - MBSA (Microsoft Baseline Security Analyzer), 93
    - performance, 90
    - systems, 469-470
  - batching patches, 100

**554** INDEX

- beds (patch test), building, 88-90
- Bell-LaPadula model, 225
- best practices
  - ACLs (access control lists), 509-513
  - Exchange Server Best Practices Analyzer Tool, 454
  - passwords, 334
    - account lockout, 344
    - disabling LM hashes, 335-336
    - protecting cached credentials, 334-335
    - selection, 337-344
- Bill Payer service, 216
- black-box tests, 30
- blocking
  - ICMP echoes, 38
  - spyware, 527-528
  - unnecessary interfaces, 420
- borders, connecting routers, 190-191
- browser functionality, restricting, 402-407
- buffers, troubleshooting, 483
- building
  - patch test beds, 88-90
  - slipstreamed installation points, 102-108
- built-in shares, 510
- C**
- CA Unicenters, 95
- cached credentials, 315-316
  - attacks, 331
  - disabling, 386
  - protecting, 334-335
- caches, 244
  - California law SB 1386 (public disclosure), 120
- call detail record (CDR), 115
- cardinal points, 102
- casual attackers, 5
- CDR (call detail record), 115
- CERNIC (China Education and Research Network Information Center), 184
- certificates, 284
- Certified Information Systems Security Professional (CISSP), 225, 494
- challenge-response transactions, 229-234
- Character Map tool, 476
- characters, passwords, 307-308, 311-316
- China Education and Research Network Information Center (CERNIC), 184
- circuit proxies, 195
- circumvention vulnerabilities, 137
- CISSP (Certified Information Systems Security Professional), 225, 494
- classification systems (security policies), 127
- cleaning attackers, 74, 76
- clearing virtual memory, 387
- cleartext data, troubleshooting, 484
- clients (businesses)
  - information, storing on servers, 455-458
  - protecting PCs, 169-172
- clients (networks)
  - password policies, 382
  - quarantine, 297
  - security tweaks
    - anonymous restrictions, 384
    - blank passwords, 383
    - enabling auditing, 384-385
    - LAN Manager authentication, 383
    - limiting malicious code, 377-378
    - removable media, 385
    - SafeDllSearchMode, 379-382
    - SMB message signing, 383
    - VPN, 208
  - Clustering Service, 317
- clusters, 251
- CMAK (Connection Manager Administration Kit), 300
- code
  - malicious, 377-378
  - worms, 13
- Cold Fusion Expression Evaluator, 417
- components
  - quarantine systems, 297-300
  - RMS (Rights Management Services), 516-517

- uninstalling, 418-419
- unused (turning off functionality), 400
- compromising networks, cleaning attackers, 74-76
- computation, LM hash, 309
- computers
  - dealing with stolen, 173-179
  - family (physical security), 180
  - protecting (physical security), 169-172
  - small businesses
    - applying anti-spyware/antivirus software, 450
    - configuring firewalls, 451-453
    - controlling automatic updating, 449
    - protecting, 447-448, 464-465
    - updating software, 448-449
- conclusions of penetration testing, 29
- confidentiality, 178, 185
- configuration
  - audit settings, 377
  - firewalls for small business, 451-453
  - passwords (administrators), 536-539
  - replicating, 88
  - security
    - false information about guides, 354-363
    - tools, 387-391
    - troubleshooting, 483
- SQL Server
  - customizing
    - authentication, 435
  - dropping stored procedures, 436-438
  - hardening, 426-427
  - securing service accounts, 427-434
  - supportability, 416
- Connection Manager Administration Kit (CMAK), 300
- connections
  - anonymous (null sessions), 50
  - border routers, 190-191
  - outbound, 264
- controls
  - access (physical security), 165-168
  - remote, 201-202
- cracking, 327-331
- CrashOnAuditFail, 386
- credentials
  - cached, 315-316
    - attacks, 331
    - protecting, 334-335
  - caches, 386
- critical updates, 83
- cross-site scripting, 45, 479
- crypto algorithms, troubleshooting, 485
- customization
  - audit settings, 377
  - defense-depth model, 20-23
  - firewalls for small business, 451-453
- network threat modeling
  - processes, 237-238
  - access restriction, 253-257, 264
  - documentation, 238-248
  - segmentation, 248-251
- passwords (administrators), 536-539
- replicating, 88
- security, 114
  - analyzing security needs, 118-128
  - creating awareness of, 128-129
  - enforcing, 130
  - failure of, 116
  - false information about guides, 354-363
  - identifying threats, 117
  - modifying, 129
  - necessity of, 115
  - structure of, 114-115
  - tools, 387-391
  - troubleshooting, 483
- SQL Server
  - customizing
    - authentication, 435
  - dropping stored procedures, 436-438
  - hardening, 426-427
  - securing service accounts, 427-434
  - supportability, 416
  - tradeoffs (vendors), 19-20

**556** INDEX

- D**
- damage from attacks
    - (types of), 10, 13
  - data destruction
    - attacks, 10
  - Data Encryption Standard (DESX), 176
  - data flow diagrams (DFDs), 238-240
  - data modification attacks, 10, 12
  - data protection for small businesses, 461-462
  - Data Source Name (DSN), 441
  - data-protection
    - mechanisms, 491-492
    - ACLs (access control lists), 493
    - best practices, 509-513
    - layers, 507-509
    - security descriptors, 495-506
    - applications, 517-518
    - rights management systems, 513-517
    - security groups, 493
  - databases
    - security, 482
    - troubleshooting, 471-479
  - DC (domain controller), 32, 165
  - DDoS (distributed denial-of-service) attacks, 188
  - debugging LSA, 53
  - defense-in-depth model, 20-23, 363-364
  - demilitarized zone (DMZ), 32
  - denial of service. *See* DoS
  - dependencies, 215
    - administrative security, 218-228
    - overview of, 215-217
    - service accounts, 222
    - types of, 229-234
    - UNIX, 233
  - deperimeterization, 210-212
  - descriptors, security, 495-506
  - DESX (Data Encryption Standard), 176
  - detecting attacks, 150
  - deterministic passwords, 536
  - development
    - audit settings, 377
    - defense-depth model, 20-23
    - firewalls for small business, 451-453
    - network threat modeling processes, 237-238
    - access restriction, 253-257, 264
    - documentation, 238-248
    - segmentation, 248-251
    - passwords (administrators), 536-539
    - replicating, 88
    - security, 114
      - analyzing security needs, 118-128
      - creating awareness of, 128-129
      - enforcing, 130
      - failure of, 116
      - false information about guides, 354-363
      - identifying threats, 117
      - modifying, 129
      - necessity of, 115
      - structure of, 114-115
      - tools, 387-391
      - troubleshooting, 483
  - SQL Server
    - customizing
      - authentication, 435
    - dropping stored procedures, 436-438
    - hardening, 426-427
    - securing service accounts, 427-434
    - supportability, 416
    - tradeoffs (vendors), 19-20
  - DFDs (data flow diagrams), 238-240
  - diagrams, DFDs (data flow diagrams), 238-240
  - dialog boxes, Manage Add-ons, 397
  - digital certificates, IPsec, 284
  - direct tap policy (DTP), 127
  - disabling
    - cached credentials, 386
    - LM hashes, 335-336, 368
    - unnecessary features, 419
    - USB drives, 171
  - DiscoverHosts, executing, 54
  - distributed denial-of-service (DDoS) attack, 188

