Index

Note to the Reader: Throughout this index boldfaced page numbers indicate primary discussions of a topic. *Italicized* page numbers indicate illustrations.

A
A records, 61
abandon rate (AR), 199, 301
abuse of resources, 196
accept risk strategy, 218
acceptable use policies (AUPs), 233, 244, 319–320
access
  network segmentation, 335, 335
  remote, 40–41, 41, 357–358
access control lists (ACLs), 97, 110–114, 111, 113, 457–458
access-list command, 111–113
accountability, 315
accreditation in SDLC, 373
ACKCMD tool, 135
acknowledge (ACK) flag in TCP, 56
ACLs (access control lists), 97, 110–114, 111, 113, 457–458
acquisitions, 201, 331–332
Active Directory (AD), 64
active fingerprinting, 174–175
Address Resolution Protocol (ARP), 402
  flooding and poisoning, 178
overview, 48–49
Adleman, Len, 15
administrative controls, 320
Advanced Encryption Standard (AES), 9, 12
advanced fee fraud, 286
advanced network design, 39
  remote access, 40–41, 41
SCADA, 44–45, 45
  security device placement, 41–44, 42–43
TCP/IP, 39
VoIP, 45–47, 46–47
advanced persistent threats (APTs), 314
AES (Advanced Encryption Standard), 9, 12
after-action reviews, 302–303
Agent.BTZ attack, 314
Agreed Upon Procedures document, 271
agreements, 297
  availability, 199
  business documents, 237–238
AHs (Authentication Headers), 29
AICPA (American Institute of Certified Public Accountants), 300
Ajax (Asynchronous JavaScript and XML) language, 161
ALE (annualized loss expectancy) in risk assessment, 215–216
algorithms, 5
alpha tests, 148
Alvarez, Vanessa, 85
...
ARP (Address Resolution Protocol), 402
flooding and poisoning, 178
overview, 48–49
asset value (AV) in risk assessment, 215–216
assets
  defined, 191
  identification, 210–211
  management, 133–134
asymmetric encryption, 5–6, 13–16, 13
Asynchronous JavaScript and XML (Ajax) language, 161
attachments, 206
attacker types, 295
attestation, 363
“Auditing Hash Sets: Lessons Learned from Jurassic Park” paper, 428
audits
  cloud computing, 88
  IT, 204
  managing, 336
  requirements and frequency, 247
  security, 166
  standards, 300
AUPs (acceptable use policies), 233, 244, 319–320
Aurora attacks, 289, 363
authentication, 275
  certificate-based, 361, 369–370, 369
  cloud computing, 90
  collaboration platforms, 361
  as cryptography goal, 3–4
  description, 314
  federated identity management, 365–366
  hashing, 20
  IA measures, 293
  KDC, 368
  SSO, 367–368
Authentication Headers (AHs), 29
authorization in federated identity management, 365–366
Autopsy tool, 422–425
AV (asset value) in risk assessment, 215–216
availability, 79
  description, 302
  IA measures, 293
availability agreements, 199
Avalanche tool, 301
avoid risk strategy, 218
awareness training, 245

B
Back Orifice (BO) program, 57, 348, 348
background checks, 243
BackTrack tool, 170, 270, 445–446, 448
bandwidth command, 456
Basel Accord Standard II, 331
baselines
  description, 235, 272–273
  verifying, 411–413, 412
Bastille Linux, 336
bastion servers, 128
Bell-LaPadula model, 119–120
benchmarking, 298
best practices
  risk assessments, 220–221
trends and research, 270–273, 272
Biba model, 120
Big Brother fears, 330
BIND software, 60
biometric systems, 276–277
bit-level copies, 253
BitLocker tool, 3, 363
blabla tool, 134
black box tests, 148, 167–168, 333
black hat hackers, 295
black hat search engine optimization, 288
blacklist spam filters, 128
block ciphers, 5, 7, 7
Blockbuster, 201
Blowfish algorithm, 9
BO (Back Orifice) program, 57, 348, 348
BO2K tool, 57
boot record infectors, 125
BootRoot rootkit, 433–437, 435–437
Boson NetSim emulation software, 449
botnets, 287–288, 287
bots, 123
bottom-up testing, 149
BoundsChecker tool, 301
Bowes, Ron, 431
BP oil spill, 195
BPAs (business partnership security agreements), 238
brainstorming, 303, 322
breaches
  cost, 375–376
  data, 242–243, 248
  defined, 192
Brewer and Nash model, 120
bridges in X.509, 24
broken agreements, 200
brute-force password cracking, 179
BT5R1 tool, 445–446, 448
buffer overflows, 162–163, 162, 284
building layouts, 66–67
Burp Proxy tool, 151, 152
business documents, 237–239
business models, risk in, 195–197
business partnership security agreements (BPAs), 238
business tools, 290–292
butt dialing, 350
byte substitution, 12
C

