INDEX

3DES, 651

door, 68–69
gates, 36–39
control relays, 21–23
sliding, 20
swinging, 21
ingress, 13
inner perimeter, 67–69
intruders, 13
regress, 13
rights, 13

ACK (acknowledge), 651, 703
ACLs (access control lists), 157–158, 244, 258, 427, 651, 703
Active Directory, 651
active RFID (Radio Frequency Identifier) tags, 651
ActiveX, 651–652
administrative tools, 652
administrator account, 342, 427, 691, 692
Windows, 343
Adobe Reader, 652
advanced persistent threats, 652
adversaries, 104
adware, 219, 652
AES (Advanced Encryption Standard), 652, 703
AFHSS (Adaptive Frequency Hopping Spread Spectrum), 413, 652, 703
AH (authentication headers), 283–284, 295, 551, 654, 703
AIM (Apple/IBM/Motorola), 703
algorithm, 652
allow permissions, 193
AM (Asset Management), 5
analog camera, 652
analysis, 105

A

AAA (Authentication, Authorization, Accounting), 331, 651, 654, 703
access, inherited, 672
access codes, 651
access control, 651
natural access control, 679
role-based, 437–438
servers
automated provisioning, 339
DAC (Discretionary Access Control), 338–339
MAC (Mandatory Access Control), 338–339
RBAC (Role-Based Access Control), 338–339
Rule-Based Access Control, 339
access control gate, 651
access control policy, 651
access rights, 244
access-control systems, 12, 98. See also remote-control access
authentication
biometric scanners, 27–29
inheritance, 23
knowledge, 23
location, 23
magnetic stripe systems, 24
possession, 23
RFID badges, 26
smart cards, 25–26
authorization, 13
Android OS, 166–168, 652
annunciators, 653
anomaly analysis, 653
anomaly-based IDS/IDPS, 653
anonymous proxy, 653
anti-malware software, 205
antispyware, 221–222, 653
antivirus programs, 220–221, 653
Apple OS
  iOS, 166
  MacOS, 165–166
Apple OS X, 653
Apple Time Machine, 653
appliance servers, 329
appliance-based virtualization, 653
appliances, UTM devices, 519–520
application packages, 653
application servers, 329, 653
application zone, 653
application-level encryption, 653
applications
  smart phone, 692
  software exploitation, 223–224
ARM (Acorn RISC Machine/Advanced RISC Machine), 703
ARP (Address Resolution Protocol), 703
  spoofing attacks, 394, 430, 652
ARP command, 314
ARP utility, 318
AS (Authentication Server), 654
  Kerberos and, 540
ASLR (Address Space Layout Randomization), 652, 703
  software exploits and, 597
ASP (Application Service Provider), 653, 703
assessments, policies, 252
assets, 654
asymmetric encryption, 182, 543
asymmetric keys, 654
asymmetrical virtualization, 654
attack surface, 654
attacks
  buffer overflow, 657
  CDP (Cisco Discovery Protocol), 659
  clickjacking, 659
dictionary attacks, 606
DoS (Denial of Service), 302
double encapsulation VLAN hopping attack, 665
Fraggle attack, 636, 669
Layer 7, 676
logjam, 676
MAC broadcast, 430
MAC duplicating, 430
masquerade, 431, 678
MITM (man-in-the-middle) attacks, 217, 431
network connectivity, 393–397
packet sniffing
  ARP (Address Resolution Protocol), 394
  DoS (Denial-of-Service), 395–396
  MAC cloning, 395
  MAC flooding, 394
  masquerade, 397
  MITM (Man-in-the-Middle), 395, 397
  rerouting, 397
  router flood, 394
  session replay, 397
  spoofing, 395
  switch port stealing, 395
password attacks, 683
phishing, 600–603
  spear phishing, 602–603, 693
ping flood attack, 684
PVLAN (Private VLAN) attacks, 686
race condition, 687
replay, 283–284, 295, 689
rerouting, 431, 689
router flood, 430, 689
script kiddies, 607
session replay, 431, 692
side channel attacks, 692
spanning-tree, 693
spoofing, 431, 694
  ARP, 652
switch port stealing, 695
teardrop attack, 636, 696
Wireshark and, 585–588
attenuation, 654
audit entries, 654
audit event log files, 654
audit policy, 654
audit trail, 654
auditing, 245, 256, 427, 654
  detection-specific audit records, 663
  Linux, 180–181
  program development, 253
  records, 178
  servers, 331, 352–354
  Windows, 178–180
authentication, 40–41, 99, 244, 245, 256, 536,
  630, 631, 654
biometric scanners, 27–29
CAPTCHA and, 549–550
CHAP, 631
false acceptance, 99, 110
false rejection, 99, 110
inner perimeter security, 67–68
IP, 539
Kerberos, 631
MAC, 539
MFA (multifactor authentication), 679
multifactor, 537–538
  passwords, 538–539
PAKE, 631
PAP, 631
passphrase, 683
passwords, 348
physical devices, biometric scanners,
  176–177
protocols
  CHAP, 540
  CRAM, 541
  Kerberos, 540–541
  LDAP, 542
  PAKE, 541
  PAP, 539–540
  RADIUS, 541
  SRP, 541
RFID badges, 26
servers and, 331
single-factor, 537, 630, 692
spam and, 613
two-factor, 99, 630, 698
authentication systems, 654
  inheritance, 23
  knowledge, 23
  location, 23
  magnetic stripe systems, 24
  possession, 23
  smart cards, 25–26
authoritative server, 654
authorization, 13, 98, 655
automated access control, 32–33, 655
automated provisioning, 339, 655
Autorun, 655

B
B2B (Business-to-Business), 657, 703
B2C (Business-to-Customer), 657, 703
BAA (Business Associate Agreement), 703
backup operator accounts, Windows, 344
backups
  media, 655
  policy, 655
  servers, 354–356
  media security, 356
bandwidth, 408, 655
barriers, 655
baseline, 691
bastion host, 655
BCP (Bridging Control Protocol), 301
beacon frames, 655
beacon interval, 655
BeEF (Browser Exploitation Framework), 576,
  657, 703
BES (Bulk Electric System), 703
Bin group (Linux), 346
biometric scanners, 27–29, 176–177
biometrics, 656
BIOS (Basic Input/Output System),
  655, 703
Autorun, 136
boot devices, 136
exercises, 137–147
port enabling, 135
securing, 125–127
BitLocker, 162, 656
black hat hackers, 224, 656
blacklisting, 493, 633, 656
block cipher, 656
Blowfish, 656
Bluebugging, 656
Bluejacking, 656
Bluesnarfing, 656
Bluetooth, 407, 412–414, 656
boot files, 152, 656
boot services, 656
bot herder, 656
botnets, 220, 657
bots, 657
BPDUs (Bridge Protocol Data Units), 604, 703
bridge servers, 329, 429
bridges, 391
broadcast messaging, 464–465, 627
broadcast storms, 603–604, 635, 657
broadcast traffic, 657
brute force attacks, 245, 657
BSD (Berkeley Software Distribution), 703
buffer overflow, 224, 260, 657
bus topology, 280, 657
BYOD (bring-your-own-device), 657, 704
bypass mode, 657
bypassing, 657