- Distributed Management Objects (DMO), 436
- distribution, password length, 324
- DMO (Distributed Management Objects), 436
- DMZ (demilitarized zone), 32
- DNS (Domain Name Server) lookup requests, 37
- Do Not Duplicate markings, 167
- Document Tracking and Administration (DTA), 436
- documentation
  - passwords, 341
  - network threat modeling processes, 238-248
  - security policies
    - analyzing security needs, 118-128
    - creating awareness of, 128-129
    - developing, 114
    - enforcing, 130
    - failure of, 116
    - identifying threats, 117
    - modifying, 129
    - necessity of, 115
    - structure of, 114-115
- domain controller (DC), 32, 165
- Domain Name Server (DNS) lookup requests, 37
- domains
  - cached credentials, 315-316
    - attacks, 331
    - protecting, 334-335
  - isolation, 294
  - LM hash value storage, 368
  - Local groups, 493
  - Microsoft, 146
  - taking over, 59-67, 69-71
- doors, locking, 167
- DoS (denial of service), 10, 188, 243
- downtime, preventing, 99
- DPAPI (Windows Data Protection API), 179
- drives, disabling USB, 171
- dropping stored procedures, 436-438
- DSN (Data Source Name), 441
- DTA (Document Tracking and Administration), 436
- DTP (direct tap policy), 127
- dumpinfo, 55
- E**
- e-mail
  - attachment manager, 408-410
  - HTML security, 405-407
- EAP-TLS, 273
- echoes (ping), 38
- education for users, 152-153
- EFS (encrypting file system), 175-178, 227
- Eggshell Principle (hacking), 31
- ejecting removable media, 385
- elevating privileges, 46, 48, 50
- elevation-of-privilege attacks, 243
- EMS (enterprise management system), 95-96, 223
- enabling
  - anonymous restrictions, 369-372
  - auditing, 384-385
  - automatic updates, 449
  - controls (physical security), 165-168
  - GUIs, 60
  - IPsec, 283-285, 287-294
  - LUA (least user access), 398
  - masks, 503
  - remote access, 198-200
  - restrictions, 253-257, 264
- rogue access
  - applying 802.1X, 272-282
  - enabling IPsec, 283-294
  - layer 2/3 protection, 269-271
  - network quarantine systems, 296-300
  - preventing, 267
  - sniffing, 267-268
  - startup keys, 179
  - Web, 198-199
- encrypting file system (EFS), 175-178, 227

**558** INDEX

- encryption
    - files, 175-177
    - PPTP (Point-to-Point Transfer Protocol), 36
  - end users (security)
    - exploits against, 140-141
    - involvement vs.
      - influence, 142-143
    - protecting, 148-153
    - social engineering,
      - 137-139, 143-148
    - value of passwords, 139
  - enforcement
    - 802.1X, 298
    - IPsec, 298
    - quarantine systems, 297
    - security policies, 130
  - enterprise management
    - system (EMS),
      - 95-96, 223
  - enumeration, tools, 92
  - environments, analyzing,
    - 415-416
  - ESP (encapsulated security payload), 286
  - evaluation
    - access masks, 503
    - applications
      - baselining systems,
        - 469-470
      - reviewing, 471-474,
        - 477-487
      - security, 467
    - network threat modeling
      - processes, 237-238
      - access restriction,
        - 253-257, 264
      - documentation,
        - 238-248
      - segmentation, 248-251
  - events, logon, 384
  - Everyone group, 505
  - Exchange Server 2003, 199
  - Exchange Server Best Practices Analyzer Tool, 454
  - executing
    - audit settings, 377
    - defense-depth model,
      - 20-23
    - DiscoverHosts, 54
    - firewalls for small
      - business, 451-453
    - LUA (least user access)
      - applications, 398
    - network threat modeling
      - processes, 237-238
      - access restriction,
        - 253-257, 264
      - documentation,
        - 238-248
      - segmentation, 248-251
    - passwords (administrators),
      - 536-539
    - replicating, 88
    - security, 114
      - analyzing security
        - needs, 118-128
      - creating awareness of,
        - 128-129
      - enforcing, 130
      - failure of, 116
      - false information about
        - guides, 354-363
      - identifying threats, 117
      - modifying, 129
      - necessity of, 115
      - structure of, 114-115
      - tools, 387-391
      - troubleshooting, 483
  - SQL Server
    - customizing
      - authentication, 435
      - dropping stored
        - procedures, 436-438
      - hardening, 426-427
      - securing service
        - accounts, 427-434
      - supportability, 416
      - tradeoffs (vendors),
        - 19-20
    - existing systems,
      - analyzing, 512
    - expected hosts, 37-38
    - expiration (of
      - passwords), 345
    - exploits against users,
      - 140-141
    - exposed applications (on
      - hosts), 39
    - extended stored procedure
      - (xproc), 47
- F**
- failures, CrashOnAuditFail,
    - 386
  - family PCs (physical
    - security), 180
  - fault trees, 245
  - features, disabling, 419
  - feedback, receiving, 14-20
  - file encryption key
    - (FEK), 175
  - files
    - audit settings, 377
    - defense-in-depth model,
      - 20-23
    - DiscoverHosts, 54
    - encrypting, 175-177



- firewalls for small
    - business, 451-453
  - generic rights on, 500
  - HOSTS, 527-528
  - LUA (least user access)
    - applications, 398
  - network threat modeling
    - processes, 237-238
    - access restriction, 253-257, 264
    - documentation, 238-248
    - segmentation, 248-251
  - passwords (administrators), 536-539
  - replicating, 88
  - security, 114
    - analyzing security needs, 118-128
    - creating awareness of, 128-129
    - enforcing, 130
    - failure of, 116
    - false information about guides, 354-363
    - identifying threats, 117
    - modifying, 129
    - necessity of, 115
    - structure of, 114-115
    - tools, 387-391
    - troubleshooting, 483
  - SQL Server
    - customizing authentication, 435
    - dropping stored procedures, 436-438
    - hardening, 426-427
    - securing service accounts, 427-434
  - SRPs (software restriction policies), 366-367
  - supportability, 416
  - TIF (temporary Internet files), 244
  - tradeoffs (vendors), 19-20
  - filtering
    - IPsec, 284, 365, 379
    - traffic, 254-257
  - firewalls
    - applying, 192-198
    - malicious code (limiting), 378
    - small businesses, 451-453
    - types of, 193
    - Windows XP Service Pack 2, 256
  - first-level zombies, 188
  - fixes, 83
  - folders, redirecting, 456
  - footprinting networks, 34
    - address ranges, 34, 36
    - application/OS version information, 40
    - expected hosts, 37-38
    - exposed applications, 39
    - host names, 37
    - patch states (of applications and hosts), 41
    - public information, 42-43
    - structure (of applications and back-end servers), 42
  - forewarning, 154
  - formatting
    - audit settings, 377
    - firewalls for small business, 451-453
    - passwords (administrators), 536-539
    - replicating, 88
    - security
      - false information about guides, 354-363
      - tools, 387-391
      - troubleshooting, 483
  - SQL Server
    - customizing authentication, 435
    - dropping stored procedures, 436-438
    - hardening, 426-427
    - securing service accounts, 427-434
    - removable media, 385
    - supportability, 416
  - FRK (file encryption key), 175
  - full IP VPNs, 203-210
  - full privilege auditing, 386
  - functionality
    - restricting browser, 402-407
    - turning off, 400-402
  - functions, LSALogonUser, 222
- G**
- Gates, Bill, 216
  - GDR (General Distribution Release), 103
  - General Distribution Release. *See* GDR