C&C (command and control) servers, 63–64, 123
Caesar, Julius, 2
Caesar cipher, 2, 6
Cain and Abel tool
description, 180, 267, 268
password decoding, 160, 430
VoIP capture, 46, 49, 354, 355
web conferencing, 346
CAL9000 tool, 267
California Senate Bill 1386, 242
caller ID spoofing, 286
caller services, 199
Cameras, 363–364
CanSecWest convention, 294
CANVAS tool, 181
capability in performance, 302
Captain Crunch, 296
Capture Filters tool, 406
Capture the Flag competitions, 294
cardholder data protection, 236
Carlisle Adams/Stafford Tavares (CAST) cipher, 9
CAs (certificate authorities), 22–23
CASE (computer-aided software engineering) tool, 336–337
CAST (Carlisle Adams/Stafford Tavares) cipher, 9
CBC (cipher block chaining) mode, 10–11
CC (Common Criteria), 118, 280, 377–378
cell phones
butt dialing, 350
SMiShing, 288
central monitoring IDS systems, 136
CER (Crossover Error Rate), 276
Cerf, Vinton, 47
certificate authorities (CAs), 22–23, 23
certificate revocation lists (CRLs), 23–24
certificates
authentication, 361, 369–370, 369
digital, 24–26, 25
distribution, 26
Nessus, 409
certification in SDLC, 373
Certified Information Systems Auditor (CISA), 293
Certified Information Systems Security Professional (CISSP), 293
CFB (cipher feedback) mode, 10–11
chain of custody, 85, 251
Challenge Handshake Authentication Protocol (CHAP), 29, 40, 41, 358
change and change management
interorganizational. See interorganizational change
technology life cycle, 372–373
Chaos Communication Congress conference, 294
CHAP (Challenge Handshake Authentication Protocol), 29, 40, 41, 358
checksums, 389–390
China, IPv6 in, 52
Chrysler merger, 201
CIA (confidentiality, integrity, and availability), 211, 314, 314
cipher block chaining (CBC) mode, 10–11
cipher feedback (CFB) mode, 10–11
cipher text, 4–5
ciphers
block, 7, 7
stream, 8
transposition, 7
Circuit City, 201
CIS (Computer Information Systems) benchmarks, 129
CISA (Certified Information Systems Auditor), 293
Cisco Fatty incident, 291
Cisco Skinny protocol, 355
Cisco type 7 passwords, 160
CISSP (Certified Information Systems Security Professional), 293
Clark-Wilson model, 120
classification
cloud data, 88
information, 212–213
clear text, 4
clickjacking, 151, 289
clients
anti-spyware software, 127
attacks, 282–285, 282
Kerberos, 65
PKI, 26–27
spam filters, 128
clock rate command, 456
cloud computing, 81–82
benefits, 83–86
e-mail, 88
errors in, 89
exam essentials, 103–104
large file transfer services, 91
models, 82–83, 82
providers, 83
review questions, 105–108
risks, 89–90, 207, 208
security, 86–90
services, 86
summary, 103
vulnerabilities, 90–91
CNAME records, 61
CNGI infrastructure, 52
COBIT (Control Objectives for Information and Related Technology) guidelines, 129, 300
code
reviews, 149–150, 169
signing, 18–19
standards, 156–157
Code red malware, 124
Cohen, Fred, 124
collaboration
and communication. See communication and collaboration
teams, 322–324, 325
collisions in hashing, 17
command and control (C&C) servers, 63–64, 123
command shell for bypassing restrictions, 132
commercial information classification, 212–213
commercial off-the-shelf (COTS) software, 332–334
Committee for Sponsoring Organizations of the Treadway Commission (COSO), 331
Committee on National Security Systems Instruction CNSSI-4009, 293
Common Criteria (CC), 118, 280, 377–378
Common Object Request Broker Architecture (CORBA), 70
Common Vulnerabilities and Exposures (CVEs) list, 193
communication and collaboration, 343–345
certificate-based authentication, 369–370, 369
exam essentials, 378–379
external communications, 359–360, 360
federated identity management, 365–366
mobile devices, 358–359, 363–365
platforms implementation, 360–361
prioritizing traffic, 362
remote access, 357–358
review questions, 380–383
secure solutions, 60–66
SOAP, 366–367, 367
SPML, 368
SSO, 367–368
summary, 378
technology life cycle. See technology life cycle
unified communication security, 345–353, 348–349
VoIP security, 354–357, 355
XACML, 366
compliance, 202, 330
comprehensive security solutions, 37–39
advanced network design. See advanced network design
exam essentials, 71–72
review questions, 73–76
secure communication solutions, 60–66
secure facility solutions, 66–67
secure infrastructure design, 67–70
summary, 70–71
computer-aided software engineering (CASE) tool, 336–337
counter zero day attacks, 289
CPUs
thread information, 417
usage, 452–453, 452–453
Crack program, 351
Crackers, 295
cracking
encrypted files, 429–431, 429–430
passwords, 179–180, 277, 429–431, 429–430
tools, 179–180
cramming, 333
credit cards
protecting, 236
skimmers, 241
crimeware kits, 288–289
CRLs (certificate revocation lists), 23–24
cross-site request forgery (XSRF or CSRF) attacks, 120
client-side attacks, 283
description, 150
HTTP, 59
JavaScript vulnerabilities, 161
cross-site scripting (XSS) attacks
    client-side attacks, 283–284
    HTTP, 59
    JavaScript vulnerabilities, 161
    overview, 150
    WAFs for, 43
Crossover Error Rate (CER), 276
cryptanalysis, 4, 30
cryptographic keys, 5
cryptographic tools and techniques, 1–2
    application layer encryption, 27–28
    asymmetric encryption, 13–16
    attacks, 30
    benefits, 283
    block ciphers, 7, 7
    defined, 4
    digital signatures, 20–22, 21
    exam essentials, 31–32
    goals, 3–6
    hashing, 17–20, 18
    history, 2–3
    hybrid encryption, 16–17, 17
    Internet layer controls, 28–29
    lab manual, 428
    mobile devices, 363
    physical layer controls, 29
    plug-ins, 289
    public key infrastructure, 22–27, 23, 25
    review questions, 33–36
    stream ciphers, 8
    summary, 31
    symmetric encryption, 8–13, 8
    transport layer encryption, 28
    VoIP traffic, 355
    weak, 160
CSIRT (computer security incident response team), 248
CSLAs (customer service-level agreements), 298
CSRF (cross-site request forgery) attacks, 120
    client-side attacks, 283
    description, 150
    HTTP, 59
    JavaScript vulnerabilities, 161
    cultural fit in partnerships, 200
    custom development, 333–334
    customer service-level agreements (CSLAs), 298
    CVEs (Common Vulnerabilities and Exposures) list, 193
    cyber criminals, 295–296
    cyber defense aids, 299
    cyber laws and crimes, 202
    cyber terrorists, 296
    cybercrime, 296
    cyberterrorism, 192

D

Daemen, Joan, 12
Daimler merger, 201
DAM (database activity monitoring) systems, 65
Damn Vulnerable Linus (DVL) application, 269
DARPA (Defense Advanced Research Projects Agency), 248
DAS (direct access storage), 101
data breaches, 242–243, 248
data de-duplication, 102
data diddling, 122
Data Encryption Standard (DES), 9–11
data exfiltration, 134–135
data extraction in cloud computing, 90
data handling in incident response, 250
data owners, 237
data remanence, 89, 372
data retention policies, 237
data risks, 204
data at rest, 204–205
data in transit, 205–206
    EDI, 206–207
    network boundaries, 207, 208
    personal devices, 207–209
data activity monitoring (DAM) systems, 65
data base administrators, 326
data base components in IDS systems, 136
DDoS (distributed denial-of-service) attacks
    bots, 123
    description, 192, 286
    DNS, 60
    and DNSSEC, 63
de-mergers, 331–332
decentralized access control, 358
decommissioning in technology life cycle, 372
deconstructing existing solutions, 301
DefCon conference, 294, 295
Defense Advanced Research Projects Agency (DARPA), 248
defense in depth, 39
    firewall design, 43, 43
    host-based firewalls, 114, 115
    spam, 128
Delphi technique, 217
demilitarized zones (DMZs), 42, 43
denial of service (DoS) attacks
    assessment area, 168
    bots, 123
    cloud computing, 90
    description, 286
    DNS, 60
    resource exhaustion, 164–165
    testing, 168
    VoIP, 355–356
deny all clause, 111
deny icmp command, 457
Department of Defense (DoD) Directive 8570, 293
Department of Defense (DoD) TCP/IP four-layer model, 48, 48
Department of Homeland Security (DHS), 273
DES (Data Encryption Standard), 9–11
Description Protocol layer in SOAP, 367
desktop sharing, 348–350
detection
anomalies, 136, 273–274
data breaches, 242
rootkit, 437–440, 438–440
development/acquisition phase in SDLC, 373, 374
DHS (Department of Homeland Security), 273
diagramming tools, 269
DIAMETER standard, 40, 357–358
dictionary password attacks, 179
differentiated services (DiffServ), 362
Diffie, W., 14
Diffie-Hellman protocol, 14–15
diffusion method in block ciphers, 7
digital certificates in PKI, 24–26, 25
digital forensics, 250–254, 252
Digital Signature Standard, 22
digital signatures, 4, 15, 20–22, 21
direct access storage (DAS), 101
Directors Desk Product, 361
disaster recovery and business continuity plan (DR/BCP), 89
disciplines, 325–328, 325
disclosure of information, 197
Discovery Protocol layer in SOAP, 367
discrete logarithms, 14
disgruntled employees, 296
disposal phase in SDLC, 373, 374
distributed denial-of-service (DDoS) attack bots, 123
description, 192, 286
DNS, 60
and DNSSEC, 63
dlls (dynamic link libraries), 419
dmalloc tool, 301
DMVPNs (dynamic multipoint VPNs), 335
DMZs (demilitarized zones), 42, 43
DNS (Domain Name Service), 60–66
DNSSEC (DNS Security Extensions), 62–63
documentation
auditing, 247
business documents, 237–239
digital forensics, 250–254, 252
exam Essentials, 256–257
high-level view, 231–232
incident response framework, 248–250
policies and procedures, 233–237, 234
policy development process, 232–233, 232
retention time, 251
review questions, 258–261
sensitive information. See sensitive information summary, 255–256
training and employee awareness, 254–255
DoD (Department of Defense) Directive 8570, 293
DoD (Department of Defense) TCP/IP four-layer model, 48, 48
domain kiting, 60
Domain Name Service (DNS), 60–66
DoS attacks. See denial of service (DoS) attacks
double flux, 63
double tagging, 97–98
DPT (Dynamic Trunking Protocol), 69
Dr. Solomon’s Antivirus Toolkit, 124
DR/BCP (disaster recovery and business continuity plan), 89
Draper, John, 296
Drop.io service, 100
DropBox service, 87, 100
dsniff package, 59
dual control, 245
dual-homed gateways, 42
dual-use keys in symmetric encryption, 8
due diligence, 85, 89, 270, 296, 332
DVl (Damn Vulnerable Linus) application, 269
dynamic link libraries (DLLs), 419
dynamic multipoint VPNs (DMVPN), 335
dynamic ports, 173
dynamic program analysis, 301
Dynamic Trunking Protocol (DPT), 69
discovery (e-discovery), 251
EA (Enterprise Architecture), 220
earthquakes, 196
eavesdropping at web conferences, 346
ebXML (Electronic Business using Extensible Markup Language), 366
ECB (Electronic codebook mode), 10–11
ECC (elliptic curve cryptography), 16
dynamic link libraries (DLLs), 419
EDI (Electronic Data Interchange), 206–207
education verification, 243
eEye Retina scanner, 269
EF (exposure factor) in risk assessment, 215–216
effectiveness analysis, 299–300
eFS (encrypted file system), 204
eFuzz tool, 180
EICAR (European Institute for Computer Anti-virus Research) test, 125
El Gamal algorithm, 16
Electronic Business using Extensible Markup Language (ebXML), 366
Electronic codebook (ECB) mode, 10–11
Electronic Data Interchange (EDI), 206–207
electronic discovery (e-discovery), 251
elliptic curve cryptography (ECC), 16
email, 351–352
attachments, 206
cloud computing, 88
sniffling, 352
embezzlement, 197
emergency response, 254
emergency response teams, 327
emergent issues
sources, 295–296
technology life cycle, 375–376
trends, 287–289, 287
employees dealing with, 318–319
disgruntled, 296
policies, 243–247
training, 244–245, 254–255
employers, social network searches by, 291
employment policies, 244–246
enable password command, 160
enable secret command, 160
Encapsulated Secure Payload (ESP), 28
capsulation ppp command, 455
Encase tool, 270
encrypted file system (EFS), 204
encrypted files, cracking, 429–431
encryption. See cryptographic tools and techniques
end of employment policies, 246–247
end-to-end solution ownership, 370–371
endpoint-based NACs, 274
endpoint security software, 121–123
Enterprise Architecture (EA), 220
enterprise security
mobile devices configuration management, 358–359
overview, 79–81, 80
Enterprise Security Architecture (ESA) frameworks, 220
enterprise security integration, 311–313
disciplines, 325–328, 325
exam essentials, 338
governance, 315–317, 316
interorganizational change. See interorganizational change management guidance, 320–322, 321
purpose, 313–315, 314–315
review questions, 339–341
summary, 337–338
team collaboration, 322–324, 325
Enterprise Service Bus (ESB), 69
enterprise storage
exam essentials, 103–104
online, 100–101
overview, 98–102, 98, 100
review questions, 105–108
summary, 103
entropy, 5
Entrust CAs, 22
equipment settings, 196
ESA (Enterprise Security Architecture) frameworks, 220
ESB (Enterprise Service Bus), 69
escalation of privilege, 96, 158, 158
ESP (Encapsulated Secure Payload), 28
ethical hackers, 295, 300
Ettercap tool, 346
European Institute for Computer Anti-virus Research (EICAR) test, 125
evaluating controls, 322
evaluation step for data breaches, 242