C
CA (Certificate Authority), 704
cabinetry, 657
cabling, 407
copper, 660
Ethernet, 311
Fiber Optic, 668
twisted-pair cabling, 408–409
cache poisoning, 658
caching devices, 658
caching servers, 658
caching web proxies, 658
CAM (content addressable memory) tables, 299, 704
camera deployment strategy, 658
cameras (video surveillance), 46–47, 63–65
analog, 47
applications, 52–53
black and white, 51
CCD (Charged Coupled Device), 47, 108
color, 51, 55
day/night, 52
deployment, 53–56
digital, 47, 110
display definition, 56
external/interior video triggers, 52
fixed, 52
fixed field, 55
image display, 55
indoor/outdoor, 52
infrared, 55, 108, 111
IP, 47–48
IR illumination, 51
lenses, 111
fish eye, 51
pinhole, 51
telephoto, 50
varifocal, 50
wide-angle, 50
lux rating, 50
movable field, 55
multiplexing, 53
placement, 53–54
PTZ (pan-tilt-zoom), 48–49
resolution, 49, 111
sequencing, 53
signal processing, 56
signal transmission, 56
telephoto lens, 696
thermal, 55
varifocal lens, 699
wide angle lens, 701
candela, 658
CANs (campus/corporate area networks),
    274, 704
cantenna, 658
CAPTCHA (Completely Automated Public
    Turing test to tell Computers and Humans
    Apart), 549–550, 632, 660, 704
capturing passwords, 683
carbon dioxide (CO₂) detectors, 86–87
carbon monoxide (CO) detectors, 86–87
CATV (commercial cable television), 704
CC (Common Criteria), 659
CCD (Charged Coupled Devices), 108, 658,
    704
CCTV (closed-circuit TV), 45, 659, 704
CDFS (Compact Disc File System), 161, 704
CDP (Cisco Discovery Protocol) attacks,
    659, 704
certificate chain, 658
certificates, public key, 687
CHAP (Challenge-Handshake Authentication
    Protocol), 540, 631, 658, 704
chokepoint, 658
chroot, 658
CIA (confidentiality, integrity, availability),
    331, 660, 704
CIFS (Common Internet File Systems), 659,
    704
CIP (Critical Infrastructure Protection), 704
cipher locks, 19–20, 658
ciphers, 658
    simple stream, 544–545
ciphertext, 542, 631, 658
CISC (Complex Instruction Set Computing),
    704
cleartext, 659
clickjacking attacks, 605–606, 636, 659
client operating systems
    terminal clients, 154
    thick clients, 154
    thin clients, 154
client-server, 659
client/server networks, 311, 659
    advantages, 312–313
    diskless workstations, 313
closed-condition monitoring, 30–31
cloud computing, 659
cloud-based services, 659
CloudFlare, 609
CMOS Setup utility, 125–127
CMS (Centers for Medicare and Medicaid
    Services), 704
CMSA/CD (Carrier Sense Multiple-Access with
    Collision), 704
cable, 311, 659
cable, 409–410
Command Prompt window, modifying,
    314–315
color options, 316
command-line programming, network
    switches and, 387
communication media, 660
complexity, 660
Conficker, 660
connectivity, devices, 660
contingency planning, 660
control relays
    NC (Normally Closed) output, 22
    NO (Normally Open) output, 22
    relay operations, 22–23
    SPDT (single-pole, single-throw),
        21
controllers, 660
    zones, 74–77
controls, passive, 682
cookies, 247, 548–549, 660
    attributes, 216
    persistent cookies, 216, 684
    poisoning, 217, 660
    session cookies, 216, 692
    super cookies, 632, 694
    theft, 216, 660
    tracking, 697
copper wire, 407, 660
    coaxial cabling, 409–410
    twisted-pair cabling, 408–409
Corporate Cyber Security Policies, 110
corporate facility scenario, 6
    plans, 7
    risk assessment, 7–8
CPE (Common Platform Enumeration), 470–471, 659, 704
CPTED (crime prevention through environmental design), 14, 704
Crackers, 224, 660
Crack, 661
Craig, Philip, 102, 249, 432
CRAM (Challenge Response Authentication Mechanism), 541, 704
CRAM-MD5, 661
Credential harvesting, 661
Critical infrastructure, 715–716
CRL (Certificate Revocation List), 704
crypt utility, 661
cryptography, 182, 246, 631, 661
asymmetric keys, 543
Ciphers, 543
simple stream, 544–545
symmetric-key, 545
Keys, 543
pseudorandom key generators, 545
Private keys, 543
Public keys, 543
authentication and, 543–544
DSS, 544
encryption and, 543–544
GNU, 544
PGP, 544
RSA encryption algorithm, 544
S/MIME, 544
SSH, 544
SSL, 544
TLS, 544
Reverse engineering and, 544
Symmetric keys, 543
3DES, 544
AES, 544
Blowfish, 544
ciphers, 545
RC4, 544
shared secrets, 544
CryptoLocker, 661
cryptology, 661
CSMA/CD (carrier sense multiple-access with collision detection), 309
CSP (Cloud Storage Provider), 704
CSR (Certificate Signing Request), 705
current loop, 76, 661
CVE (Common Vulnerabilities and Exposures), 470, 659, 705
CVSS (Common Vulnerability Scoring System), 470, 660, 705
Cyber Kill Chain, 661
cyber security policy, 661
cyber warfare, 661
cybercriminals, 661
cybersecurity, 97, 661
definition, 10
OSI Layer 7, 279
as skill set, 459
Cybersecurity Framework. See NIST Cybersecurity Framework
cyberterrorists, 661

D
DAC (Discretionary Access Control), 427, 664, 705
servers, 338–339
DACL (discretionary access control list), 664, 705
daemon, 661
Daemon group (Linux), 346
DAI (Dynamic ARP Inspection), 398, 665, 705
dark-side hackers, 224
DAS (Direct-Attached Storage), 705
data concentrators, 662
data diodes, 662
data encoding, 662
data in motion, 662
data in use, 662
data security, 630
data transmission packets, 277–278
database servers, 329
datagrams, 461
DCS (Distributed Control System), 705
DDoS (distributed Denial-of-Service) attacks, 607, 636, 664, 705
DEA (Drug Enforcement Administration), 705
deadband, 662
deadbolts, 37–38
    key-locking, 17
    solenoid-operated, 18–19
deauthentication flood attack, 662
decrypt, 662
decryption, 662
decryption key, 662
default user accounts, 663
defense-in-depth, 663
defined threat environment, 105
deny permissions, 193
    explicit deny, 193
DEP (Data Execution Prevention) mode, 157, 662, 705
    software exploits and, 597
DES (Data Encryption Standard), 662, 705
desktop/single user, 662
detachable devices, 253
Detect function (framework), 3
    corporate facility scenario, 8
    electrical substation scenario, 6
detection-specific audit records, 663
device security
    administration electronic policies, 256
    BIOS, 125–127
    docking stations, 123–124
    DVD drives, 116, 118
eSATA ports, 132–133
    FireWire, 132
    host devices, 123–124
        inner-perimeter portals, 127–137
        outer-perimeter portals, 124–127
    implementation, 254
    keyboards, 116, 118
    layers, 121–122
    legacy ports, 133–134
    mice, 116
    monitors, 116
    Office 2013 software, 116, 118
    perimeters, 121
    removable media, 135–137
    risk assessment, 117, 119
    scenario 1, 249–255
    scenario 2, 255–257
    SD card reader slot, 118
    system hardening, 127
    USB connection ports, 116, 118
    USB (Universal Serial Bus) ports, 130–132
    UTP LAN connection ports, 116, 118
    VGA display, 118
    vulnerabilities, 251
    Windows 7 Pro operating systems, 116, 118
    wireless networking, 118
    devices
        Bluetooth, 412–414
        connectivity, 660
        digital IP devices, 663
        input, 672
        network connectivity, 385, 423
            attacks, 393–397
            bridges, 391
            gateways, 390–391
            routers, 388–390
            switches, 386–387
            wireless networks, 392
        Plug and Play, 429
        repeaters, 689
        single point of failure, 512
    DHAs (Directory Harvest Attacks), 637, 664, 705
    DHCP (Dynamic Host Configuration Protocol)
        servers, 330, 488, 663, 665, 705
        IP addresses, 469
    DHCP (Dynamic Host Configuration Protocol)
        spoofing, 663
    DHE (Diffie-Hellman key exchange), 615, 705
    DHT (distributed hash tables), 548, 705
    dictionary attacks, 606, 636, 663
digital cameras, 663
digital certificates, 545–547, 632, 663
    SSL (Secure Sockets Layer), 547
    TLS (Transport Layer Security), 547–548
digital data, 407
digital IP device, 663
direct-attached storage, 663
directory traversals, 160, 664
Disk group (Linux), 346
diskless workstations, 313
disk-level encryption, 246, 664
displays, securing, 125
distorting proxy, 664
distributed IDS system, 664
distributions, 664
diversion, 664
DMZ (demilitarized zone), 514, 522–523, 629, 663, 705
dual-firewall, 524–525, 665
single firewall, 692
single-firewall, 523–524
DNP3 (Distributed Network Protocol), 705
DNS (Domain Name Service), 665, 705
DNS RRL (DNS Response Rate Limiting), 610, 664
servers, 329
docking stations, 123–124, 665
documentation, 665
domain accounts, windows, 344–345
domain controllers, 665
domain user accounts, 665
domains, 467–468, 628, 665
name servers, 467
TLD (top-level domain), 467–468
door locks, 93
DOS (disk operating system), 152, 664, 705
boot files, 152
file management files, 152
file structure, 153
kernel files, 152
utility files, 152
DoS (Denial-of-Service) attacks, 302, 395–396, 431, 636, 663, 705
sticky honeypot, 611–612
tarpitting, 611–612
double encapsulation VLAN hopping attack, 665
downstream interface, 665
DPI (deep packet inspection), 662
DRAM, 429
DRDoS (Distributed Reflection and Amplification Denial of Service) attack, 609–610, 636, 664, 705
DRP (Disaster Recovery Plan), 705
DS4P (Data Segmentation for Privacy), 662, 705
DTP (dynamic trunking protocol), 666, 706
dual-firewall DMZ, 524–525, 665
DVD drives, 116
built-in, 255
DVRs (digital video recorders), 101, 663, 706
dynamic ports, 207
dynamic variable, 666
E
EAL (Evaluation Assurance Levels), 706
EAP (Extensible Authentication Protocol), 416, 706
eCryptfs, 666
effective permissions, 194
EFL (Effective Focal Length), 706
EFS (encrypting file system), 161–162, 666, 706
egress, 666
electric deadbolts, 666
electric signatures, 666
electrical substation scenario
risk assessment, 4–6
switch gear, 4
Electronic Keyless Door Lock, 69
eMail servers, 666
EMV chip-and-PIN technology, 666
encryption, 158, 245, 630, 666
application-level, 653
asymmetric, 182
ciphertext, 542, 631
disk-level, 246, 664
file-and-folder level, 187–188
applying, 194–195
file-level, 668
cylinder-level, 668
hardware-level, 183–185
  TPM chips, 183–185
  TPM tools, 186
  keys, 246, 666
  levels, 261
  packet sniffing and, 542
  password, 683
  passwords, 542–543
  private key, 182
  process steps, 258
  public key, 182, 631, 687
  secret key, 182
  symmetric, 182
  testing, 199–200
enterprise networks, 666
  entropy, 667
  entry delay, 667
  enumerate, 667
eSATA (External Serial AT Attachment) ports, 667, 706
  security, 132–133
  escort, 667
ESIGN (Electronic Signatures in Global and National Commerce Act), 706
ESP (Encapsulating Security Payloads), 283–284, 296, 551, 666, 706
Ethernet, 667
  CSMA/CD (carrier sense multiple-access with collision detection), 309
  frame, 310–311, 425
  topologies, 311
Ettercap, 667
EV (Extended Validation) certificates, 667, 706
  event logging, 178–181
  servers, 352–354
  exam questions, 647–650
  exclusion, 667
exercises
  BIOS settings, 137–147
  firewalls, 225–230
  hashing, 552–563
  ICMP outbound rules, 234–241
  inner perimeter security, 188–202
  interior security, 90–94
Internet security, 471–485
  network connectivity, 313–325, 399–404
  networks, Hyper-V, 496–508
  perimeter security, 33–44
    inner perimeter, 60–69
  PING capture, 583–585
  servers, 361–382
  software exploits, 616–626
  TCP outbound rules, 230–234
  transmission media, 417–421
  VPNs, 528–533
Wireshark
  attacks and, 585–588
  launch, 579–583
exFAT, 667
  exit delay, 667
  explicit permissions, 194
  exploits, 667
    Metasploit, 678
  export-grade encryption, 667
  ext#, 667
  extensible, 668
  extranets, 526–527, 668