**560** INDEX

- generating passwords, 228, 529-539
- generic rights (on files), 500
- global groups, 493
- graphical user interface (GUI), 60
- gratuitous ARP replies, 271
- group passwords, 341
- Group Policy password policies, 373
- groups
  - Everyone, 505
  - restrictions, 376-377
  - security, 493
- Guel, Michael D., 121
- guessing (passwords), 326-327
- GUI (graphical user interface), 60
- guides (security)
  - applying, 362
  - false information about, 354-363
  - necessity of, 360
- H**
- hackers
  - definition of, 6
  - Warez, 47
- hacking
  - avoiding, 521
  - Eggshell Principle, 31
  - networks
    - address ranges, 34-36
    - analyzing, 72-73
    - application/OS version information, 40
    - cleaning attackers, 74-76
- detecting initial compromise of, 43-45
- elevating privileges, 46-50
- expected hosts, 37-38
- exposed applications, 39
- footprinting, 34
- hosts names, 37
- null sessions, 50-57
- patch states (of applications and hosts), 41
- public information, 42-43
- structure (of applications and back-end servers), 42
- taking over, 59-71
- target, 32
- overview of, 31
- hardening, 416
- IIS (Internet Information Services), 439-444
- SQL Servers, 426-427
  - customizing authentication, 435
  - dropping stored procedures, 436-438
  - securing service accounts, 427-434
- TCP, 375-376
- hardware
  - firewalls, 196-198
  - vulnerabilities, 249
- Hardware Compatibility List. *See* HCL
- hash value storage (LM), 368
- hashing, 306
  - LM hash, 308-313, 335-336
  - NT hash, 314-315
  - passwords, 307
  - precomputed hashing, 329
- HCL (Hardware Compatibility List), 87
- Help management, 151-152
- HFNetChk Pro, 94
- hiding systems, 357
- high security, 361-362
- hosts, 22
  - ASR (attack surface reduction), 418
  - blocking unnecessary interfaces, 420
  - disabling unnecessary features, 419
  - uninstalling unnecessary components, 418-419
  - expected, 37-38
  - exposed applications, 39
  - names, 37
  - patch states, 41
- HOSTS file, 527-528
- hotfixes, 83
- Howard, Michael, 471
- HP OpenView, 95
- HTML (Hypertext Markup Language), e-mail security, 405-407
- hubs, 270

- I**
- ICMP (Internet Control Message Protocol), 38
  - IDS accounts, 52
  - IE (Microsoft Internet Explorer), 81
  - IEEE (Institute of Electrical and Electronic Engineers), 272
  - IIS (Internet Information Services), 439-444
  - IKE (Internet Key Exchange), 287
  - implementation of security policies, 130
  - indexed administrator passwords,
    - configuring, 537
  - information disclosure attacks, 10-11, 243
  - information protection policy (IPP), 124
  - information resources (physical security), 167
  - information security, 184-189
  - infrastructure resources (physical security), 167
  - initial compromise (of networks), 43, 45
  - initiation of SSL, 231
  - injection (SQL), 45, 471-479
  - inoculation, 154
  - input
    - known (passgen tool), 530-534
    - validations (SQL), 472-474
  - installation points,
    - building slipstreamed, 102-108
  - Institute of Electrical and Electronic Engineers (IEEE), 272
  - integrity, 178, 186
  - interfaces, 22
    - ASR (attack surface reduction), 418
    - blocking unnecessary interfaces, 420
    - disabling unnecessary features, 419
    - uninstalling unnecessary components, 418-419
  - functionality (restricting), 402-407
  - GUIs, 60
  - Internet Control Message Protocol (ICMP), 38
  - Internet Information Services (IIS), 439-444
  - Internet Key Exchange (IKE), 287
  - Internet Print Provider (IPP), 439
  - Internet Protocol (IP), 203-219
  - Internet Relay Chat (IRC), 64
  - Internet Security and Acceleration (ISA) Server, 451
  - Internet use policies, 463
  - IP (Internet Protocol), 203-210
  - IPP (information protection policy), 124
  - IPP (Internet Print Provider), 439
  - IPsec (IP Security), 19
    - applying, 283-294
    - enforcement, 298
    - filters, 365, 379
    - ipseccmd.exe tool, 291
    - ipsecpol.exe tool, 291
  - IRC (Internet Relay Chat), 64
  - ISA (Internet Security and Acceleration) Server, 451
  - ISA Server 2000, 200
  - ISO Standard 17799, 120-121
  - isolation of domains,
    - applying IPsec, 294
- J-K**
- Kerberos, 284
  - keyloggers, 450
  - keys
    - IKE (Internet Key Exchange), 287
    - IPsec (IP Security), 284
    - regeneration, 279
    - uniqueness, 279
  - keystroke loggers, 332
  - known input (passgen tool), 530-534
- L**
- labeling, 125
  - LAN Manager
    - authentication, 375, 383
    - hash value storage, 368
  - laptops
    - dealing with stolen, 173-179
    - passwords, 174

**562** INDEX

- small businesses
    - applying anti-spyware/antivirus software, 450
    - configuring firewalls, 451-453
    - controlling automatic updating, 449
    - protecting, 447-448, 464-465
    - updating software, 448-449
  - laws of security, 164, 541-549
  - layers
    - ACLs (access control lists), 507-509
    - protecting, 269-271
  - least user access (LUA), 398
  - LeBlanc, David, 471
  - length, password distribution, 324
  - limiting malicious code (client security tweaks), 377-378
  - LM hash, 308-313, 335-336
  - load balancing, 99
  - local groups, 493
  - Local Security Authority (LSA) Secrets, 53, 179
  - LocalService, 222
  - LocalSystem, 222
  - locking doors, 167
  - lockout (accounts), 344, 385
  - logic of penetration tests, 24
  - logon
    - cached credentials, 315-316
    - events, 384
    - passwords, 307
  - long passwords, selection of, 338
  - lookup requests (DNS), 37
  - LSA (Local Security Authority) Secrets, 53, 179, 223
  - LSALogonUser function, 222
  - LUA (least user access), 398
- M**
- macros, turning off, 401
  - malicious code, limiting, 377-378
  - Manage Add-ons dialog box, 397
  - management
    - attachments, 408-410
    - Help, 151-152
    - passwords, 225-228, 307
    - applying, 317-325
    - attacks, 326-332
    - configuring, 536-539
    - passgen tool, 529-539
    - storage, 307-316
  - patches
    - advanced techniques, 97-100
    - as risk management, 83-84
    - AU/WSUS, 94
    - automatic updates, 94
    - building test bed, 88-90
  - definition of, 81, 83
  - EMS (enterprise management system), 95-96
  - MBSA (Microsoft Baseline Security Analyzer), 93
  - need for, 79-80
  - security update tools, 91-93
  - selection of, 96
  - slipstreaming, 101-108
  - testing security updates, 85-87
  - penetration testing, 28-31
  - rights systems, 513-517
  - risk, 113, 118-119
  - security, 135-136
    - administrator responsibilities, 18
    - receiving feedback, 14-20
    - usability, 16-18
    - vendor design tradeoffs, 19-20
  - system administration, 135-136
  - manual attacks, 7
  - masks, access, 503
  - MBSA (Microsoft Baseline Security Analyzer), 93, 454
  - meatspace, 159
  - mechanism enforcement, 297
  - memory
    - multifactor authentication, 347
    - virtual, 387