events
in incident response, 250
managing, 336
exercises. See lab manual
exfiltration of data, 134–135
exploits
application, 157–158
frameworks, 181
exposure factor (EF) in risk assessment, 215–216
Extended Terminal Access Controller Access Control System (XTACACS), 40
Extensible Access Control Markup Language (XACML), 361, 366
Extensible Markup Language (XML) messages, 70
external communications, 359–360, 360
external influences in risk, 201–204

F
Facebook, 290–292, 292
Facilitated Risk Assessment Process (FRAP) process, 217
facilities management, 67
facilities managers, 327
fact gathering, 303
FACTA (Fair and Accurate Credit Transaction Act), 331
failure mode, effects, and criticality analysis (FMECA), 217
failure modes and effects analysis (FMEA), 217
Fair and Accurate Credit Transaction Act (FACTA), 331
false injection tools, 180–181
Farmer, Dan, 170, 266
FarmVille, 84
FASB (Financial Accounting Standards Board), 300
fast flux DNS, 63–64
fast infection viruses, 126
FBI (Federal Bureau of Investigation) estimates, 281
FCIV (File Checksum Integrity Verifier), 389–390
FCoE (Fiber Channel over Ethernet), 102
FCR (first call resolution), 199, 301
Federal Bureau of Investigation (FBI) estimates, 281
Federal Information Security Management Act (FISMA), 203, 271, 298, 300
federated access control, 335, 335
Federated IDs, 65, 365–366
Fedora Linux Security Spin tool, 269
Fiber Channel over Ethernet (FCoE), 102
File Checksum Integrity Verifier (FCIV), 389–390
file encryption, 428
File Transfer Protocol (FTP) attacks, 58–59
risks, 206
FileMon tool, 418, 421
filetype command, 171
filters
   packet, 42, 42
   spam, 128–129, 129
FIN (finish) flag in TCP, 56
final acceptance testing, 157
Financial Accounting Standards Board (FASB), 300
financial administration, 326
financial records, testing, 172
Fingerprinting Organizations with Collected Archives (FOCA) tool, 173
fingerprints
   scan systems, 276
   spam filters, 128
tools, 174–175
finish (FIN) flag in TCP, 56
fires, 196
Firesheep tool, 152, 282–283
firewalls
   access control lists, 110–114, 111, 113
   host-based, 114–117, 115
   overview, 42–43, 42
   placement, 42
firmware vulnerabilities, 192
first call resolution (FCR), 199, 301
FISMA (Federal Information Security Management Act), 203, 271, 298, 300
flags in TCP, 56
Flash-based vulnerabilities, 151
Flawfinder tool, 169, 176
flood risks, 195–196
flooding, ARP, 178
FMEA (failure modes and effects analysis), 217
FMECA (failure mode, effects, and criticality analysis), 217
FOCA (Fingerprinting Organizations with Collected Archives) tool, 173
footprinting tools, 171–173
forensic audits, 247
Forensic Tool Kit (FTK), 270
forensics
   computer, 270
digital, 250–254, 252
   Helix, 421–425
   lab manual, 413–421, 414–419, 421
Foundstone tool, 440
Foursquare network, 291
FQDNs (fully qualified domain names), 60
fragmentation handling, 175
FRAP (Facilitated Risk Assessment Process) process, 217
fraud, advanced fee, 286
FTK (Forensic Tool Kit), 270
FTP (File Transfer Protocol) attacks, 58–59
   risks, 206
   fully qualified domain names (FQDNs), 60
function tests, 148, 333
fuzzing testing technique, 180–181

G
GAO Federal Information System Controls Audit Manual, 320
Generally Accepted Accounting Principles (GAAP), 300
Ghost Rat Trojan, 122, 347
GhostNet, 296, 314
GLBA (Gramm-Leach-Bliley Act), 202–203
global information assurance community, 293–296, 295
globally unique identifiers (GUIDs), 64
Gmail, 88
GMER rootkit detector, 437–438
GNS3 emulation software, 449
GnuPGP standard, 28
goals, cryptographic, 3–4
Gonzales, Albert, 296
Google
   attacks on, 289
   commands, 171
Google Hacking Diggity Project, 171
Google Maps, 161
governance in enterprise security integration, 315–317, 316
governmental information classification, 212
GPUs for password cracking, 180
Gramm-Leach-Bliley Act (GLBA), 202–203
grey box testing, 168
grey hat hackers, 295
Group Policy, 131
/GS compile-time flag, 284
GtkHash tool, 425
guidelines, 235, 272
GUIDs (globally unique identifiers), 64
Gutierrez, Carlos, 4