F
F2FS, 668
  fail-safe, 668
  fail-secure, 668
  fail-soft, 668
  false acceptance, 99, 110
  false negative, 668
  false positive, 668
  false rejection, 99, 110
  FAT (file allocation table), 706
  Fiber Optic cabling, 668
  fiber-optic cabling, 311, 410–411, 428
  field of view, 668
file management files, 152
file management system, 157–159
file servers, 669
file structure, 153
file systems
attacks
ADS (alternative data streams), 159–160
race conditions, 159
formats
CDFS (Compact Disc File System), 161
NTFS (New Technology File System), 161
UDF (Universal Disk Format), 161
hardening, 351–352
hardening and, 260
journaling file system, 675
network, 680
file-and-folder level encryption, 187–188
applying, 194–195
file-level encryption, 668
files
FMS (file management system), 150–151
permissions, 198–199
utility files, 699
FileVault, 669
FIPS (Federal Information Processing
Standard), 706
fire brigade, 669
fire detection and reporting system, 669
fire-detection sensors, 100, 669
heat sensors, 85–86
smoke detectors, 85–86
firewalls, 204, 207–209, 246, 669, 680
blocking incoming traffic, 242
DMZs (demilitarized zones)
dual-firewall, 524–525
single-firewall, 523–524
exercises, 225–230
as gateway devices, 515–517
ICMP (Internet Control Message Protocol),
517–518
local, 676
networks, 242, 515–517
packet-filtering, 682
proxy-filtering, 686
proxy-filtering firewalls, 517
QoS (Quality of Service) functionality, 517
rules, 669
servers, 329, 629
stateful packet inspection, 634
software, 261
stateful packet-filtering firewalls, 516
static packet-filtering firewalls, 516
FireWire, 669
security, 132
firmware, 669
fisheye lens, 669
fixed focal length lens, 669
Flash, software exploits and, 593
FMS (file management system), 150, 706
folder-level encryption, 668
folders, permissions, 195–198
foot-candle, 669
Fraggle attack, 636, 669
frames, 669
Framework. See NIST Cybersecurity
Framework
FREAK (Factoring attack on RSA-EXPORT
Keys), 615, 706
Free BSD, 163
FTA (Fault Tree Analysis), 706
FTP (File Transfer Protocol), 706
servers, 330, 670

G
Games group (Linux), 345
gates, 670
control relays, 21
NC (Normally Closed) output, 22
NO (Normally Open) output, 22
relay operations, 22–23
SPDT (single-pole, single-throw), 21
sliding, 20
swinging, 21
gateways, 390–391, 425, 429
devices, 628, 629, 670
firewalls, 515–517
good enough security, 512–513
VoIP (Voice over Internet Protocol), 513
servers, 329
GBDE (GEOM-Based Disk Encryption), 670, 706
glass breakage detection, 670
glass breakage sensors, 80
GPRS (General Packet Radio System), 706
graded approach, 105–106
gray hat hackers, 224
grayware, 670
group accounts, 665, 670
Linux, 345–346
security, 346–347
Windows
administrators, 343
backup operators, 344
guests, 344
network configuration operators, 344
power users, 344
remote desktop users, 344
users, 344
group credentials, 258
guest account, 342
Windows, 344
guests, 670
GUI (graphical user interface), 670, 706

security hardware, 253
tokens, 671
hardware-level encryption, TPM (Trusted Platform Module), 183–185
hash tables, 548, 632, 671
hashing, 552
file integrity, 560
MD5deep and, 553–559
multiple, 556–559
test files, 554–556
values comparison, 560–561
HBIDS (host-based IDS), 671, 706
headers, 463
data transmission packets, 277–278
window size, 464
heat sensors, 85–86
HelpAssistant account, 342
HFS (Hierarchical File System), 671, 706
HIDS (host-based IDS), 209–210, 246
HIPAA (Health Insurance Portability and Accountability Act), 493
honeynets, 526
honeypots, 525–526, 637, 671
sticky, 611–612
host address, 671
host-based authentication, 670
HTTP (Hypertext Transfer Protocol), 463, 671, 706
Hyper-V, 496
compatibility, 497–498
enabling, 498–499
Linux distribution, 503–508
Manager on taskbar, 500
virtual switches, 500–503
hypervisor, 671

I

IANA (Internet Assigned Numbers Authority), 466, 673, 706
IC (Integrated Circuit), 707
ICANN (Internet Corporation for Assigned Names and Numbers), 467, 628, 707