- Messenger service, 419
  - Methods, IPsec, 285-287
  - Microsoft
    - domain records, 146
    - release of source code, 11
    - Windows operating system. *See* Windows operating system
  - Microsoft Baseline Security Analyzer (MBSA), 93, 454
  - Microsoft Internet Explorer (IE), 81
  - Microsoft Security Bulletin MS04-011 (patch), 85
  - Microsoft Systems Management Server (SMS), 95
  - minimizing reboots, 97-99
  - mitigation of services, 223-228
  - models
    - Bell-LaPadula, 225
    - defense-in-depth, 20-23, 363-364
    - network threat modeling processes, 237-238
    - access restriction, 253-264
    - documentation, 238-248
    - segmentation, 248-251
    - OSI (Open Systems Interconnect), 21
  - modes, IPsec, 285, 287
  - modifying
    - administrator passwords, 538-539
    - attachments, 408-410
    - Help, 151-152
    - passwords, 225-228, 307
      - applying, 317-325
    - attacks, 326-332
    - configuring, 536-539
    - passgen tool, 529-539
    - storage, 307-316
  - patches
    - advanced techniques, 97-100
    - as risk management, 83-84
    - AU/WSUS, 94
    - automatic updates, 94
    - building test bed, 88-90
    - definition of, 81, 83
    - EMS (enterprise management system), 95-96
    - MBSA (Microsoft Baseline Security Analyzer), 93
    - need for, 79-80
    - security update tools, 91-93
    - selection of, 96
    - slipstreaming, 101-108
    - testing security updates, 85-87
  - penetration testing, 28-31
  - rights systems, 513-517
  - risk, 113, 118-119
  - security, 129, 135-136
    - administrator responsibilities, 18
    - receiving feedback, 14-20
    - usability, 16-18
    - vendor design tradeoffs, 19-20
    - system administration, 135-136
  - MSADC Sample, 417
  - MSN Bill Payer service, 216
  - multifactor authentication, 346-348
  - mutual authentication, 279
- N**
- names, hosts, 37
  - NAT (Network Address Translation), 287-288
  - navigation
    - administrator passwords, 538-539
    - attachments, 408-410
    - Help, 151-152
    - passwords, 225-228, 307
      - applying, 317-325
    - attacks, 326-332
    - configuring, 536-539
    - passgen tool, 529-539
    - storage, 307-316
  - patches
    - advanced techniques, 97-100
    - as risk management, 83-84
    - AU/WSUS, 94
    - automatic updates, 94

**564** INDEX

- building test bed, 88-90
- definition of, 81, 83
- EMS (enterprise management system), 95-96
- MBSA (Microsoft Baseline Security Analyzer), 93
- need for, 79-80
- security update tools, 91-93
- selection of, 96
- slipstreaming, 101-108
- testing security updates, 85-87
- penetration testing, 28-31
- rights systems, 513-517
- risk, 113, 118-119
- security, 129, 135-136
  - administrator responsibilities, 18
  - receiving feedback, 14-20
  - usability, 16-18
  - vendor design tradeoffs, 19-20
- system administration, 135-136
- Web sites (safely), 462, 464
- necessity of security, 360
- Netcat, 47
- netsh ipsec, 291. *See also* IPsec
- Network Address Translation (NAT), 287-288
- NetworkHideSharePasswords setting, 358
- NetworkNoDialIn setting, 358
- networks
  - attacks, 7
  - analyzing, 72-73
  - ARP (Address Resolution Protocol), 270-271
  - cached credentials, 331
  - casual attackers, 5
  - cleaning attackers, 74-76
  - cross-site scripting, 479
  - damage (types of), 10, 13
  - DDoS (Distributed DoS), 188
  - detecting, 43-45, 150
  - DoS (denial-of-service), 188, 243
  - elevation-of-privilege, 46-50, 243
  - footprinting networks, 34-43
  - null sessions, 50-57
  - passwords, 326-332
  - penetration testing. *See* penetration testing
  - reflection, 230
  - spoofing, 190-191
  - taking over, 59-71
  - target networks, 32
  - types of, 7, 9-10
- dependencies, 215-217
  - administrative security, 218-222
  - mitigating services, 223-228
  - service accounts, 222
  - types of, 229-234
- Eggshell Principle, 31
- footprinting, 34
  - address ranges, 34-36
  - application/OS version information, 40
  - expected hosts, 37-38
  - exposed applications, 39
  - host names, 37
  - patch states (of applications and hosts), 41
  - public information, 42-43
  - structure (of applications and back-end servers), 42
- hacking
  - address ranges, 34-36
  - analyzing, 72-73
  - application/OS version information, 40
  - cleaning attackers, 74-76
  - detecting initial compromise of, 43-45
  - elevating privileges, 46-50
  - expected hosts, 37-38
  - exposed applications, 39
  - footprinting, 34
  - hosts names, 37
  - null sessions, 50-57
  - patch states (of applications and hosts), 41
  - public information, 42-43

- structure (of
    - applications and back-end servers), 42
    - taking over, 59-71
    - target, 32
  - initial compromises, 43-45
  - null sessions, 50-57
  - perimeters, 32
    - border routers, 190-191
  - deperimeterization, 210-212
  - firewalls, 192-198
  - full IP VPNs, 203-210
  - objectives of
    - information security, 184-189
  - protecting, 183-184
  - remote access, 198-200
  - remote control, 201-202
  - role of networks, 189-190
  - privileges, 46-50
  - protecting, 521
  - rogue access
    - applying 802.1X, 272-282
    - enabling IPsec, 283-294
    - layer 2/3 protection, 269-271
    - preventing, 267
    - quarantine systems, 296-300
    - sniffing, 267-268
  - small businesses
    - securing WLANs (wireless LANs), 458-459
    - selecting passwords, 460
  - stacks, 159
  - targeting, 13-14, 32
  - threat modeling
    - processes, 237-238
    - access restriction, 253-255, 257, 264
    - documentation, 238-248
    - segmentation, 248-251
  - wired, 274-276
  - wireless, 277-282
  - NetworkService, 222
  - nonadministrative
    - privileges, 484
  - nondisclosure
    - agreements, 30
  - NT hash, 314-315
  - NTLMv2, 320-322
  - null sessions, 50-57
- O**
- objectives
    - of information
      - security, 184
      - availability, 187-189
      - confidentiality, 185
      - integrity, 186
    - of security, 31
  - offline storage, 456
  - one-time passwords, 348
  - one-way function (OWF), 306
  - Open Systems
    - Interconnect, 21
  - OpenHack, 19
  - operating system (OS), 22, 40
  - optimization
    - administrator passwords, 538-539
    - attachments, 408-410
    - Help, 151-152
    - passwords, 225-228, 307, 334-344
    - applying, 317-325
    - attacks, 326-332
    - configuring, 536-539
    - passgen tool, 529-539
    - storage, 307-316
  - patches
    - advanced techniques, 97-100
    - as risk management, 83-84
    - AU/WSUS, 94
    - automatic updates, 94
    - building test bed, 88-90
    - definition of, 81, 83
    - EMS (enterprise management system), 95-96
    - MBSA (Microsoft Baseline Security Analyzer), 93
    - need for, 79-80
    - security update tools, 91-93
    - selection of, 96
    - slipstreaming, 101-108
    - testing security updates, 85-87
  - penetration testing, 28-31