H
Hack In The Box conference, 294
HackCon convention, 294
hackers
   attacks, 192
   conferences, 293–294
   types, 295–296, 376
Hacme Bank application, 269
hactivists, 296, 297
hand geometry systems, 276
handbooks, employee, 244
Handle tool, 418
hard changeovers, 337
hardening
  hosts, 129–133
  platforms, 336
hardware-based NACs, 274
hardware-based phones, 357
hardware-based VPNs, 360
hardware requirements for lab manual, 386–387
Hardware Security Module (HSM), 204–205
hashed message authentication code (HMAC), 20
hashing, 17
defined, 5
HAVAL algorithm, 19
HMAC, 20
lab manual, 425–428, 426–427
MD algorithms, 19
message authentication code, 20
and message digests, 17–19, 18
Secure Hash Algorithm, 19
HAVAL algorithm, 19
HBA (Host Bus Adapter) allocation, 102
Health Insurance Portability and Accountability Act (HIPAA), 202, 240, 331
Health Net, Inc. report, 240
Helix tool, 254, 421–425
Hellman, M. E., 14
help desk, 199
heuristic-based antivirus programs, 125
hidden costs in partnerships, 200
HIDSs (host-based intrusion detection systems), 137–138, 138, 273
hierarchical trust model, 22, 23
high risk category, 217
hijacking, session, 286
HIPAA (Health Insurance Portability and Accountability Act), 202, 240, 331
HIPS (Host-Based Intrusion Prevention System), 138
HMAC (hashed message authentication code), 20
home user best practices, 272
hopping, VLAN, 69, 97
horizontal privilege escalation, 158, 158
host-based firewalls, 114–117, 115
host-based intrusion detection systems (HIDSs), 137–138, 138, 273
Host-Based Intrusion Prevention System (HIPS), 138
Host Bus Adapter (HBA) allocation, 102
host security, 109–110
  anti-malware, 124–129, 129
  asset management, 133–134
  data exfiltration, 134–135
  endpoint, 121–123
  exam essentials, 139–140
  firewalls, 110–117, 111, 113, 115
  hardening, 129–133
  IDP, 135–138, 137–138
  review questions, 141–144
summary, 139
trusted operating systems, 117–120
Hostess lawsuit, 244
hostname command, 113, 454
hosts, screened, 42
Hping tool, 267
HSM (Hardware Security Module), 204–205
HTTP (Hypertext Transfer Protocol) interceptors, 181
overview, 59
risks, 206
SAML assertions, 366
HTTPS Everywhere, 283
human resources department description, 327
termination process, 246–247
hurricanes, 196
HushMail program, 28
hybrid architecture, 82
hybrid encryption, 16–17, 17
hybrid password cracking, 179
Hypertext Transfer Protocol (HTTP) interceptors, 181
overview, 59
risks, 206
SAML assertions, 366
hypervisors, 93–96, 94–95

I
I Love You malware, 124
IA (information assurance) community, 293–296, 295
IaaS (infrastructure-as-a-service) cloud model, 82
IAB (Internet Architecture Board), 278
IAX2 protocol, 355
IBM, Microsoft partnership, 200
IC3 (Internet Crime Complaint Center) report, 299
IceSword application, 440
ICMP. See Internet Control Message Protocol (ICMP)
ICV (integrity check value), 29
IDA Pro tool, 301
IDC (International Data Corporation), 84
IDEA (International Data Encryption Algorithm) cipher, 9, 12
Identify and Acquire step in digital forensics, 253
IDP (intrusion detection and prevention) systems
  lab manual, 431–433, 432–433
  overview, 135–138, 137–138, 273–274
  purpose, 336
IESG (Internet Engineering Steering Group), 278
IETF (Internet Engineering Task Force), 278
ifconfig command, 393–394, 401
IKE (Internet Key Exchange) component, 15
Ikee exploit, 363
ILM (information lifecycle management), 236
IM (instant messaging), 347–348
IMAP (Internet Message Access Protocol), 352
implementation phase in SDLC, 373, 374
implicit denies, 458
incident response framework, 248–250
incremental attacks, 122
independent reviews, 317
industries, interconnecting, 330–331
information
  classification, 212–213
  security breaches, 242
  security policies, 319
  system audits, 247
information assurance (IA) community, 293–296
information-centric approach, 121
information lifecycle management (ILM), 236
Information Technology Security Evaluation Criteria (ITSEC), 118
information-centric policies, 233
INFOSEC Assessment Methodology, 217
infrastructure-as-a-service (IaaS) cloud model, 330–331
infrastructure-based NACs, 274
infrastructure design, 67–70
  Enterprise Service Bus, 69
  router configuration, 68–69
  Web Services Security, 70
inheritance of threads, 417
initial employee training, 244
Initial Sequence Number (ISN) sampling, 175
initialization vectors (IVs), 6
initiation phase in SDLC, 373, 374
input validation, 152
insider attacks, 196
instant messaging (IM), 347–348
intangible assets, 210
integer overflow, 163, 164
Integrated Services (IntServ), 362
integration
  within business, 291–292
enterprise security. See enterprise security integration
  products and services, 336–337
integrity, 79
  as a cryptography goal, 3–4
  hashing, 18
  IA measures, 293
  integrity check value (ICV), 29
interceptors, HTTP, 181
interconnecting multiple industries, 330–331
interconnection security agreements (ISAs), 237
interdependencies, coding, 157
interfaces
  restricted, 133
  router, 454
internal influences in risks, 201–204
International Data Corporation (IDC), 84
International Data Encryption Algorithm (IDEA) cipher, 9, 12
International Organization of Standards (ISO), 280
International Organization on Computer Evidence, 252
Internet Architecture Board (IAB), 278
Internet Control Message Protocol (ICMP), 47
ACLs, 112
overview, 53–54
ping packets, 173
Smurf attacks, 165
traffic, 402
Internet Crime Complaint Center (IC3) report, 299
Internet Engineering Steering Group (IESG), 278
Internet Engineering Task Force (IETF), 278
Internet Key Exchange (IKE) component, 15
Internet layer controls, 28–29
Internet layer protocols, 50–55, 50–52
Internet Message Access Protocol (IMAP), 352
Internet Protocol (IP), 47
Internet Protocol version 4 (IPv4), 50–53, 50–51
Internet Protocol version 6 (IPv6), 52–55, 52
Internet Research Steering Group (IRSG), 278
Internet Research Task Force (IRTF), 278
Internet Small Computer System Interface (iSCSI), 102
Internet Society (ISOC), 278
interorganizational change, 328–330, 330
integration of products and services, 336–337
interconnecting multiple industries, 330–331
mergers, acquisitions, and de-mergers, 331–332
network segmentation and delegation, 334–336, 335
third-party products, 332–334
intitle command, 171
intrusion detection and prevention (IDP) systems
  lab manual, 431–433, 432–433
  overview, 135–138, 137–138, 273–274
purpose, 336
IntServ (Integrated Services), 362
Invocation property, 120
Iodine tool, 135
IP (Internet Protocol), 47
ip access-group command, 458
ip access-list command, 457
ip address command, 455
IP addressing in NETinVM, 394
IP-based mobile devices, 363–364
IP DF option, 175
IP Stack Integrity & Stability Checker (ISIC), 181
IP TOS option, 175
IP traffic ACLs, 112
IP TTL value, 174
iPads, 208
ipconfig command, 401
iPhones, 288
IPID sampling, 175
IPSec protocol, 28, 360
IPtables firewall, 115–117
IPv4 (Internet Protocol version 4), 50–53, 50–51
IPv6 (Internet Protocol version 6), 52–55, 52
iris recognition, 276
IRSG (Internet Research Steering Group), 278
IRTF (Internet Research Task Force), 278
IS security steering committee, 326
ISACA (IT Governance Institute), 300
ISAs (interconnection security agreements), 237
iSCSI (Internet Small Computer System Interface), 102
ISIC (IP Stack Integrity & Stability Checker), 181
ISN (Initial Sequence Number) sampling, 175
ISO (International Organization of Standards), 280
ISO 15408 standard, 280
ISO 20000 standard, 328
ISO 27702 standard, 280–281
ISOC (Internet Society), 278
issuance to entities for certificates, 25
IT audits, 204
IT Governance Institute, 204, 300
ITSEC (Information Technology Security Evaluation Criteria), 118
IVs (initialization vectors), 6

J
jailbreaking phones, 363
Japan, IPv6 in, 52
JavaScript language, 161–162
jitter, 357
job descriptions, 326
job rotation, 245
job search sites, 172
job titles, 328
John the Ripper program, 180, 267
Jotti.org, 433–435

K
Kahn, Robert, 47
Kerberos, 65, 367
key distribution centers (KDCs), 65, 367–368
keyboard dynamics, 276
keyloggers, 122–123
keys
asymmetric encryption, 13–14, 13
cryptographic, 5
hybrid encryption, 16–17, 17
PKI, 26
symmetric encryption, 8–9, 8
Kismet tool, 181, 267
Kornblum, Jesse, 428