H

hackers, 224, 592, 670
black hat, 656
HAN (Home Area Network), 671, 706
hardening, 127
file system, 351–352, 671
network, 398–399, 680
operating systems, 244, 260
patches, 222–223
servers, 336–338
service packs, 222
updates, 223
hardware, 628
firewall devices, 671
perimeter, 512
ports, 671
ICCP (Inter-Control Center Communications), 707
Icinga, 671
ICMP (Internet Control Message Protocol), 300–301, 517–518, 636, 672, 707
echo requests, 242
outbound rules, 234–241
ICT (Information and Communications Technology), 672, 707
ID (identify), 5, 707
Identify (ID) function (framework), 3
corporate facility scenario, 7–8
electrical substation scenario, 5
identity proofing, 672
identity theft, 671
IDF (Intermediate Distribution Frame), 707
IDPS (Intrusion Detection and Prevention Systems), 12, 71–73, 246, 673, 707. See also reporting systems
anomaly-based, 247
carbon dioxide (CO₂) detectors, 86–87
carbon monoxide (CO) detectors, 86–87
fire-detection
heat sensors, 85–86
smoke detectors, 85–86
key fobs, 85
keypads, 84
local
HIDS (host-based IDS), 209–210
NIDS (network-based IDS), 209–210
profile-based anomaly detection, 210–211
threshold-based anomaly detection, 211
output devices
remote notification, 89
sirens, 87–88
strobe lights, 88–89
third-party monitoring, 89–90
panic buttons, 85
PIR (passive infrared) detector, 80–81
security zones, 74–78
sensors, 77–79, 100
glass breakage, 80
magnetic contact switches, 79–80
motion detectors, 80–82
pressure sensors, 84
vehicle detection, 82–83
signature-based, 247
IDS (Intrusion Detection Systems), 246, 353, 673, 707
distributed, 357–358, 428
physical, 684
Snort
configuration file, 362–377
running, 378–382
IDS/IDPS, signature-based, 692
IED (Intelligent Electronic Device), 707
IEEE (International Electrical and Electronic Association), 707
IEEE-1394, 672
IETF (Internet Engineering Task Force), 470, 628, 673, 707
ifconfig, 565
IGD (Internet Gateway Device), 707
IKE (Internet Key Exchange), 283–284, 296, 551, 673, 707
illegal, 672
in-band, 672
informative references, 672
infrared light, 407
infrastructure security, 97–98, 672
access-control systems, 12
exam questions, 109–111
inner perimeter, 11
interior, 11
intrusion-detection systems, 12
monitoring systems, 12
natural access control, 12
outer perimeter, 10–11
overview, 9–10
physical security, 10
remote-access monitoring, 29
automated access control, 32–33
closed-condition monitoring, 30–31
opened-condition monitoring, 30–31
reporting systems, 12
review, 101–109
scenario 1, electrical substation diagram, 4–6
scenario 2, corporate facility, 6–8
territorial reinforcement, 12
video surveillance systems, 12
ingress, 672
inheritance, authentication and, 23
inherited access, 672
inner perimeter security, 11, 149–150, 244, 672
access controls, 67–69
authentication/access control, 67–68
devices, 121
exercises, 60–70, 188–202
FMS (file management system), 150–151
OS (operating system), 151–152
   Android, 166–168
   Apple, 165–166
   attack areas, 155–160
   boot files, 152
   client operating systems, 154
   DOS (disk operating system), 152
   encryption, 182–188
   file management files, 152
   file structure, 153
   kernel files, 152
   Linux, 163–165
   position, 153
   security choices, 168–169
   server operating systems, 155
   standalone, 154
tools
   administrative, 177–181
   system security, 169–177
Unix, 162–163
utility files, 152
Windows, 160–162
OSI Layer 2, 279
physical structures, 14
private networks, 487
input devices, 672
insider threat, 672
intangible asset, 672
intangible property security, 672
interior security, 11, 98, 673
door locks, 93
exercises, 90–95
monitoring, 14
motion detectors, 93
interior sounders, 673
Internet
   businesses, 460
   CPE (Common Platform Enumeration), 470–471
   customers, 460
   CVE (Common Vulnerabilities and Exposures), 470
   CVSS (Common Vulnerability Scoring System), 470
   employees, 460
   environment, 460–461
   information access, 460
   information exchange, 460
   OCIL (Open Checklist Interactive Language), 471
   OVAL (Open Vulnerability and Assessment Language), 471
   players, 460–461
   protocols, ports, 465–466
   RFCs (Requests for Comments), 470
   routing, 466–467
      domains, 467–468
   SCAP (Security Content Automation Protocol), 470, 471
   secure connections, 204
   service providers, 460
   services, 460
   standards, 470–471
   TCP/IP (Transmission Control Protocol/Internet Protocol), 461
datagrams, 461
layers, 461
OSI model and, 461–462
packets, 461
segments, 461
UDP, 464
Internet gateways, 673
Internet security
  exercises
    browsing history, 474–476
    Internet Explorer settings, 472–474, 485
    privacy controls, 482–485
    security zones, 476–481
  network security and, 458
Internet services
  asymmetrical, 468
  full duplex, 468
  half duplex, 468
  ISPs and, 468–469
Internet zone, 673
interoperability, 673
intranets, 673
intruders, 13, 98, 673
I/O (input/output) controller, 672
I/O (input/output) ports, 208
  connectors, 134
iOS, 166, 674
IoT (Internet of Things), 673, 707
IP (Internet Protocol), 707
  traffic, 462–464
IP addresses, 424, 674
  authentication, 539
  DHCP server, 469
  spoofing, 539, 674
IP blocking, 674
IP cameras, 674
IP header manipulation, 674
IP spoofing, 301, 424
IP-based devices, 674
IP-based notification, 674
ipconfig, 565
IPCONFG /all command, 314
IPCONFIG utility, 316–317
IPS (Intrusion Prevention Systems). See IDPS
  (Intrusion Detection and Prevention Systems)
IPsec (Internet Protocol Security), 283–284, 551, 634, 673, 674, 707
  access, 284–286
  AH (Authentication Headers), 551
  connection monitoring, 293–295
  Connection Security Rules, 286–293
  ESP (Encapsulating Security Payloads), 551
  IKE (Internet Key Exchange), 551
  SAs (Security Associations), 551
  transport mode, 284
  tunnel mode, 284
IPv4, 674
IPv6, 674
IRP (Incident Response Policy), 707
ISO 2700xx, 674
ISO 15408, 674
isolation, 674
ISPs (Internet Service Providers), 468–469, 628, 707
IT (Information Technology), 707
IV (Initialization Vector), 707

J

Jackshaft Liftmaster, 69
jamming, 675
Java, software exploits and, 597–599
JavaScript, 675
JFFS2, 675
journaling file system, 675

K

Kerberos authentication, 540–541, 631, 675
  kernel files, 152, 675
  attacks, 156–157
  key control policies, 17
  key fobs, 85, 675
  relays, 22
  keyboards, 116
    access, 259
    detachable, 253
  keypads, 39, 84, 107, 108, 675
    relays, 22
keys, 16–17, 675
  key-locking deadbolts, 17
  solenoid-operated deadbolts, 18–19
KillerBee, 675
knowledge, authentication and, 23

L
L2TP (Layer 2 Tunneling Protocol), 634, 707
LANs (local area networks), 273, 676, 707
  physical security, 415
latency, 675
laws, 676
Layer 7 attacks, 636, 676
LDAP (Lightweight Directory Access Protocol), 542, 631, 676, 708
  injection attacks, 597
least privilege, 676
legal, 676
light waves, 407
Linux, 676
  auditing, 180–181
  distributions, 164
  encryption, 164–165
  file systems, 164
  group accounts, 345–346
  permissions, 349–350
local firewalls, 676
local login, 260–261
local protection tools, 206
  firewalls, 207–209
local security
  scenario 1, 266–270
  scenario 2, 270–272
location, authentication and, 23
locked condition monitoring, 676
lockout policy settings, 676
locks, 16–17, 676
  cipher, 19–20
  electric deadbolts, 666
  relays, 22
logic bombs, 219–220, 676
logical perimeter, 676
logical topologies, 282
login, local login requirements, 171–172
  computer locking, 175–176
  passwords, 172–175
logjam attacks, 615, 676
LOIC (Low Orbit Ion Cannon), 708
LOPA (Layer of Protection Analysis), 708
lux rating, 111, 677
  video cameras and, 107

M
MAC (Mandatory Access Control), 157–158, 426, 678, 708
  servers, 338–339
MAC (Media Access Control), 424, 708
MAC address filtering, 677
MAC address table, 428, 677
MAC addresses, 298–299, 677
  authentication, 539
  network switches, 386
MAC broadcast flood attack, 424, 430
MAC cloning attacks, 395
MAC duplicating attacks, 430, 677
MAC flooding attacks, 394, 677
MAC learning and discovery, 677
MAC spoofing, 424, 677
MacOS, 165–166
magnetic contact switches, 79–80, 677
magnetic stripe systems, 24, 677
Mail group (Linux), 346
mail servers, 329
malicious proxy servers, 677
malware, 247, 678
  access port, 260
  adware, 219
  anti-malware software, 205
  botnets, 220
  logic bombs, 219–220
  ransomware, 219
  rootkits, 218–219
  spyware, 219, 221–222, 247
Trojans, 218
viruses, 218
worms, 218
zombies, 220
managed switches, 387, 429, 678
MANs (Metropolitan Area Networks), 274, 708
masquerade attacks, 397, 431, 678
µC (microcontroller), 703
MDF (Main Distribution Frame), 708
MDK3, 678
mesh network, 678
mesh topology, 282
metadata, 678
Metasploit, 575, 678
MFA (multifactor authentication), 679
mice, 116
detachable, 253
microcontroller, 678
Microsoft Network Monitor, 572, 678
mid-tier servers, 678
MIT (Massachusetts Institute of Technology), 708
MITM (Man-in-the-Middle) attacks, 217, 395, 431, 604–605, 635, 678, 708
MMC (Microsoft Management Console), 617–618
monitoring systems, 12, 352–353
Nagios, 679
network, 680
unlocked conditions, 108
monitoring tools, 570–571
BeEF (Browser Exploitation Framework), 576
Metasploit, 575
Microsoft Network Monitor, 572
Nagios, 572
Nikto, 575
Nmap, 575, 576
OpenVAS, 575
packet analyzers, 571
Snort, 573–574
SolarWinds, 572
Wireshark, 572
monitors, 60, 116, 678
Thunderbolt Ports, 253
motion detectors, 93, 101, 679
locations, 81–82
PIR (passive infrared) detectors, 80–81
multicast messaging, 464–465, 627
multifactor authentication, 537–538
password management, 538–539