**566** INDEX

- rights systems, 513-517
  - risk, 113, 118-119
  - security, 129, 135-136
    - administrator
      - responsibilities, 18
    - receiving feedback, 14-20
    - usability, 16-18
    - vendor design
      - tradeoffs, 19-20
    - system administration, 135-136
  - options, authentication, 435
  - OS (operating system), 22, 40
  - OSI (Open Systems Interconnect) model, 21
  - outbound connections, preventing, 264
  - Outlook Web Access (OWA), 199
  - overflows, troubleshooting
    - buffers, 483
  - OWA (Outlook Web Access), 199
  - OWASP project (<http://www.owasp.org>), 478
  - OWF (one-way function), 306
- P**
- packet-filtering
    - firewalls, 193
  - packets
    - ACKnowledge, 38
    - sniffers, 8
  - pass phrases (password selection), 338
  - passgen (password generator) tool, 228, 529-539
  - passive administrative dependencies, 219
  - passive attacks, 7
  - passive-automated attacks, 8
  - passive-manual attacks, 8
  - password policy (PP), 122
  - passwords, 303, 305
    - authentication, 482
    - best practices, 334
      - account lockout, 344
      - disabling LM hashes, 335-336
      - protecting cached credentials, 334-335
      - selection, 337-344
    - blank, 383
    - cracking, 328-331
    - deterministic, 536
    - documentation, 341
    - group, 341
    - guessing, 326-327
    - laptops, 174
    - length distribution, 324
    - management, 225-228, 307
      - applying, 317-325
      - attacks, 326-332
      - storage, 307-316
    - multifactor authentication, 346-348
    - one-time, 348
    - overview of, 305-307
    - passgen (generating), 228
    - policies, 122, 345, 373, 382
    - selecting, 460
    - values of, 139
  - patches
    - applications, 41, 395-398
    - batching, 100
    - management
      - advanced techniques, 97-100
      - AU, WSUS, 94
      - automatic updates, 94
      - building test beds, 88-90
      - definition of, 81-83
      - EMS (enterprise management system), 95-96
      - MBSA (Microsoft Baseline Security Analyzer), 93
      - need for, 79-80
      - as risk management, 83-84
      - security update tools, 91-93
      - selection of, 96
      - slipstreaming, 101-108
      - testing security updates, 85-87
    - scanners, 91, 396
    - updates, 104
  - path maximum
    - transmission unit (PMTU), 38
  - PCs (personal computers)
    - dealing with stolen, 173-179
    - family (physical security), 180
    - protecting (physical security), 169-172



- small businesses
    - applying anti-spyware/  
antivirus software, 450
    - configuring firewalls,  
451-453
    - controlling automatic  
updating, 449
    - protecting, 447-448,  
464-465
    - updating software,  
448-449
  - PEAP (Protected EAP), 273
  - penetration testing, 23-31
  - performance
    - audit settings, 377
    - baselining, 90
    - firewalls for small  
business, 451-453
    - passwords (administrators),  
536-539
    - replicating, 88
    - security
      - false information about  
guides, 354-363
      - tools, 387-391
      - troubleshooting, 483
  - SQL Server
    - customizing
      - authentication, 435
      - dropping stored  
procedures, 436-438
      - hardening, 426-427
      - securing service  
accounts, 427-434
    - supportability, 416
  - Performance Monitor, 90
  - perimeter protection
    - policy (PPP), 123,  
126-127
  - perimeters
    - ASR (attack surface  
reduction), 418
    - blocking unnecessary  
interfaces, 420
    - disabling unnecessary  
features, 419
    - uninstalling  
unnecessary  
components, 418-419
  - borders, 190-191
  - deperimeterization,  
210-212
  - firewalls, 192-198
  - full IP VPNs, 203-210
  - functionality  
(restricting), 402-407
  - GUIs (Graphical User  
Interfaces), 60
  - networks, 32
  - objectives of information  
security, 184
    - availability, 187-189
    - confidentiality, 185
    - integrity, 186
  - protecting, 183-184
  - remote access, 198-200
  - remote control, 201-202
  - rogue access
    - applying 802.1X,  
272-282
    - enabling IPsec,  
283-294
    - layer 2/3 protection,  
269-271
    - network quarantine  
systems, 296-300
    - preventing, 267
    - sniffing, 267-268
  - role of networks,  
189-190
- permissions
  - PUBLIC, 523-524
  - tools, 512
- personal computers (PCs)
  - dealing with stolen,  
173-179
  - family (physical  
security), 180
  - protecting (physical  
security), 169-172
  - small businesses
    - applying anti-spyware/  
antivirus software, 450
    - configuring firewalls,  
451-453
    - controlling automatic  
updating, 449
    - protecting, 447-448,  
464-465
    - updating software,  
448-449
- personal identification  
number (PIN),  
168, 303
- personally identifiable  
information  
(PII), 124
- phase two (IPsec), 283
- physical security, 159-164
  - access controls, 165-168
  - client PCs, 169-172
  - family PCs, 180
  - laptops (dealing with  
stolen), 173-179
  - laws of security, 164
  - need for, 181-182
  - policies, 128
  - security tweaks, 362-363
  - USB drives, 171
- PII (personally identifiable  
information), 124

**568** INDEX

- PIN (personal identification number), 168, 303
- PKI (Public Key Infrastructure), 226
- placement of VPN servers, 206
- PMTU (path maximum transmission unit), 38
- policies
  - APP (administrator password policy), 122
  - AUP (acceptable use policies), 122
  - AVP (antivirus policy), 123
  - DTP (direct tap policy), 127
  - Internet use, 463
  - IPP (information protection policy), 124
  - passwords, 345, 373, 382
  - physical security, 128
  - PP (password policy), 122
  - PPP (perimeter protection policy), 123, 126-127
  - RAP (remote access policy), 123
  - recovery, 176
  - security
    - analyzing security needs, 118-128
    - creating awareness of, 128-129
    - developing, 114
    - enforcing, 130
    - failure of, 116
    - identifying threats, 117
    - modifying, 129
    - necessity of, 115
    - structure of, 114-115
  - software restriction, 379
  - SRPs (software restriction policies), 366-367, 420
  - SSCP (system sensitivity classification policy), 127
  - UPP (user password policy), 122
  - WNAP (wireless network access policy), 125
- porn dialers, 450
- possession, 186
- PP (password policy), 122
- PPP (perimeter protection policy), 123, 126-127
- PPTP (Point-to-Point Transfer Protocol), 36
- precomputed hashes, 329
- presared keys, 284
- preventing
  - downtime, 99
  - outbound connections, 264
  - rogue access, 267
    - applying 802.1X, 272-282
    - enabling IPsec, 283-292, 294
    - layer 2/3 protection, 269-271
    - network quarantine systems, 296-300
    - sniffing, 267-268
  - spoofing, 190-191
- privileges
  - elevating, 46-50
  - servers, 47, 457
  - services, 421-422, 426
  - troubleshooting, 484
- probability, 218
- procedures
  - dropping, 436-438
  - enforcing security policies, 130
- processes
  - cracking, 329
  - hashing, 306
  - network threat modeling, 237-238
    - access restriction, 253-257, 264
    - documentation, 238-248
    - segmentation, 248-251
    - security, 4
- profiles, roaming, 455
- proposed standard status, 204
- protected assets (quarantine systems), 297
- Protected EAP (PEAP), 273
- protecting
  - administrative accounts, 224-228
  - applications, 415-416
  - cached credentials, 334-335
  - client PCs, 169-172
  - computers
    - applying anti-spyware/antivirus software, 450
    - configuring firewalls, 451-453
    - controlling automatic updating, 449
    - for small businesses, 447-448, 464-465
    - updating software, 448-449