L
L0phtcrack tool, 180, 429–430
L2F (Layer 2 Forwarding), 359
L2TP (Layer 2 Tunneling Protocol), 29, 41, 360
lab manual, 386
baseline security configuration, 411–413, 412
cracking encrypted files, 429–431, 429–430
file encryption, 428
forensic tools, 413–421, 414–419, 421
further exploration, 460–461
hashing, 425–428, 426–427
Helix tool, 421–425
intrusion detection, 431–433, 432–433
Metasploit Framework, 442–445, 442–444
Nessus Vulnerability Scanner, 408–411, 409–410
port scanners, 396–400, 398
protocol analyzers, 400–406, 402, 404
requirements, 386–387
rootkit detection, 437–440, 438–440
routing, switching, and security, 449–459, 450–459
signature-based scanning, 433–437, 435–437
social engineering, 445–449, 446–448
summary, 387–389
threat modeling, 440–441
virtual environments, 389–392, 391–392
virtual networks, 392–396, 393–396
web vulnerabilities, 406–408, 407
land attacks, 165
LANGuard tool, 177, 269
laptops, 363–364
large file transfer services in cloud computing, 91
 latency, 301, 357
Layer 2 Forwarding (L2F), 359
Layer 2 Tunneling Protocol (L2TP), 29, 41, 360
layered access control, 335, 335
layouts, building, 66–67
LDAP (Lightweight Directory Access Protocol), 64, 358, 368
LDAP over SSL (LDAPS), 64
Lessons Learned
enterprise reviews, 302–303
incident response, 249
libpcap, 304
libraries
DLL, 419
standard, 155–156
libtiff exploit, 363
Lightweight Directory Access Protocol (LDAP), 64, 358, 368
linear mix transform, 12
LinkFerret tool, 181
links, recommended, 460–461
Linux platforms
hardening, 336
tools, 269
ListDLLs tool, 419, 419
Local Security Authority (LSA) component, 351
location redundancy, 102
lock picking, 294
logic bombs, 287
logical deployment diagrams, 68
logs, 361
LOKI tool, 135
loss of competency, 199
lost phones, 363
Low Orbit Ion Cannon (LOIC)
cloud computing, 90
DDoS attacks, 192
flood guards, 165
low risk category, 216
LSA (Local Security Authority) component, 351
LulZSec Twitter page, 296, 297
LUN masking, 102
Mean Time Between Failure (MTBF), 302
Mean Time To Restore (MTTR), 302
Mebroot rootkit, 57, 435
MediaFire service, 100
MediaMax service, 89
medium risk category, 216
Melissa malware, 124
memoranda of understanding (MOU), 238
memory leaks, 163
Men & Mice website, 61
mergers, 201, 331–332
Merkle-Hellman Knapsack algorithm, 16
meshes in X.509, 24
message authentication code (MAC), 20
message digests and hashing, 17–19, 18
Messaging Protocol layer in SOAP, 367
metadata, 173
Metasploit Framework, 181
description, 267
lab manual, 442–445, 442–444
Microsoft, IBM partnership, 200
Microsoft Baseline Security Analyzer (MBSA), 129, 411–413, 412
Microsoft Loopback Adapter, 401
Microsoft Sysinternals Suite. See Sysinternals tools
Microsoft Windows tools, 269
MIME in SAML assertions, 366
minimization
data breaches, 242
downtime, 250
mitigate risk strategy, 218
mitigation and response for data breaches, 242
MiTM attacks. See man-in-the-middle (MiTM) attacks
mix column, 12
mobile code, sandboxing, 154
mobile devices, 205–206, 363
e enterprise configuration management, 358–359
IP-based, 363–364
VPNs, 206
modified Delphi technique, 317
ModSecurity WAF, 116
modules, coding, 157
money laundering schemes, 286
money mules, 288
monitoring-as-a-service (MaaS) cloud model, 82
monitoring risk, 219–220
Morris worm, 248
MOU (memoranda of understanding), 238
MRI (magnetic resonance imaging)
radiologists, 197
MTBF (Mean Time Between Failure), 302
MTTR (Mean Time To Restore), 302
Mudge, 41
multipartite infectors, 125
multipath solutions, 102
multiple industries, interconnecting, 330–331
multitier network data design, 67–68
Murdoch, Rupert, 376
MX records, 61
N

NAC (network access control), 274
Nagios tool, 275
name servers, 61
NAS (network attached storage), 101
NAT (network address translation), 51
nation-state hackers, 296
National Institute of Standards and Technology (NIST) best practices, 271
change management, 328
continuous monitoring, 219–220
control categories, 321
and DES, 9–12
IDPs, 138, 274
National Vulnerability Database website, 65, 267
OpenSSH vulnerabilities, 400
Risk Assessment guidelines, 272
SCAP, 269
SDLC, 154–155, 373
standards, 271–272
system design validation, 376
system hardening, 129
National Security Agency (NSA), 129
National Strategy for Trusted Identities in Cyberspace (NSTIC), 277
National Vulnerability Database (NVD), 267, 284
native remote applications, 134
natural disasters, 191, 195–196
NetBus program, 348
NDAs (nondisclosure agreements), 238, 243–244
neighbor command, 454
Neighbor Discovery Protocol (NDP), 49, 52
Nessus HomeFeed dialog box, 409
Nessus Server Manager, 409
Nessus Vulnerability Scanner, 131, 269
descriptor, 267
lab manual, 408–411, 409–410
overview, 411
NetBus program, 348
netcat tool, 135, 267
NETinVM environment, 390, 392–396, 393–396
NetStumbler tool, 181
network access control (NAC), 274
network address translation (NAT), 51
network administrators, 326
network analysis in digital forensics, 250
network attached storage (NAS), 101
Network-Based Intrusion Detection System (NIDS), 136–137, 137, 273
Network-Based Intrusion Prevention System (NIPS), 138
network command, 454
network engineers, 318
network enumeration tools, 177
network interface layer, 48–49, 48
network loop attacks, 97
networks
advanced design. See advanced network design boundaries, 207, 208
partitioning, 334
segmentation and delegation, 334–336, 335
traffic analysis, 303–304
virtual, 392–396, 393–396
new technologies, 273
business tools, 290–292
IDP systems, 273–274
network access control, 274
security systems and services, 275–277
SIEM, 274–275
technology evolution, 278–281
NIDS (Network-Based Intrusion Detection System), 136–137, 137, 273
Nigerian money laundering scheme, 286
Night Dragon attacks, 39, 64
Nikto Web Scanner, 406–408, 407
Nimda worm, 59, 124, 194
NIPS (Network-Based Intrusion Prevention System), 138
NIST. See National Institute of Standards and Technology (NIST)
Nmap Network Scanning, 433
Nmap Scripting Engine (NSE), 397, 411
nmap tool
discovery, 400
fingerprinting, 175
password cracking, 431
port scanning, 396–400, 398
nones, 6
nondisclosure agreements (NDAs), 238, 243–244
nonlinear transform, 12
nonrepudiation
as cryptography goal, 3–4
description, 315
hashing, 18
IA measures, 293
Nping tool, 397
NS records, 61
NSA (National Security Agency), 129
NSA IAM technique, 217
NSE (Nmap Scripting Engine), 397, 411
nslookup utility, 62
NSTIC (National Strategy for Trusted Identities in Cyberspace), 277
NVD (National Vulnerability Database), 267, 284

O

OASIS (Organization for the Advancement of Structured Information Standards), 365–366
Obama, Barack, 359
observe-orient-decide-act (OODA) model, 324, 325
OCSP (Online Certificate Status Protocol), 25–26
Oechslin, Philippe, 180
OFB (output feedback) mode, 10–11
offshore risks, 197
oil industry operational risks, 195
OISF (Open Information Security Foundation), 273
OLAs (operating level agreements), 238, 298
OllyDBG tool, 301
one-way functions, 13
ongoing research, 266–270
out-of-band transmissions in symmetric encryption, 8
output feedback (OFB) mode, 10–11
outsourcing, 197–199
overflows
buffer, 162–163, 162, 284
integer, 163, 164
OWASP (Open Web Application Security Project), 150, 155, 157–158, 267
ownership of end-to-end solutions, 370–371