N
Nagios, 572, 679
name servers, 467
NAN (Neighborhood Area Network), 708
NAS (Network Attached Storage) servers, 330, 680, 708
NAT (Network Address Translation), 488, 633, 634, 679, 708
PAT (Port Address Translation), 489–490
PBR (policy-based routing), 488
native audit records, 679
NAT-T (Network Address Translation-Traversal), 490, 708
natural access control, 12, 107, 679
NBIDS (Network-Based IDS), 708
NBTSTAT, 314, 320
Need-to-Know policy, 679
NET VIEW, 314, 320–322
NETSTAT, 314, 318–320
network administrators, 427
AAA (Authentication, Authorization, Accounting), 331
CIA (confidentiality, integrity, availability), 331
responsibilities, 332
network analyzer, 679
network configuration operator account, Windows, 344
network connectivity, 385, 423
attacks
packet sniffing, 394–397
unnecessary, 393
bridges, 391
network protocols • networks

defenses, 397–398
devices, 679
exercises, 399–404
gateways, 390–391
routers, 388–390
switches
  command-line programming, 387
  MAC addresses, 386
  managed switches, 387
  OSI model, 386
  VLANs, 386–387
  web-browser-based interfaces, 387
vulnerabilities, 392–393
wireless networks, 392
network protocols, 297–298, 423–424
  BCP (Bridging Control Protocol), 301
  Ethernet, 309–310
  CSMA/CD, 309
  frame, 310–311
topologies, 311
  ICMP (Internet Control Message Protocol), 300–301
  MAC addresses, 298–299
  TCP/IP, 299–301
  IP addresses, 302–308
  vulnerabilities, 301–302
network security and Internet security, 458
  addresses, 679
  administrator, 679
  appliances, UTM devices, 519–520
  attacks
    broadcast storms, 603–604
    session hijacking, 604–606
  authentication, 347–348
  passwords, 348
  bridges, 429, 679
  CANs (campus/corporate area networks), 274
  client/server, 311, 659
    advantages, 312–313
    diskless workstations, 313
data transmission packets, 277–278
  DMZs (demilitarized zones), 522–523
dual-firewall, 524–525
  single-firewall, 523–524
  exercises, 283–296
  extranets, 526–527
  file system, 680
  firewalls, 242, 515, 680
    ICMP, 517–518
    proxy-filtering, 517
    QoS (Quality of Service), 517
    stateful packet-filtering firewalls, 516
    static packet-filtering firewalls, 516
  hardening, 398–399, 680
  honeypots, 525–526
  Hyper-V, 496
    compatibility, 497–498
    enabling, 498–499
    Linux distribution, 503–508
    Manager on taskbar, 500
    virtual switches, 500–503
  IPsec, 283–284
  LANs (local area networks), 273
  MANs (metropolitan area networks), 274
  mesh, 678
  messaging
    broadcast, 464–465
    multicast, 464–465
    unicast, 464–465
  monitoring, 634
  monitoring tools, 680
  OSI model, 423
    1 - physical layer, 276
    2 - data link layer, 276
    3 - network layer, 276
    4 - transport layer, 276
    5 - session layer, 276
    6 - presentation layer, 277
    7 - application layer, 277
  layers, 275
  security focus, 278–279
  overlay, 682
  packets, 299–300, 680
  SYN (Synchronize), 301
  SYN/ACK (Synchronize/Acknowledge), 301
PANs (personal area networks), 684
peer-to-peer, 311–312, 684
private, 487
DHCP (Dynamic Host Configuration Protocol) servers, 488
NAT, 488
port forwarding/mapping, 490–492
segmenting, 492–493
software-defined, 494–495
proxy servers, 520
distorting proxy, 521
reverse proxy server, 521
transparent proxy, 521, 629
public, 514
DMZ (demilitarized zone), 514
repeaters, 689
routers, 690
SANs (storage area networks), 274
segments, 680
servers (See servers)
topologies, 423, 680
bus, 280
logical, 282
mesh, 282
ring, 280–281
star, 281
user accounts, 341
administrator, 342
guest account, 342
HelpAssistant, 342
root, 342
SUPPORT_XXXXX, 342
utilities
ARP, 314, 318
IPCONFIG, 314
NBTSTAT, 314, 320
NET VIEW, 314, 320–322
NETSTAT, 314, 318–320
PING, 314
TRACERT, 314, 322–323
virtualization, 494
VLANs (virtual local area networks), 495
vulnerability scanners, 358–359
SNMP (Simple Network Management Protocol), 360–361
WANs (wide area networks), 273
wireless, 701
WLANs (wireless local area networks), 274
New Path Rule, 622–625
NFC (Near Field Communication), 708
NFS (network file system), 680
NIC (network interface adapter), 680
NIDS (network-based IDS), 209–210, 246
Nikto, 575, 680
NIST (National Institute of Standards and Technology), 3, 679, 708
controls, 252
NIST Cybersecurity Framework, 3–4, 715–725
Detect, 3
Identify, 3
Protect, 3
Recover, 3
Respond, 3
Nmap, 575, 576, 680
Nobody group (Linux), 346
nodes
bus topology, 280
peer-to-peer networks, 312
NOS (Network Operating Systems), 155, 680, 708
NS (Name Servers), 708
nslookup, 567
NTFS (New Technology File System), 161, 349–350
file creation, 190–191
folder creation, 190–191
permissions, 189, 681
creating, 191–194
NVT (Network Vulnerability Tests), 708
NX (No eXecution) bit, 157, 258, 681, 708

O

OAuth, 681
observations, recording, 4
OCIL (Open Checklist Interactive Language), 471, 681, 708
OCSP (Online Certificate Status Protocol), 708
octets, 681
Office 2013 software, 116
OPC (Open Platform Connectivity), 708
OpenBSD, 163
open/close conditions, 681
opened-condition/closed-condition
  monitoring, 30
  locked-condition, 31
  time-of-day, 31
  unlocked-condition, 31
  window sensors, 31
OpenVAS, 575, 681
Opera browser, 528–531
operators, 681
OS (operating system), 150–152, 681, 709
  Android, 166
    flash memory files, 167–168
  Apple
    iOS, 166
    MacOS, 165–166
attack areas, 155
  file management system, 157–159
  file system attacks, 159–160
  kernel, 156–157
client operating systems
  terminal clients, 154
  thick clients, 154
  thin clients, 154
directory traversals, 160
DOS (disk operating system), 152
  boot files, 152
  file management files, 152
  file structure, 153
  kernel files, 152
  utility files, 152
encryption
  asymmetric, 182
  cryptography, 182
  file-and-folder level, 187–188
  hardware-level, 183–185
  private key, 182
  public key, 182
  secret key, 182
  symmetric, 182
  TPM chips, 183–185
  TPM tools, 186
FMS (file management system), 150
hardening, 244
patches, 222–223
service packs, 222
updates, 223
kernel attacks, 156–157
Linux, 163–164
  distributions, 164
  encryption, 164–165
  file systems, 164
NOS (Network Operating Systems), 155
permissions, 158
position, 153
POSIX (Portable Operating System
  Interface), 158
security comparisons, 168–169
security steps, 169–170
  authentication, 176–177
  computer locking, 175–176
  local logins, 171–172
  passwords, 172–175
server operating systems, 155
  hardening, 336–338
standalone, 154
tools, administrative, 177–178
  auditing, 178–181
  event logging, 178–181
Unix, 162
  encryption, 163
  Free BSD kernel, 163
  GBDE, 163
  NFS, 162
  PEFS, 163
  UFS, 162
Windows, 160
  encryption, 161–162
  file system formats, 161
  grayware, 168
  packet filtering, 162
  versions, 161
OSI (Open Systems Interconnection) model,
  423, 681, 708
layers, 275
  1 - physical layer, 276
  2 - data link layer, 276
  3 - network layer, 276, 284
  4 - transport layer, 276
  5 - session layer, 276
6 - presentation layer, 277
7 - application layer, 277
network switches and, 386
security focus, 278–279
TCP/IP and, 461–462
OTP (One-Time Passwords), 709
outer perimeter security, 10–11, 243, 681
devices, 121
portals, 124–127
OSI Layer 1, 279
physical port access, 128–129
out-of-band, 681
output devices for intrusion-detection
remote notification, 89
sirens, 87–88
strobe lights, 88–89
third-party monitoring, 89–90
OVAL (Open Vulnerability and Assessment
Language), 471, 681, 709
overlay networks, 682
overview, camera viewpoint, 682
owners, 682
owning group, 682
owning user, 682