- data for small
    - businesses, 461-462
  - data-protection
    - mechanisms, 491-492
    - ACLs (access control lists), 493-501, 505-513
    - incorporating into applications, 517-518
    - reviewing security groups, 493
    - rights management systems, 513-517
  - networks, 521
    - securing WLANs (wireless LANs), 458-459
    - selecting passwords, 460
  - perimeters, 183-184
    - 802.1X, 272-282
    - applying firewalls, 192-198
    - availability, 187-189
    - confidentiality, 185
    - connecting border routers, 190-191
    - deperimeterization, 210-212
    - enabling IPsec, 283-294
    - full IP VPNs, 203-210
    - integrity, 186
    - layer 2/3 protection, 269-271
    - network quarantine systems, 296-300
    - objectives of information security, 184
    - preventing rogue access, 267
    - remote access, 198-200
    - remote control, 201-202
    - role of networks, 189-190
    - sniffing, 267-268
    - physical security, 166-168
    - servers
      - for small business, 454
      - for storing client information on, 455-458
    - users, 148-153
    - Web sites for small businesses, 462-464
    - Web-based services, 199
  - protocols
    - ARP (Address Resolution Protocol), 270-271
    - ICMP (Internet Control Message Protocol), 38
    - IPsec (IP Security), 19
    - NTLMv2, 320-322
    - PPTP (Point-to-Point Transfer Protocol), 36
  - proxies, circuits, 195
  - proxy server
    - dependencies, 232
  - public disclosure laws, 120
  - public information (of implementation details), 42-43
  - Public Key Infrastructure (PKI), 226
  - PUBLIC permissions, 523-524
- Q**
- QFE (Quick Fix Engineering), 103
  - quarantine systems, 296-300
  - Quick Fix Engineering. *See* QFE
  - quick mode (IPsec), 283
- R**
- RADIUS, 273
  - ranges, addresses, 34-36
  - RAP (remote access policy), 123
  - rating risk, 84
  - Real Time Communication Server (RTC), 317
  - reality check, 154
  - reboots, minimizing, 97-99
  - records
    - CDR (call detail record), 115
    - Microsoft domain, 146
  - recovering encrypted files, 176-177
  - redirecting folders, 456
  - reflection attacks, 230
  - regeneration (of keys), 279
  - registration
    - for security bulletins, 82
    - Trojans, 63
  - Reinhold, Arnold, 339
  - relative identifier (RID), 226
  - Release To Manufacturing (RTM), 103
  - remote access, 198-200. *See also* access
  - remote access policy (RAP), 123

**570** INDEX

- remote control, 201-202
  - Remote Installation
    - Services (RIS), 101
  - removable media, 385
  - removing service
    - privileges, 421-426
  - replacing encrypted files, 178
  - replicas, configuring, 88
  - replication, 416
  - replies, gratuitous
    - ARP, 271
  - reports, 23-31
  - repudiation, 243
  - requests, unsolicited
    - ARP, 271
  - resetting administrator passwords, 538
  - resistance training, 153
  - restriction
    - access, 253-257, 264
    - anonymous, 369-372, 384
    - browser functionality, 402-407
    - groups, 376-377
    - software policies, 379
    - SRPs (software restriction policies), 366-367
  - return on investment (ROI), 360
  - reviewing
    - applications, 471-474, 477-487
    - security groups, 493
  - revoking PUBLIC
    - permissions, 523-524
  - RFC 1928, 195
  - RID (relative identifier), 226
  - rights
    - on files, 500
    - management systems, 513-517
  - RIS (Remote Installation Services), 101
  - risk management, 83-84, 118-119. *See also* security policies
  - r mode (passgen tool), 534-535
  - RMS (Windows Rights Management Services), 514-515
    - components, 516-517
    - workflow, 515
  - roaming profiles, 455
  - rogue access
    - applying 802.1X, 272-282
    - enabling IPsec, 283-294
    - layer 2/3 protection, 269-271
    - network quarantine systems, 296-300
    - preventing, 267
    - sniffing, 267-268
  - ROI (return on investment), 360
  - role of networks, protecting perimeters, 189-190
  - rollup (updates), 83
  - routers
    - borders, 190-191
    - DMZ DCs, 33
  - RRAS (Windows Routing and Remote Access Services), 207, 458
  - RSA SecureID, 170, 226
  - RTC (Real Time Communication Server), 317
  - RTM (Release To Manufacturing), 103
- S**
- SafeDllSearchMode, 379-382
  - salting, 307
  - SAM (security accounts manager), 179
  - SBS (Small Business Server), 449
  - scanners
    - patches, 91, 396
    - SYN, 38
    - vulnerability, 91
  - SCE (Security Configuration Editor), 387-391
  - SCM (Services Control Manager), 418
  - screened subnets, 32
  - scripting
    - cross-site scripting, 479
    - PUBLIC permissions, 523-524
    - XSS (cross-site scripting), 45
  - SCW (Security Configuration Wizard), 354
  - SeBCAK (security between chair and keyboard), 412
  - seccedit.exe tool, 469
  - second-level zombies, 188
  - secrets, LSA, 53, 179, 223
  - SecureID, 170, 226

- security
  - 10 immutable laws of, 541-549
  - administrators, 220
  - applications
    - baselining systems, 469-470
    - evaluating, 467
    - reviewing, 471-479, 482-487
  - associations, 283
  - awareness, 149-150
  - bulletins, 82
  - client tweaks
    - anonymous
      - restrictions, 384
    - blank passwords, 383
    - enabling auditing, 384-385
    - LAN Manager
      - authentication, 383
    - limiting malicious code, 377-378
    - password policies, 382
    - removable media, 385
    - SafeDllSearchMode, 379-382
    - SMB message
      - signing, 383
  - configuration
    - false information about guides, 354-363
    - tools, 387-391
  - databases, 482
  - dependencies, 215
    - administrative security, 218-228
    - overview of, 215-217
    - service accounts, 222
    - types of, 229-234
    - UNIX, 233
  - descriptors, 495-501, 505-506
  - design
    - audit settings, 377
    - defense-in-depth model, 20-23
    - firewalls for small
      - business, 451-453
    - network threat
      - modeling processes, 237-248, 264
    - passwords (administrators), 536-539
    - replicating, 88
    - SQL Server, 426-436
    - supportability, 416
    - tradeoffs (vendors), 19-20
  - desktops
    - family (physical security), 180
    - protecting (physical security), 169-172
    - small businesses, 447-448, 464-465
  - EFS, 177-178
  - firewalls
    - applying, 192-198
    - malicious code (limiting), 378
    - small businesses, 451-453
    - types of, 193
    - Windows XP Service Pack 2, 256
  - groups, 493
  - guides
    - applying, 362
    - necessity of, 360
  - high, 361-362
  - HTML e-mail, 405, 407
  - information security, 184
  - management
    - administrator
      - responsibilities, 18
      - receiving feedback, 14-20
      - usability, 16-18
      - vendor design
        - tradeoffs, 19-20
  - MBSA (Microsoft Baseline Security Analyzer), 93
  - objectives, 31
  - passgen tool, 535
  - passwords, 303-305
    - applying, 317-325
    - attacks, 326-332
    - best practices, 334-344
    - management, 307-311, 313-316
    - multifactor
      - authentication, 346-348
    - overview of, 305-307
    - policies, 345
  - patches, 81
    - advanced techniques, 97-100
    - applications, 41, 395-398
    - batching, 100
    - AU, WSUS, 94
    - automatic updates, 94
    - building test beds, 88-90
    - definition of, 81-83
    - EMS (enterprise management system), 95-96