P
P0f tool, 175
PaaS (platform-as-a-service) cloud model, 83
packet filtering, 42, 42
packet sniffers, 268
description, 177–178, 179
Wireshark. See Wireshark packet sniffer
PacMan game, 163
PAIN algorithm, 3
palm scan systems, 276
PAP (Password Authentication Protocol), 29, 358
parallel operations, 337
parallel tests, 148, 333
parallel virtual machines, 92
parity checking, 10
partitioning networks, 334
partnerships, 199–201
Pass the Hash toolkit, 351
passive fingerprinting, 174–175
Password Authentication Protocol (PAP), 29, 358
password command, 455
passwords
cracking, 179–180, 277, 429–431, 429–430
inconvenience, 275–276
single sign-on. See single sign-on (SSO)
strength, 30
patches, 193, 285
Payment Card Industry Data Security Standard (PCI DSS), 236, 240
PBX systems, 353
PCAOB (Public Company Accounting Oversight Board), 300
PCI (Peripheral Component Interconnect) slots, 205
PCI DSS (Payment Card Industry Data Security Standard), 236, 240
PDAs, 208
PDDs (Presidential Decision Directives), 271
PEM (Privacy Enhanced Mail), 352
penetration testing. See security assessments and penetration testing
Pentesting VoIP section, 47
perfect forward secrecy (PFS), 17
performance analysis, 301–302, 317
“Protocol for Packet Network Interconnection” paper, 47
protocols
  data exfiltration, 134
  IDS, 273
prototyping and testing multiple solutions, 298–299
provisioning, 85
pseudorandom number generators, 6
PsFile tool, 420
PSH (push) flag in TCP, 56
PsList tool, 419, 419
PsService command, 420
PSTNs (public switched telephone networks), 354
PTR records, 61
public classification, 213
Public Company Accounting Oversight Board (PCAOB), 300
public key cryptography, 13–14
public key exchange (PKI) framework, 22
certificate authorities, 22–23, 23
certificate-based authentication, 369
certificate distribution, 26
certificate revocation lists, 23–24
client role, 26–27
digital certificates, 24–26, 25
registration authorities, 23
trust, 27
public switched telephone networks (PSTNs), 354
public use services, 82
publishers, verifying, 415
push (PSH) flag in TCP, 56
PuTTY tool, 270
Pwn2Own conference, 294

Q
QEMU product, 269
Qovia products, 356
qualitative risk assessment method, 216–217
Quality of service (QoS)
  prioritizing traffic, 362
  VoIP, 357
quantitative risk assessment method, 214–216

R
race conditions, 163–164
RADIUS (Remote Authentication Dial-In User Service), 40, 357
rail fence ciphers, 7, 7
rainbow tables, 180, 430
RAM-resident viruses, 126
random keys, 5
RAs (registration authorities), 23
RAS (Remote Access Services), 40
RAT (Remote Access Tool), 57
Rational AppScan tool, 301
RATS (Rough Auditing Tool for Security), 169, 176
RC ciphers, 13
RC4 (Rivest Cipher 4), 9
RC5 (Rivest Cipher 5), 9
rcrack tool, 430
rcrack_mt tool, 430
recommended links, 460–461
Recommended Security Controls for Federal Information Systems and Organizations, 271
recovery of data breaches, 243
registered ports, 173
registration authorities (RAs), 23
RegMon tool, 418
regression tests, 148, 333
regulatory policies, 233
remote access, 40–41, 41, 357–358
Remote Access Services (RAS), 40
Remote Access Tool (RAT), 57
remote assistance programs, 351
Remote Authentication Dial-In User Service (RADIUS), 40, 357
report analysis in IDS systems, 136
reputation
damage, 376
value, 211
Requests for Comment (RFC) group, 278–280
requests for information (RFIs), 297
requests for proposal (RFPs), 297, 333
requests for quotation (RFQs), 297
requirements for contracts, 296–298
resistance to change, 330
resource exhaustion, 164–165
resource management, 317
response boxes in IDS systems, 136
response to data breaches, 242
restricted interfaces, 133
results of solutions in technology life cycle, 371–372
retention policies for data, 237
retention time for documents, 251
retina pattern systems, 276
Retina tool, 131, 177, 269
retired smartphones, 210
return on investment (ROI), 337
reverse engineering, 301
reviews
  after-action, 302–303
code, 149–150, 169
documents, 239
  policies and procedures, 235–237
RFC (Requests for Comment) group, 278–280
RFIs (requests for information), 297
RFPs (requests for proposal), 297, 333
RFQs (requests for quotation), 297
Rijmen, Vincent, 12
Rijndael cipher, 9, 12
risk, 189–191
  analysis options, 217–218, 218
  assessment, 213–217
  asset identification, 210–211
  best practices, 220–221
  cloud computing, 89–90
  continuous monitoring, 219–220
  controls, 218–219
  corporate governance for, 316
  ESA frameworks, 220
  exam essentials, 222–223
  information classification, 212–213
  operational. See operational risks
  review questions, 224–227
  summary, 221
  terminology, 191–192
  vulnerabilities identification, 192–194, 194
risk management teams, 213–214
risk matrices, 217–218, 218
Ristic, Ivan, 116
Rivest, Ron, 13, 15, 19
Rivest Cipher 4 (RC4), 9
Rivest Cipher 5 (RC5), 9
Rivest cipher algorithms, 13
ROI (return on investment), 337
roles in disciplines, 325–328, 325
rolling back changes, 373
root name servers, 60
rootkit detection, 437–440, 438–440
Rootkit Revealer, 440
ROT3 ciphers, 2
rotation, job, 245
Rough Auditing Tool for Security (RATS), 169, 176
rounds, cipher, 9–10
route protection, 68
router command, 454
router configuration, 68–69
routing, lab manual for, 449–459, 450–459
RSA algorithm, 15
RSA Secure PC encryption, 363
RTM worm malware, 124
Rule element in XACML, 366
rules
  ACLs, 110–111
  spam filters, 128
Russinovich, Mark, 416