P
packet analyzers, 571, 578–579, 682
packet filtering, 162, 431, 489, 630, 682
stateful packet-filtering firewalls, 516
static packet-filtering firewalls, 516
packet sniffing attacks, 430, 542, 682
ARP (Address Resolution Protocol)
spoofing, 394
DoS (Denial-of-Service), 395–396
MAC cloning, 395
MAC flooding, 394
masquerade, 397
MITM (Man-in-the-Middle), 395
rerouting, 397
router flood attacks, 394
session replay, 397
spoofing, 395
switch port stealing, 395
packet-filtering firewall, 682
packets, 461, 463, 682
drawbacks, 463–464
pagers, 682
pairing, 682
PAKE (Password-Authentication Key
Agreement), 541, 631, 683, 709
panic buttons, 85
panning, 682
PANs (Personal Area Networks), 684, 709
PAP (Password Authentication Protocol),
539–540, 631, 683, 709
passageway, 682
passive controls, 682
passphrase, 683
passwords, 243, 245, 258, 260, 348, 683
attacks, 683
capturing, 683
CMOS access, 257
 cracking, 683
encryption, 683
encryption and, 542–543
local login requirements, 8:24–8:27
lockout, 258
managing, 538–539, 683
PAKE, 631
PAP (Password Authentication Protocol),
539–540
remote access and, 206
supervisory, 695
user passwords, 699
PAT (Port Address Translation), 283–284, 296,
489–490, 633, 634
Patch Tuesday, 591, 683
patches, 206, 222–223, 683, 691
applying, 224–225
PathPing, 569, 683
PBR (policy-based routing), 488, 633
PC (Personal Computer), 709
PCI-DSS (Payment Card Industry Data
Security Standard), 492–493, 683
peer-to-peer networks, 311–312, 684
PEFS (Private Encrypted File System), 709
perimeters, 10–11, 98, 451–455
exercises, 33–44
hardware, 512
inputs, 684
logical, 676
permissions, 158, 244, 684
allow, 193
deny, 193
explicit deny, 193
effective, 194
explicit, 194
files, 198–199
folders, 195–198
Linux, 349–350
NTFS, 189, 681
creating, 191–194
persistent cookies, 684
PF (packet filter), 709
PGP (Pretty Good Privacy), 685, 709
pharming, 684
phishing attacks, 600–603, 635, 684
 spear phishing, 693
photoelectric sensors, 110
PHP, software exploits and, 592–593
physical security, 10, 15–16, 97, 684
access-control systems, 12
authentication, 23–29
authorization, 13
ingress, 13
intruders, 13
regress, 13
rights, 13
key control policies, 17
keys, 16–17
deadbolts, 17–19
locks, 16–17
cipher, 19–20
ports, 128–129
zones, 101
physical-intrusion-detection system, 684
piconet, 684
PII (Personally Identifiable Information), 25
PIN (password or personal identification number), 709
PING, 314, 324–325, 567–568, 684
capture, 583–585
ping flood attack, 684
pinhole lens, 684
PIR (passive infrared) detector, 46, 682, 709
motion detectors, 80–81
PKE (Public Key Encryption), 687, 709
PKI (Public Key Infrastructure), 687, 709
PLCs (Programmable Logic Controllers), 122
Plug and Play devices, 429
plugins, 685
software exploits and, 592
PnP (plug and play), 709
PoE (Power over Ethernet), 685, 709
policies, 14–15, 107, 685
polynomial instantiation, 685
POODLE (Padding Oracle on Downgraded Legacy), 709
port forwarding/mapping, 490–492
port scanning, 489, 685
portal system, 685
ports, 128–129, 627
 blocking, 627
closing, 241
dynamic, 207
enabling, 135
eSATA, 132–133
FireWire, 132
hardware, 671
IANA (Internet Assigned Numbers Authority), 466
Internet protocols, 465–466
I/O, 208
IO port connectors, 134
legacy, 133–134
promiscuous, 686
registered, 207
USB (Universal Serial Bus), 130–132
uses, 466
VLANs, 685
well-known, 207
POS (Point of Sale), 685, 709
POSIX (Portable Operating System Interface), 158, 685, 709
possession, authentication and, 23
power user account, Windows, 344
PPP (Point-to-Point Protocol), 551, 634
PPTP (Point-to-Point Tunneling Protocol), 551, 634
PR (protect), 709
practices, 107
pressure mats, 685
prime number sieve, 615
principle of least privilege, 427
print servers, 330, 669
Privacy Rule, 686
private key encryption, 182, 543
private networks, 487
DHCP (Dynamic Host Configuration Protocol) servers, 488
NAT (Network Address Translation), 488
PAT (Port Address Translation), 489–490
port forwarding/mapping, 490–492
segmenting, 492–493
software-defined, 494–495
privileges
escalation, 428, 686
least privilege, 676
managing, 686
profile-based anomaly detection, 210–211, 686
programmable zone, 686
promiscuous mode, 685
promiscuous port, 686
Protect function (framework), 3
corporate facility scenario, 8
electrical substation scenario, 6
protocols, 686
AAA (Authentication, Authorization, Accounting), 651
authentication
CHAP, 540
CRAM, 541
Kerberos, 540–541
LDAP, 542
PAKE, 541
PAP, 539–540
RADIUS, 541
SRP, 541
Internet, ports, 465–466
L2TP, 634
network protocols, 297–298, 423–424
BCP (Bridging Control Protocol), 301
Ethernet, 309–311
ICMP (Internet Control Message Protocol), 300–301
MAC addresses, 298–299
TCP/IP, 299–308
routting, 690
STP (spanning-tree protocol), 604
proxies
anonymous, 653
distorting proxy, 664
transparent, 697
web proxies, 701
proxy servers, 329, 517, 520, 628, 629, 687
distorting proxy, 521
malicious, 629, 677
reverse proxy server, 521, 629, 689
transparent proxy, 521, 629
web proxies, 629
proxy-filtering firewalls, 517, 686
PSTN (public switched telephone network), 687, 709
psychological engineering, 687
PTZ (Pan/Tilt/Zoom), 709
public key certificates, 687
public key encryption, 182, 543, 631, 687
public networks, 514
DMZ (demilitarized zone), 514
public-key cryptography
authentication and, 543–544
DSS (Digital Signature Standard), 544
cryptography and, 543–544
GNU (GNU Privacy Guard), 544
PGP (Pretty Good Privacy), 544
RSA encryption algorithm, 544
S/MIME (Secure/Multipurpose Internet Mail Extensions), 544
SSH (Secure Shell), 544
SSL (Secure Sockets Layer), 544
TLS (Transport Layer Security), 544
purging, 687
PVLAN (Private VLAN) attacks, 686, 709
Q

QoS (Quality of Service), 687, 709
  exam questions, 647–650
  infrastructure security exam questions, 109–111
  review questions, 627–637, 644–647

R

race condition attack, 687
rack-mount server cabinet, 328
RADIUS (Remote Authentication Dial-In User Service), 541, 688, 710
rainbow tables, 688
ransomware, 219, 635
RARP (Reverse ARP), 710
RAS (Remote Access System) servers, 330
RAT (remote access Trojan), 710
RBAC (Role-Based Access Control), 157–158, 427, 689, 690, 710
  servers, 338–339
RC (recover), 710
RDC (Remote Desktop Connection), 688, 710
RDS (Remote Desktop Services), 688
Recover function (framework), 3
  corporate facility scenario, 8
  electrical substation scenario, 6
reed switches, 79
reflection servers, 688
registered ports, 207
regress, 688
relay operations, 22–23
remote access, 100, 203–204
  control, 688
  default features disable, 205
  firewalls, 204, 207–209
  intrusion-detection tools, 209–210
    anomaly detection, 210–211
  local protection tools, 206–209
  monitoring, 688
  nonessential services, 205
  patches, 206
  secure connections, 204
software
  anti-malware, 205
  exploitation, 223–224
  malicious, 218–222
  unnecessary, 205
  updates, 206
  web browser, 205
  web browsers, security configuration, 211–217
remote desktop users, Windows, 344
remote intrusion notification, 89, 100
remote monitoring, 100, 688
remote notification systems, 108, 688
remote-access monitoring, 29
  automated access control, 32–33
  opened-condition/closed-condition monitoring, 30
  locked-condition, 31
  time-of-day, 31
  unlocked-condition, 31
  window sensors, 31
remote-control access, 100, 688
remote-notification systems, 108
telephone dialers, 108
removable media, security, 135–137
repeaters, 689
replay attacks, 283–284, 295, 689
reporting systems, 12, 71–73. See also IDPS (Intrusion Detection and Prevention Systems)
rerouting attacks, 397, 431, 689
ResearchKit, 688
resolution, 689
Respond function (framework), 3
  corporate facility scenario, 8
  electrical substation scenario, 6
reverse proxy server, 629, 689
reverse-engineering, 591
review questions, 644–647
summary points, 627–637
RF (radio frequency), 407, 412, 710
RFCs (Requests for Comments), 470, 689, 710
RFID (radio frequency identification), 688, 710
  badges, 26, 69, 110
  tags, 651
    passive, 683
rights, 13, 98, 689
ring topology, 280–281, 689
RISC (Reduced Instruction Set Computing), 710
risk assessment, 689
device security, 117, 119
electrical substation scenario, 4–6
local security, 269–272
risk management, program development, 252
role-based access control, 437–438
root account, 342
root bridges, 604
Root group (Linux), 346
rootkits, 218–219, 689
router flood attacks, 394, 430, 689
router servers, 329
routers, 388–390, 429, 628, 690
routing, 466–467, 628, 690
domains, 467–468
NAT (Network Address Translation), 488
PBR (policy-based routing), 488
protocols, 690
table, 690
RS (respond), 710
RTU (Remote Telemetry Unit), 689
rule sets, 690
rule types, 622–626, 690
Rule-Based Access Control, 339
rule-based anomaly detection, 690