**572** INDEX

- MBSA (Microsoft Baseline Security Analyzer), 93
- need for, 79-80
- as risk management, 83-84
- scanners, 91, 396
- security update tools, 91-93
- selection of, 96
- slipstreaming, 101-108
- testing security updates, 85-87
- updates, 104
- penetration tests, 24-31
- physical, 159
  - access controls, 165-168
  - client PCs, 169-172
  - family PCs, 180
  - laptops (dealing with stolen), 173-179
  - laws of security, 164
  - need for, 181-182
  - policies, 128
  - security tweaks, 362-363
  - USB drives, 171
- policies
  - analyzing security needs, 118-128
  - creating awareness of, 128-129
  - developing, 114
  - enforcing, 130
  - failure of, 116
  - identifying threats, 117
  - modifying, 129
  - necessity of, 115
  - structure of, 114-115
- process, 4
- service accounts, 427-434
- small businesses, 447
  - applying anti-spyware/antivirus software, 450
  - configuring firewalls, 451, 453
  - controlling automatic updating, 449
  - data protection, 461-462
  - protecting, 447-448, 464-465
  - securing WLANs (wireless LANs), 458-459
  - selecting passwords, 460
  - servers, 454-458
  - updating software, 448-449
  - Web sites, 462-464
- stored procedures, 436-438
- tweaks, 354
  - anonymous restrictions, 369-372
  - audit settings, 377
  - avoiding, 385-386
  - defense-in-depth model, 363-364
  - IPsec filters, 365
  - LAN Manager authentication, 375
  - LM hash value storage, 368
  - necessity of, 360
  - number of settings, 357-359
  - password policies, 373
  - physical security, 362-363
  - restricted groups, 376-377
  - restricting access, 254
  - SMB message signing, 374
  - SRPs (software restriction policies), 366-367
  - stopping worms/viruses, 363
  - TCP hardening, 375-376
  - updates
    - testing, 85-87
    - tools, 91-93
  - users
    - exploits against, 140-141
    - involvement vs. influence, 142-143
    - protecting, 148-153
    - social engineering, 137, 139-148
    - value of passwords, 139
    - vulnerabilities, 155-156
  - VPN clients, 208
  - WLANs (wireless LANs), 458-459
  - security accounts manager (SAM), 179
  - security between chair and keyboard (SeBCAK), 412
  - Security Configuration Editor (SCE), 387-391

- Security Configuration Wizard (SCW), 354
- Security Guidance Center, 354
- security identifier (SID), 373
- SeDebugPrivilege, 53
- segmentation, 248-251
- selection
  - of access controls (physical security), 166-168
  - of firewalls, 192-198
  - of passwords, 323-325, 337-344, 460
  - of patch management solutions, 96
- senior management, 114. *See also* management
- servers
  - applications, 417
    - analyzing, 415-416
    - ASR (attack surface reduction), 418-420
    - removing service privileges, 421-422, 426
  - back-end, 42
  - DNS lookup requests, 37
  - enforcement, 297
  - Exchange Server Best Practices Analyzer Tool, 454
  - for small businesses
    - protecting, 454
    - storing client information on, 455-458
  - IPsec protecting, 292, 294
  - ISA (Internet Security and Acceleration) Server, 451
    - privileges, 47
    - proxy, 232
  - SBS (Small Business Server), 449
  - SQL Server
    - customizing
      - authentication, 435
      - dropping stored procedures, 436-438
      - hardening, 426-427
    - IIS (Internet Information Services), 441
      - securing service accounts, 427-434
  - VPN, 206
  - Windows Server 2003, 299-300
- service level agreement (SLA), 486
- service packs, 82-83, 94, 230
- services
  - accounts, 421
  - dependencies, 222
  - securing, 427-434
- ACS (Audit Collection Services), 458
- administrative security
  - dependencies, 223-228
- Alerter, 418
- ASR (attack surface reduction), 418
  - blocking unnecessary interfaces, 420
  - disabling unnecessary features, 419
  - uninstalling unnecessary components, 418-419
- Messenger, 419
- MSN Bill Payer, 216
- privileges, 421-422, 426
- Web-based, 199
- Services Control Manager (SCM), 418
- sessions, null, 50-57
- shares, built-in, 510
- showaccs.exe tool, 469
- SID (security identifier), 373
- SLA (service level agreement), 486
- slipstreaming, 101-108
- small business
  - computers
    - applying anti-spyware/antivirus software, 450
    - configuring firewalls, 451, 453
    - controlling automatic updating, 449
    - protecting, 447-448, 464-465
    - updating software, 448-449
  - data protection, 461-462
  - networks
    - securing WLANs (wireless LANs), 458-459
    - selecting passwords, 460

**574** INDEX

- servers
  - protecting, 454
  - storing client information on, 455-458
  - Web sites, 462-464
- Small Business Server (SBS), 449
- smart cards, 347
- SMB (Serve Message Block)
  - message signing, 230, 374, 383
  - reflection attacks, 230
- Smith, Ben, 5
- s mode (passgen tool), 535
- SMS (Microsoft Systems Management Server), 95
- sniffers, 8, 267-268
- social engineering, 137-148
- SOCKS, 195-196
- software
  - analyzing, 415-416
  - ASR (attack surface reduction), 418
  - blocking unnecessary interfaces, 420
  - disabling unnecessary features, 419
  - uninstalling unnecessary components, 418-419
  - data-protection mechanisms, 517-518
  - exposed (on hosts), 39
  - functionality
    - restricting browser, 402-407
    - turning off, 400-402
  - hiding, 357
  - LUA (least user access), 398
  - patch states, 41
  - patches, 395-398
  - security
    - baselining systems, 469-470
    - evaluating, 467
    - reviewing, 471-474, 477-487
  - servers, 417
  - services, 421-426
  - small businesses
    - applying anti-spyware/antivirus software, 450
    - configuring firewalls, 451-453
    - controlling automatic updating, 449
    - updating, 448-449
  - spyware, 411
  - structure of, 42
  - updates, 96
  - version information, 40
  - Web, 441
- software restriction policies (SRPs), 366-367, 420
- source code, release of Microsoft, 11
- spoofing, 190-191, 243
- spyware, 411
  - anti-spyware software, 450
  - blocking, 527-528
- SQL (Structured Query Language)
  - injection, 45, 471-479
  - input validations, 472-474
- Security.com (<http://www.sqlsecurity.com>), 478
- Server
  - hardening, 426-434, 436-438
  - IIS (Internet Information Services), 441
- SRPs (software restriction policies), 366-367, 420
- SSCP (system sensitivity classification policy), 127
- SSL transactions, 231
- stacks
  - with ISA Servers installed, 452
  - networks, 159
  - RRAS, 207
- starting service
  - accounts, 222
- startup keys, enabling, 179
- storage
  - client information on servers, 455-458
  - passwords, 307-316
  - stored procedures, dropping, 436-438
- strengthening
  - passwords, 339
- STRIDE, 243
- structure
  - of applications and back-end servers, 42
  - of security policies, 114-115
- substitution (of passwords), 339