S

S-HTTP (Secure Hypertext Transfer Protocol), 28
S/MIME (Secure Multipurpose Internet Mail Extension), 352
SaaS (Software as a Service), 83, 333
SABSA (Sherwood Applied Business Security Architecture), 220
SAFER (Secure and Fast Encryption Routine) cipher, 10
SAINT tool, 131, 176, 269
salami attacks, 122
sales staff, dealing with, 318
SAML (Security Assertion Markup Language), 365–366
SAN snapshot software, 102
SAN storage, 101–102
sandboxing, 154
SANS Policy project, 234
SARA tool, 269
Sarbanes-Oxley Act (SOX), 203–204, 231, 240, 331
SAs (Security Associations), 29
SAS (Statements on Accounting Standards), 300
SAS 70 (Statement of Auditing Standards 70), 239
SASL (Simple Authentication and Security Layer), 64
SATAN (Security Administrator Tool for Analyzing Networks) program, 170, 266
SCADA (supervisory control and data acquisition) systems, 39, 44–45, 45
scalability, 302
Scanners and scanning
  Nessus Vulnerability Scanner, 408–411, 409–410
  port. See port scanners
  signature-based, 433–437, 435–437
  for vulnerabilities, 131, 175–177
SCAP (Security Content Automation Protocol), 269
scareware, 288
Schneier, Bruce, 41, 204
screened host firewalls, 42, 42
screened subnets, 42
Scytale system, 2
SDL (security development lifecycle) process, 440–441
SDL At Modeling Tool, 270
SDLC (systems development life cycle)
  overview, 373–375, 374–375
  steps, 154–155
search engine poisoning, 288
secret classification, 212
Sectera Edge smartphone, 359
Sectools site, 267
Secure and Fast Encryption Routine (SAFER) cipher, 10
secure communication solutions, 60–66
secure directory services, 64
secure DNS, 62–63
secure facility solutions, 66–67
Secure Hash Algorithm (SHA), 19, 391
Secure Hypertext Transfer Protocol (S-HTTP), 28
secure infrastructure design, 67–68
  Enterprise Service Bus, 69
  router configuration, 68–69
Web Services Security, 70
Secure Multipurpose Internet Mail Extension (S/MIME), 352
Secure Shell (SSH), 27, 270
Secure Sockets Layer (SSL), 28, 64, 409
secure storage management systems, 102
Securities and Exchange Act, 329
Security Administrator Tool for Analyzing Networks (SATAN) program, 170, 266
Security Assertion Markup Language (SAML), 365–366
Security Assessment Process document, 271
security assessments and penetration testing, 165
assessment areas, 168–170
assessment types, 167–168
exam essentials, 182–183
penetration testing steps, 166–167
review questions, 184–187
summary, 182
test methods, 145, 166
tools, 170–171
fingerprinting, 174–175
footprinting, 171–173
fuzzing and false injection, 180–181
HTTP interceptors, 181
network enumeration, 177
password cracking, 179–180
port scanning, 173–174
protocol analyzers, 177–178, 179
testing, 270
vulnerability scanners, 175–177
wireless, 181
Security Associations (SAs), 29
security audits, 166
security code reviews, 169
Security Content Automation Protocol (SCAP), 269
security development lifecycle (SDL) process, 440–441
Security Event Management (SEM), 65
Security Information and Event Management (SIEM), 65, 274–275, 336
Security Information Management (SIM), 65
security policies, 233
security requirements traceability matrix (SRTM), 374–375, 375
security research and analysis. See trends and research
Security Socket Layer (SSL), 64
security system development life cycle (SSDLC), 373–374
security systems and services, new, 275–277
security triad, 314, 314
SELinux tool, 336
SEM (Security Event Management), 65
sensitive classification, 213
sensitive information, 196, 239
data breaches, 242–243
employee policies, 243–247
personally identifiable information, 240–241
security concerns, 240
storing, 159
sensors in IDS systems, 136
separation of duties, 245
servers
anti-spyware software, 127
C&C, 63–64, 123
Kerberos, 65
virtual, 93–96, 94–95
service deterioration in partnerships, 200
service level agreements (SLAs)
cloud computing, 88
contracts, 297–298
description, 238
outsourcing, 199
service-oriented architecture (SOA), 70
service password-encryption command, 459
Service Provisioning Markup Language (SPML), 368
services
hardening and removing, 132
integration with products, 336–337
Sesame SSO, 367
session hijacking, 286
session management attacks, 151–152, 152
session state, cookies for, 159–160
SET (Social Engineering Toolkit), 445–449, 446–448
Set-Cookie command, 159
Sf.c.exe (Windows System File Checker), 18
SHA (Secure Hash Algorithm), 391
shadow security scanners, 176
Shady RAT, 296
Shaft tool, 192
Shamir, Adi, 15
shared keys in symmetric encryption, 8
sharing, desktop, 348–350
Sherwood Applied Business Security Architecture (SABSA), 220
shift row method, 12
ShmooCon conference, 294
Short Message Service (SMS), 288
show access-lists command, 457
SIEM (Security Information and Event Management), 65, 274–275, 336
sigcheck command, 417, 417
signature-based antivirus programs, 125
signature-based scanning, 433–437, 435–437
signatures
digital, 4, 15, 20–22, 21
IDS, 135–136, 273
SIM (Security Information Management), 65
Simple Authentication and Security Layer (SASL), 64
Simple Integrity property, 120
Simple Mail Transfer Protocol (SMTP), 59, 206, 352
Simple Network Management Protocol (SNMP), 59, 177
Simple Object Access Protocol (SOAP), 70, 361
overview, 366–367, 367
SAML assertions, 366
Simple Security property

single flux, 63
single loss expectancy (SLE) in risk assessment, 215–216
single sign-on (SSO), 361
benefits, 65
description, 277
overview, 367–368
single-tier packet filtering, 42, 42

situational awareness, 281
client-side attacks, 282–285
emergent issues, 287–289
threats, 285–287
skimmers, 241

Skipjack cipher, 10
SkyDrive service, 101
slamming, 353
SLAs (service level agreements)
cloud computing, 88
contracts, 297–298
description, 238
outsourcing, 199

SLE (single loss expectancy) in risk assessment, 215–216
SmartDraw tool, 269
smartphones, 208, 210, 288, 363–365
SMiShing, 288
SMobile Systems report, 365
SMTP (Simple Mail Transfer Protocol), 59, 206, 352
Smurf attacks, 165
sniffers, 268
description, 177–178, 179
Wireshark. See Wireshark packet sniffer
sniffing
email, 352
IPv4, 51
VoIP traffic, 46–47, 47, 354
SNMP (Simple Network Management Protocol), 59, 177
Snort IDS, 267, 273
importance, 136
lab manual, 431–433, 432–433
SOA (service-oriented architecture), 70
SOA (Start of Authority) records, 61–62
SOAP (Simple Object Access Protocol), 70, 361
overview, 366–367, 367
SAML assertions, 366
sociability tests, 148, 333
social engineering
lab manual, 445–449, 446–448
testing, 169
Social Engineering Toolkit (SET), 445–449, 446–448
social media/networking, 172, 290–291
software analysis in digital forensics, 230
Software as a Service (SaaS), 83, 333
software-based VPNs, 360
software escrow, 334
software patches, 193, 285
software requirements for lab manual, 387
solution results in technology life cycle, 371–373
Song, Dug, 59
source code scanners, 175–176
SOX (Sarbanes-Oxley Act), 203–204, 231, 240, 331
Space and Warfare Command (SPAWAR), 273
spam
description, 122, 351–352
filters, 128–129, 129
overview, 285
SMTP, 59
Spam over Instant Messaging (SPIM), 348
Spam over Internet Telephony (SPIT), 356
SPAN (Switch Port Analyzers), 178, 354
Spanning Tree Protocol (STP), 97
sparse infection viruses, 126
SPAWAR (Space and Warfare Command), 273
spea-boarding, 285
Special Publication 800-53, 271
Special Publication 800-100, 271
speed bumps, 284
SPIKE tool, 180
SPIKEFile tool, 180
SPIM (Spam over Instant Messaging), 348
SPIT (Spam over Internet Telephony), 356
SPITTER tool, 356
SPML (Service Provisioning Markup Language), 368
spoofing
caller ID, 286
MAC addresses, 49
SMTP, 59
switch, 97–98
SpyEye botnet, 123
spyware, 122, 126–128, 285–286
SQL injection
data exfiltration, 134
description, 284
overview, 153–154
SRTM (security requirements traceability matrix), 374–375, 375
SSDLC (security system development life cycle), 373–374
SSH (Secure Shell), 27, 270
SSL (Secure Sockets Layer), 28, 64, 409
SSO (single sign-on), 361
benefits, 65
description, 277
overview, 367–368
stakeholders, 326
standard libraries, 155–156
standard of due care, 270
standard operating systems, 130
standards, 235, 272
audits, 300
coding, 156–157
NIST. See National Institute of Standards and Technology (NIST)
Star Security property, 120
Start of Authority (SOA) records, 61–62
state management, 151
Statement of Auditing Standards 70 (SAS 70), 239
Statements on Accounting Standards (SAS), 300
static analysis, 301
steganography, 134
Stevens, W. Richard, 268
stolen phones, 363
storage
cookies, 159–160
telephony systems
slamming and cramming, 353
testing
antivirus programs, 125
application security, 147–149
coding, 157
penetration testing. See security assessments and penetration testing
TFTP (Trivial File Transfer Protocol), 59
TGS (ticket-granting service), 368
TGTs (ticket-granting tickets), 368
Thawte CAs, 22, 26, 369
THC-Amap tool, 174
The Brain malware, 124
theft
cookies, 282, 282
devices, 197
third-party products
key distribution centers, 65
risk from, 332–334
Thomas’ English Muffins lawsuit, 244
thread information, 417
threats
defined, 191
emerging, 375–376
modeling
lab manual, 440–441
tools, 270
situational awareness, 285–287
thumb drives, 208
ticket-granting service (TGS), 368
ticket-granting tickets (TGTs), 368
time of check (TOC) in race conditions, 163
time of use (TOU) in race conditions, 163
time service factor (TSF), 199, 301
time-to-live (TTL) values, 62
Time-Warner merger, 201
timeout exploitations, 151
TKIP (Temporal Key Integrity Protocol), 181
TLS (Transport Layer Security), 28
TOC (time of check) in race conditions, 163
ToorCon convention, 294
top-down testing, 149
top secret classification, 212
tornados, 196
TOS (Type of Service), 175
TOSs (trusted operating systems), 117–120
total cost of ownership (TCO), 130
TOU (time of use) in race conditions, 163
TPM (Trusted Platform Module), 204–205, 363
TPoX (Transaction Processing over XML), 206
tracert command, 393
traffic
analysis, 303–304
prioritizing, 362
training
cloud computing, 88
employee, 244–245, 254–255
Transaction Processing over XML (TPoX), 206
Transaction Signature (TSIG), 63
transfer risk strategy, 218
Transmission Control Protocol. See TCP
(Transmission Control Protocol)
transport layer, 28, 35–56, 35, 37
Transport Layer Security (TLS), 28
transport mode, 29
Transport Protocol layer in SOAP, 367
transport security in router configuration, 68–69
transposition ciphers, 7
trap doors, 13–14
trends and research, 265–266
analysis
benchmarking, 298
cost-benefit analysis, 299
cyber defense aids, 299
existing security, 299–300
judgment to solve problems, 303
Lessons Learned, 302–303
network traffic analysis, 303–304
prototyping and testing multiple solutions, 298–299
reverse engineering, 301
security solutions, 301–302
best practices, 270–273, 272
exam essentials, 305
global IA community, 293–296, 295
new business tools, 290–292
new technologies. See new technologies
ongoing research, 266–270, 267–268
requirements for contracts, 296–298
review questions, 306–309
situational awareness, 281
client-side attacks, 282–285, 282
devices, 197
emergency issues, 287–289, 287
threats, 285–287
summary, 304–305
technology life cycle, 375–376
Tribal Flood Network tool, 192
Trinoo attacks, 165
Triple DES (3DES), 11–12
Tripwire program, 18
Trivial File Transfer Protocol (TFTP), 59
Trojans, 122
tropical storms, 196
TrueCrypt tool, 3, 204, 425, 428
trunking protocols in VLANs, 97
trunking security in router configuration, 69
trust
hierarchical trust model, 22, 23
PKI, 27
webs of trust, 26–27
trusted computer base (TCB), 119
Trusted Computer System Evaluation Criteria (TCSEC), 118, 377
trusted operating systems (TOSs), 117–120
Trusted Platform Module (TPM), 204–205, 363
TSF (time service factor), 199, 301
TSIG (Transaction Signature), 63
tsunamis, 196
TSweb (Terminal Services), 349, 349
TTL (time-to-live) values, 62
tunnel mode, 29
2600 magazine, 296, 346
Twofish cipher, 10
Type 1 and Type 2 errors, 276
Type of Service (TOS), 175