S
SA (Security Association), 710
SaaS (Software as a Service), 710
sanitization, 690
SANs (storage area networks), 274
servers, 330, 694, 710
SAs (Security Associations), 283–284, 296, 551, 691
SATA (Serial AT Attachment), 710
SBS (Small Business Server), 710
SCAP (Security Content Automation Protocol), 470, 471, 691
scenario review, 637–644
SCP (Secure Copy Protocol), 710
script kiddies, 607
scripts, 247, 690
ActiveX, 214–215
cookies
attributes, 216
HTTP transfer, 215–216
persistent cookies, 216
poisoning, 217
session cookies, 216
theft, 216
JavaScript, 214
VBScript, 215
XSS (cross-site scripting), 216, 483
SDN (software-defined networking), 693, 710
SDO (Standards Development Organization), 710
secret key encryption, 182
security, 97
authorization, 13
baseline, 691
challenge, 432–443
cybersecurity, 10
guards, 15
infrastructure, 672
access-control systems, 12
intrusion-detection systems, 12
monitoring systems, 12
natural access control, 12
overview, 9–10
physical, 10
reporting systems, 12
territorial reinforcement, 12
video surveillance systems, 12
intruders, 13
physical, 10
policies, 14–15, 99, 691
rights, 13
security hardware, 253
security software, 253
strategies, 105
zones, 74–77
segments, 461, 463, 632
private networks, 492–493
segregation, 691
sensors, 100
carbon dioxide ($\text{CO}_2$) detectors, 86–87
carbon monoxide (CO) detectors, 86–87
fire detection, 669
  heat sensors, 85–86
  smoke detectors, 85–86
intrusion-detection systems, 77–79
  glass breakage, 80
  magnetic contact switches, 79–80
  motion detectors, 80–82
  security zones, 75
microwave beam, 83
photoelectric beam, 82–83, 110
pressure sensors, 84
server administrator, 692
server operating systems, 155
server racks, 328
  locks, 333, 335
server rooms, 691
servers, 327–328, 425, 691
  access, physical, 332–333
  door locks, 333
  rack locks, 333, 335
access control
  automated provisioning, 339
  DAC (Discretionary Access Control), 338–339
  MAC (Mandatory Access Control), 338–339
  RBAC (Role-Based Access Control), 338–339
  Rule-Based Access Control, 339
appliance servers, 329
application servers, 329
auditing, 331, 352–354
authentication and, 331
backups, 354–356
  media security, 356
bridge servers, 329
database servers, 329
DHCP (Dynamic Host Configuration Protocol) servers, 330
DNS (Domain Name Service), 329
domain accounts, 344–345
e-mail servers, 666
event logging, 352–354
exercises, 361–382
file servers, 669
firewall servers, 329
FTP servers, 330
gateway servers, 329
IDS (intrusion detection systems), distributed, 357–358
mail servers, 329
name servers, 467
NAS (Network Attached Storage) servers, 330
network, 680
operating systems, hardening, 336–338
print servers, 330, 669
proxy servers, 329, 520–522, 687
  distorting proxy, 521
  reverse proxy server, 521
  transparent proxy, 521, 629
RAS (Remote Access System) servers, 330
reflection servers, 688
resource controls, 348
  Linux permissions, 350–352
  NTFS file management, 349–350
router servers, 329
  routers, 331
SAN (Storage Area Network) servers, 330
server racks, 328
  locks, 333, 335
services, default, 337
shared resources, 331, 426
software security, 335–341
subnets, 331
terminal servers, 329
terminal servers, 329
web servers, 329, 701
service packs, 222, 692
services, well-known, 207
session cookies, 692
session hijacking, 635
  clickjacking attacks, 605–606
  MITM (man-in-the-middle) attacks, 604–605
session replay attacks, 397, 431, 692
SET (Social Engineering Toolkit), 693, 710
SFTP (SSH File Transfer Protocol), 710
side channel attacks, 692
signature analysis, 692
signature-based IDS/IDPS, 247, 692
SilQ (Silicon Intelligence), 710
single authentication, 692
single firewall DMZ, 692
single point of failure, 512
single-factor authentication, 537, 630
single-firewall DMZ, 523–524
sirens, 87–90, 692
SLE (Single Loss Expectancy), 710
sliding gates, 20
smart cards, 25–26, 692
smart network appliances, 630
smart phone applications, 692
smart switches, 630
SMB (Server Message Block), 691
SMBFS (Server Message Block File System), 710
smoke detectors, 85–86
SMTP (Simple Mail Transfer Protocol), 462–463, 711
Smurf attacks, 636, 692
SNMP (Simple Network Management Protocol), 711
network switches and, 387
Snort, 573–574, 693
Snort IDS
configuration file, 362–377
running, 378–382
social engineering exploits, 635, 693
phishing attacks, 600–603
sockets, 693
soft targets, 693
softphone, 693
software
antispyware, 221–222
antivirus programs, 220–221, 256
exploitation, 223–224, 248
exploits, 693 (See also vulnerabilities)
anti-malware and, 599
antivirus and, 599
exercises, 616–626
Flash and, 593
FREAK exploits, 615
Java, 597–599
LDAP attacks, 597
logjam attacks, 615
networks, session hijacking, 604–606
PHP and, 592–593
plugins and, 592
social engineering, phishing attacks, 600–603
SQL injection, 594–597
TLS (Transport Layer Security) exploits, 614–615
firewalls, 261, 693
malware
adware, 219
botnets, 220
logic bombs, 219–220
ransomware, 219
rootkits, 218–219
spyware, 219, 221–222
Trojans, 218
viruses, 218
worms, 218
zombies, 220
security software, 253
software-defined networks, 494–495
SOHO (small office/home office), 490
SolarWinds, 572, 693
solenoid-operated deadbolts, 18–19
spam, 612
authentication and, 613
e-mail blacklists, 614
notification for e-mail volumes, 613
outgoing recipient limits, 613
webmail server restrictions, 613–614
spammers, 637
spanning-tree attack, 693
SPDT (single-pole, single-throw) relay, 21
spear phishing attacks, 602–603, 635, 693
spoofing attacks, 395, 431, 694
ARP, 652
IP addresses, 674
spyware, 219, 221–222, 247, 694
SQL injection attacks, 594–597, 635, 694
SQLi (SQL injection), 711
SRK (Storage Root Key), 711
SRP (Secure Remote Password), 541, 690, 711
SSH (Secure Shell), 570, 690, 711
SSH tunneling, 492, 694
SSL (secure socket links), 258, 632, 691, 711
cookies, 217
SSL (Secure Sockets Layer), digital certificates and, 547
SSO (Single Sign-On), 711
STA (Spanning Tree Algorithm), 711
standalone operating systems, 154
star topology, 281, 694
stateful packet-filtering firewalls, 516, 634, 694
stateless packet-filtering firewalls, 694
static packet-filtering firewalls, 516
sticky honeypot, 611–612
storage, video recorders, 57
DAS (direct-attached storage), 58
NAS (Network Attached Storage), 58
SAN (Storage Area Network), 58
STP (Shielded Twisted Pair), 711
STP (spanning-tree protocol), 604, 693
stream cipher, 694
strobe lights, 88–89
subnet, 694
super cookies, 548, 632, 694
supervisory passwords, 695
suPHP, 695
SUPPORT_XXXXX account, 342
surveillance systems, video, 45–46
 cameras, 46–60
swinging gates, 21
switch port stealing attacks, 395, 695
switch-based virtualization, 695
switchers, 59–60
switches, 429, 695
 command-line programming, 387
 MAC addresses, 386
 managed switches, 387, 678
 managed switches, 429
OSI model, 386
unmanaged, 429
VLANs, 386–387
web-browser-based interfaces, 387
switch-port-stealing attacks, 430
symmetric encryption, 182, 695
symmetric key cryptography
3DES, 544
AES (Advanced Encryption Standard), 544
Blowfish, 544
RC4, 544
shared secrets, 544
SYN (Synchronize) flood, 424, 695, 711
SYN (Synchronize) packet, 301
SYN/ACK (Synchronize/Acknowledge) packet, 301, 711
tarpitting and, 611
system hardening, 127
T
tagged packet, 695
tangible assets, 695
tangible property security, 695
target sets, 104
tarpitting, 611–612, 637
TCP (Transmission Control Protocol), 627, 711
TCP outbound rules, 230–234
TCP packets, 569
TCP segment, 695
TCP window size, 695
TCP/IP (Transmission Control Protocol/Internet Protocol), 299–301, 695, 711
datagrams, 461
headers, 463
 window size, 464
Internet and, 461
IP addresses, 302–308
IPv4, 302–303
IPv6, 306–307
private classes, 307–308
subnets, 303–305
IP spoofing, 301
layers
  application layer, 461
  Internet layer, 461
  link layer, 461
  transport layer, 461
network packets, 299–300
  SYN, 301
  SYN/ACK, 301
OSI model and, 461–462
packets, 461, 463
drawbacks, 463–464
segments, 461
UDP (User Datagram Protocol), 462
  latency, 464
vulnerabilities, 301–302
tear drop attack, 636, 696
telephone dialers, 108
telephoto lens, 696
Telnet, 569–570, 696
terminal servers, 329
territorial reinforcement, 12, 108, 696
TGS (Ticket Granting Server), 631, 711
  Kerberos and, 540–541
third-party monitoring, 89–90
threat agent, 696
threat vector, 696
threat-informed pyramid, 104–105
threats, 696
defined threat environment, 105
threshold-based anomaly detection, 211, 696
time-of-day settings, 696
TKIP (Temporary Key Integrity Protocol), 416, 711
TLD (top-level domain), 467–468, 696, 711
TLS (Transport Layer Security), 632, 697, 711
digital certificates and, 547–548
TO (Transmission Owner), 711
TOCTOU (time of check or time of use), 696, 711
tools
  administrative, 652
  command line
    ifconfig, 565
    ipconfig, 565
nslookup, 567
whois, 566–567
Core Impact, 576
monitoring, 570–571
BeEF (Browser Exploitation Framework), 576
Metasploit, 575, 577
Microsoft Network Monitor, 572
Nagios, 572
Nikto, 575
Nmap, 575, 576
OpenVAS, 575
packet analyzers, 571, 578–579
Snort, 573–574
SolarWinds, 572
Wireshark, 572
Nessus, 576
Netscout, 576
Nexpose, 576
protocols
  SSH (Secure Shell), 570
  Telnet, 569–570
TOP (Transmission Operator), 711
top secret, 697
topologies, 423, 680, 684, 697
  bus, 657
  Ethernet, 311
  networks
    bus, 280
    logical, 282
    mesh, 282
    ring, 280–281
    star, 281
    ring, 689
    star, 694
TOU (time of use), 696, 711
TPID (Tag Protocol Identifier), 711
TPM (Trusted Platform Module), 183–185, 246, 712
  BitLocker utility, 186
TRACEROUTE, 568–569, 697
TRACERT, 314, 322–323
tracking cookies, 697
transmission media
bandwidth, 408
cabling, 407
copper wire, 407
coaxial cabling, 409–410
twisted-pair cabling, 408–409
exercises, 417–421
infrared light, 407
light waves, 407
fiber optics, 410–411
physical security, 415–416
wireless signals
  Bluetooth, 407, 412–414
  physical security, 415–416
  RF (radio frequency), 412
  RF (radio frequency) signals, 407
  Wi-Fi, 407, 412
  WiMAX, 407, 414
ZigBee, 407
Z-Wave, 407
transparent proxies, 697
Triple DES, 651
Trojans, 218, 697
TrouSerS, 697
trick, 697
Trusted VPNs, 697
TrustedGrub, 697
TTL (Time-To-Live), 712
tunneling, 697
twisted-pair cabling, 311, 408–409
two-factor authentication, 99, 630, 698
two-man control, 698