- supplicants, 273
  - supportability, 416
  - SYN scans, 38
  - SYSKEY, 168
  - system administration, 135-136. *See also* administration
  - system sensitivity
    - classification policy (SSCP), 127
  - systems
    - analyzing existing, 512
    - baselining, 469-470
    - hiding, 357
    - LM hash value
      - storage, 368
    - quarantine, 296-300
    - rights management, 513-517
- T**
- tampering, 243
  - target networks, 13-14, 32
  - TCP (Transmission Control Protocol), hardening, 375-376
  - Templates, ACLs (access control lists), 353
  - temporary Internet files (TIF), 244
  - ten (10) immutable laws of security, 541-549
  - testing
    - black-box tests, 30
    - patches, 88, 90
    - penetration, 23-31
    - security updates, 85-87
  - text, troubleshooting
    - cleartext data, 484
  - theft of laptops, 173-179
  - threats
    - analyzing, 244-248
    - identifying, 117
    - network threat modeling
      - processes, 237-238
      - access restriction, 253-264
      - documentation, 238-248
      - segmentation, 248-251
  - TIF (temporary Internet files), 244
  - Tivoli, 95
  - tokens, RSA SecureID, 226
  - tools
    - Character Map, 476
    - enumeration, 92
    - Exchange Server Best Practices Analyzer Tool, 454
    - IIS Lockdown Tool, 440
    - ipseccmd.exe, 291
    - ipsecpol.exe, 291
    - Netcat, 47
    - passgen (password generator), 529-539
    - penetration testing, 28
    - Performance Monitor, 90
    - permissions, 512
    - secedit.exe, 469
    - security configuration, 387-391
    - security updates, 91-93
    - showaccs.exe, 469
    - slipstreaming, 101
    - update.exe, 100
    - wipe, 125
  - tradeoffs, vendors, 19-20
  - traffic
    - filtering, 254-257
    - ICMP, 38
    - spoofing, 190-191
  - training for users, 152-153
  - transactions
    - challenge-response, 229-234
    - SSL, 231
  - transfers, zone, 37
  - Transmission Control Protocol (TCP), hardening, 375-376
  - Transport mode (IPsec), 285
  - trees
    - fault, 245
    - threats, 244-248
  - Trojan horses, 62, 450
  - troubleshooting
    - cross-site scripting, 479
    - databases, 471-479
    - security
      - authentication, 482
      - buffer overflows, 483
      - cleartext data, 484
      - crypto algorithms, 485
      - databases, 482
      - nonadministrative privileges, 484
      - SLA (service level agreement), 486
      - unsafe settings, 483
    - tunnel mode (IPsec), 285
    - Turkish I, 471
    - turning off functionality, 400-402
  - tweaks (security), 354
    - access, 254
    - anonymous restrictions, 369-372

**576** INDEX

- audit setting, 377
  - avoiding, 385-386
  - clients
    - anonymous
      - restrictions, 384
    - blank passwords, 383
    - enabling auditing, 384-385
    - LAN Manager
      - authentication, 383
    - limiting malicious code, 377-378
    - password policies, 382
    - removable media, 385
    - SafeDllSearchMode, 379-382
    - SMB message
      - signing, 383
  - defense-in-depth model, 363-364
  - IPsec filters, 365
  - LAN Manager
    - authentication, 375
  - LM hash value
    - storage, 368
  - necessity of, 360
  - number of settings, 357-359
  - password policies, 373
  - physical security, 362-363
  - restricted groups, 376-377
  - SMB message
    - signing, 374
  - SRPs (software restriction policies), 366-367
  - stopping worms/viruses, 363
  - TCP hardening, 375-376
  - types
    - of ACLs (access control lists), 493-494
    - of attacks, 7-13
    - of dependencies, 219, 229-234
    - of exploits, 140
    - of firewalls, 193
- U**
- UMO (useless management overhead), 360
  - unbelievable software claims, 486-487
  - uninstalling unnecessary components, 418-419
  - uniqueness (of keys), 279
  - universal groups, 493
  - UNIX, dependencies, 233
  - unnecessary components, uninstalling, 418-419
  - unnecessary features, disabling, 419
  - unnecessary interfaces, blocking, 420
  - unsafe security settings, troubleshooting, 483
  - unsolicited ARP requests, 271
  - unused components (turning off functionality), 400
  - update.exe tool, 100
  - updates
    - applications, 96
    - automatic updates
      - controlling, 449
      - enabling, 449
    - rollup, 83
  - security
    - testing, 85-87
    - tools, 91, 93
  - software
    - controlling automatic updating, 449
    - for small businesses, 448-449
  - WSUS (Windows Software Update Services), 94
  - UPP (user password policy), 122
  - URL Scan (IIS), 444
  - usability of security management, 16, 18
  - USB (universal serial bus), 171
  - useless management overhead (UMO), 360
  - user password policy (UPP), 122
  - username storage, 316
  - users
    - anonymous restrictions, 369-372
    - applications
      - patches, 395-398
      - running as nonadmin, 398
    - security
      - exploits against, 140-141
      - involvement vs. influence, 142-143
      - protecting, 148-153
      - social engineering, 137-148
      - value of passwords, 139
      - vulnerabilities, 155-156

- utilities, 188
  - Character Map, 476
  - enumeration, 92
  - Exchange Server Best Practices Analyzer Tool, 454
  - IIS Lockdown Tool, 440
  - ipseccmd.exe, 291
  - ipsecpol.exe, 291
  - Netcat, 47
  - passgen (password generator), 529-539
  - penetration testing, 28
  - Performance Monitor, 90
  - permissions, 512
  - seccedit.exe, 469
  - security configuration, 387-391
  - security updates, 91-93
  - showaccs.exe, 469
  - slipstreaming, 101
  - update.exe, 100
  - wipe, 125
- V**
- values
  - of information and services, 118
  - of passwords, 139
- vendor design tradeoffs, 19-20
- verification of SQL injection, 45
- versions, applications/OS, 40
- virtual memory, clearing, 387
- virtual private network. *See* VPN
- viruses, 5
  - antivirus software, 450
  - avoiding, 13
  - stopping, 363
  - worms, 13
- VPN (virtual private network), 35
  - clients, 208
  - full IP VPNs, 203-210
  - placement of, 206
  - quarantine, 299-300
- vulnerabilities, 6, 155-156
  - automated attacks, 7
  - circumvention, 137
  - hardware, 249
  - penetration testing, 28
  - scanners, 91
  - SQL injection, 45, 474-479
  - XSS (cross-site scripting), 45
- W**
- Warez, 47
- Web access, 198-199
- Web applications, 441
- Web sites
  - cross-site scripting, 479
  - for small businesses, 462-464
- Web-based services, protecting, 199
- WF (Windows Firewall), 378
- WiFi Protected Access (WPA), 279-282
- Windows operating system, 22
- Windows Data Protection API (DPAPI), 179
- Windows Firewall (WF), 378
- Windows Management Instrumentation (WMI), 99
- Windows Rights Management Services (RMS), 514-515
  - components, 516-517
  - workflow, 515
- Windows Routing and Remote Access Services (RRAS), 458
- Windows Server 2003
  - null sessions, 55
  - VPN quarantine, 299-300
- Windows Server 2003 Service Pack 1, 230
- Windows Software Update Services, 94
- Windows Update Services (WUS), 449
- Windows Update (WU), 94
- Windows XP Service Pack 2, 94, 230, 256
- wipe tools, 125
- wired networks, applying 802.1X, 274-276
- wireless LANs (WLANs), 458-459
- wireless network access policy (WNAP), 125
- wireless networks, applying 802.1X, 277-282
- wizards, SCW (Security Configuration Wizard), 354

**578** INDEX

---

WLANs (wireless LANs),  
458-459

WMI (Windows  
Management  
Instrumentation), 99

WNAP (wireless network  
access policy), 125

workflow (RMS), 515

worms, 7, 9

- defense against, 355-356
- IPsec defending against,  
289-292
- risk management, 84
- stopping, 363
- viruses, 13

WPA (WiFi Protected  
Access), 279-282

WSUS (Windows Software  
Update Services), 94

WU (Windows Update), 94

WUS (Windows Update  
Services), 449

**X-Z**

XSS (cross-site scripting), 45

Zions, Jason, 412

zombies, 188

zone transfers, 37