U
UAs (uptime agreements), 199, 238, 301
UCSniff tool, 346
UDP (User Datagram Protocol), 47
ACLs, 112
description, 56, 57
port scanning, 174
VoIP, 355
UI redressing, 151
unacceptable use clauses (UUPs), 320
unauthorized entry, 197
Unbound software, 60
unclassified classification, 212
unified communication security, 345–353, 348–349
unit testing, 157
United Airlines merger, 331
updating policies and procedures, 235–237
uptime agreements (UAs), 199, 238, 301
US-CERT (U.S. Computer Emergency Readiness Team), 193
usability, 302
User Access Control (UAC) dialog box, 391
User Datagram Protocol (UDP), 47
ACLs, 112
description, 56, 57
port scanning, 174
VoIP, 355
user roles, 325
username command, 455
UUPs (unacceptable use clauses), 320

V
vacations, mandatory, 245
validating
input, 152, 153
system designs, 376–378
value delivery in corporate governance, 316
variable-length subnet masking (VLSM), 51
VDI (virtual desktop infrastructure), 92, 92
vector-oriented approach, 121
Venema, Wietse, 170, 266
Veridis program, 28
verifying
baseline security configuration, 411–413, 412
publishers, 415
VeriSign CAs, 22, 26, 369
Vernam cipher, 3
vertical privilege escalation, 158, 158
ViaCrypt PGP encryption, 363
videoconferencing systems, 347
VideoSnarf tool, 346
Vigenère polyalphabetic cipher, 3
virtual computing, 299
virtual desktop infrastructure (VDI), 92, 92
Virtual LANs (VLANs), 97–98
virtual machine monitors (VMMs), 94
virtual machines, 93
virtual networks, 392–396, 393–396
virtual private networks (VPNs), 40–41, 335
Virtual Private Storage (VPS), 88
virtual SANs (VSANs), 102
VirtualBox product, 269
virtualization
exam essentials, 103–104
lab manual, 389–392, 391–392
overview, 92–93, 92, 269
review questions, 105–108
servers, 93–96, 94–95
summary, 103
viruses, 122, 124–126, 150
VirusTotal, 433–436, 435–437
Visa, 271
vishing, 169
VLAN hopping, 69, 97
VLANs (Virtual LANs), 97–98
VLSM (variable-length subnet masking), 51
VM escape, 96
VM Player, 269
VMMs (virtual machine monitors), 94
VMware Player, 389–391
VMware tool, 299
voice over IP (VoIP)
implementation, 356–357
overview, 45–47, 46–47
security, 354–356, 355
Voice Over Misconfigured Internet Telephones (VOMIT) tool, 357
voice recognition system, 276
VOMIT (Voice Over Misconfigured Internet Telephones) tool, 357
VPNs (virtual private networks), 40–41, 335
hardware-based, 360
placement, 44
software-based, 360
VPS (Virtual Private Storage), 88
VSANs (virtual SANs), 102
Vt (vulnerability time), 194
vulnerabilities
assessment tools and scanners, 175–177, 269, 300
assessments, 166
cloud computing, 90–91
defined, 191
vulnerability time (Vt) – ZoneAlarm firewall

fixing, 131
identifying, 192–194, 194
lab manual, 406–408, 407
web applications, 269
vulnerability time (Vt), 194
vulnerability windows, 194, 194

W

WAFs (web application firewalls), 43, 116
warning banners, 133
Wassenaar Arrangement on Export Controls for
Conventional Arms and Dual-Use Goods
and Technologies, 30
Watt, Stephen, 134
Wayback Machine, 172
weak encryption, 160
web application firewalls (WAFs), 43, 116
web conferencing, 346
Web Services Security (WS-Security), 70
web vulnerabilities lab manual, 406–408, 407
WebFuzzer tool, 180
WebGoat application, 269
webification, 313
webs of trust, 26–27
well-known ports, 173
WEP (Wired Equivalent Privacy), 13, 181, 336
white box tests, 148, 168, 333
white hat hackers, 295
WiFi Protected Access (WPA), 181
wildcard certificates, 25
Windows Firewall, 115
Windows forensic tools, 413–421, 414–419, 421
Windows Server Update Services (WSUS)
servers, 412
Windows System File Checker (sfc.exe), 18
WinDump sniffer, 273–274, 304
WinPcap, 401
Wired Equivalent Privacy (WEP), 13, 181, 336
wireless intrusion prevention systems (WIPSs), 336
wireless security,
  network assessments, 168–169
  overview, 335–336
  testing tools, 181
Wireless Transport Layer Security
(WTLS), 28
Wireshark packet sniffer, 267–268, 268, 304
description, 178, 179
email sniffing, 352
IPv4 sniffing, 51
lab manual, 400–406, 402, 404
ping packet sniffing, 54
TCP header capture, 56
terminology, 403
token sniffing, 151
worms, 122, 124
WPA (WiFi Protected Access), 181, 336
WPA2, 336
WS-Security (Web Services Security), 70
WSUS (Windows Server Update Services)
servers, 412
WTLS (Wireless Transport Layer
Security), 28

X

X.509 digital certificates, 24, 25, 369–370
XACML (Extensible Access Control Markup
Language), 361, 366
XML (Extensible Markup Language)
messages, 70
Xprobe2 tool, 175
XSRF (cross-site request forgery) attacks, 120
client-side attacks, 283
description, 150
HTTP, 59
JavaScript vulnerabilities, 161
XSS (cross-site scripting) attacks
client-side attacks, 283–284
HTTP, 59
JavaScript vulnerabilities, 161
overview, 150
WAFs for, 43
XTACACS (Extended Terminal Access Controller
Access Control System), 40

Y

YaST2 Package Manager, 406

Z

Zatko, Peiter, 41
zero day attacks, 289
“Zero Day Malware Cleaning with the
Sysinternals Tools”, 416
zero knowledge proofs, 14
Ophcrack tool, 180, 277, 425, 430
Zeus botnet, 123–124, 288
Zimmermann, Phil, 28
zombies, 123, 287
zone transfers, 61–62
ZoneAlarm firewall, 115