U

UDF (Universal Disk Format), 161, 698
UDP (User Datagram Protocol), 462, 627, 712
  DNS (Domain Name System) lookups, 464
  flood attack, 698
  latency, 464
  RTSP (Real Time Streaming Protocol), 464
  TFTP (Trivial File Transfer Protocol), 464
UETA (Uniform Electronic Transactions Act), 712
UL (Underwriters Laboratories), 712
unauthorized access, 698
unicast messaging, 464–465, 627, 698
unidirectional security gateways, 698
Unix, 698
  access rights, 244
  encryption, 163
  file system, 699
  Free BSD kernel, 163
  GBDE (GEOM Based Disk Encryption), 163
  NFS (Network File System), 162
  PEFS (Private Encrypted File System), 163
  UFS (UNIX File System), 162
unlocked condition monitoring, 108, 699
unmanaged switches, 429, 699
untagged packet, 699
updates, 206, 223, 699
  applying, 224–225
UPnP (Universal Plug and Play), 518, 698, 699, 712
upstream interface, 698
USB (Universal Serial Bus), 698, 712
  connection ports, 116
    built-in, 253
    locks, 250
  connectors, 130–132
  ports, 130–132
user accounts, 341, 427
  administrator, 342
  guest account, 342
  HelpAssistant, 342
  root, 342
  SUPPORT_XXXXX, 342
user credentials, 258
user passwords, 699
users, Windows, 344
Users group (Linux), 345
utilities
  crypt, 661
  networks
    ARP, 318
    IPCONFIG, 316–317
    NBTSTAT, 320
virtual VLANs, 700
virtualization, 494, 633, 680
    appliance-based, 653
    switch-based, 695
viruses, 218, 628, 700
VLANs (virtual local area networks), 495, 633, 712
    double encapsulation VLAN hopping attack, 665
    hopping attacks, 700
    network switches, 386–387
    port-based, 685
    Trunking Protocol attacks, 700
    virtual, 700
VMD (Video Motion Detection), 712
VMPS (VLAN Management Policy Server), 700, 712
VNA (vendor neutral archive), 712
voice recognition, 700
VoIP (Voice over Internet Protocol), 513, 712
VPLS (Virtual Private LAN Service), 712
VPNs (virtual private networks), 550, 634, 700
    exercises, 528–533
    IPsec
        AH, 551
        ESP, 551
        IKE, 551
        SAs, 551
    PPP (Point-to-Point Protocol), 551, 634
    PPTP (Point-to-Point Tunneling Protocol), 551, 634
    secure, 551
    trusted, 551, 697
VQP (VLAN Query Protocol), 712
VTP (VLAN Trunking Protocol), 712
vulnerabilities, 700. See also software exploits
data, 257
devices, 251
dictionary attacks, 606
DoS (denial-of-service) attacks, 606–611
    DDoS attack, 609–610
    sticky honeypot, 611–612
tarpitting, 611–612
Java, 597–599
LDAP attacks, 597
networks
  broadcast storms, 603–604
  session hijacking, 604–606
Patch Tuesday, 591
programs, 257
scanners, 358–359, 428
  SNMP (Simple Network Management Protocol), 360–361
social engineering exploits, 600–603
software exploits, 592–594
spam, 612
  protections, 613–614
WordPress and, 592
XSS (cross-scripting) attacks, 597
  zero day, 591–592
vulnerability emulators, 701
vulnerability scanner, 680, 701

W
WANs (wide area networks), 273, 701, 712
WAP (wireless access point), 392, 701, 712
WBAN (Wireless Body-Area Network), 712
web browser, 211–212, 701
scripts
  ActiveX, 214–215
  cookies, 215–217
  JavaScript, 214
  VBScript, 215
  XSS (cross-site scripting), 216, 483
securing, 205
security levels, 213–214
SSL, 258
  zones, 213–214
web proxies, 629, 701
web servers, 329, 701
web-browser-based interfaces, network
  switches and, 387
well-known ports, 207
WEP (Wired Equivalent Privacy), 415, 428, 701, 712
Wheel group (Linux), 345
white hat hackers, 224
whitelisting, 493, 632, 701
whois, 566–567
wide angle lens, 701
Wi-Fi (wireless fidelity), 407, 412, 701, 712
WiGLE, 701
WiMAX, 407, 414, 701
Windows, 160–161
  auditing, 178–180
  BitLocker, 162
  domain accounts, 344–345
  EFS (encrypting file system), 161–162
  file system formats
    CDFS (Compact Disc File System), 161
    FAT/FAT16/FAT32, 161
    NTFS, 161
    UDF (Universal Disk Format), 161
grayware, 168
  group accounts
    administrators, 343
    backup operators, 344
    guests, 344
    network configuration operators, 344
    power users, 344
    remote desktop users, 344
    users, 344
  packet filtering, 162
Windows 7 Pro operating systems, 116
wireless networks, 392, 701
  physical security, 415–416
wireless RF, 311
wireless signals
  Bluetooth, 412–414
  RF (radio frequency), 412
  Wi-Fi, 412
  WiMAX, 414
Wireshark, 572, 702
  attacks and, 585–588
  launch, 579–583
WLANs (wireless local area networks), 274, 713
WordPress, 592
workstations, client/server networks, 313
worms, 218, 702
WPA (WiFi Protected Access), 416, 428, 713
WSDL (Web Services Description Language), 713

X

XD (eXecute Disable) bit, 157, 258, 667, 713
XN (Execute Never), 713
XSS (cross-site scripting), 216, 483, 597, 598, 661, 713

Z

zero day vulnerabilities, 591–592, 634, 702
Z-Force, 702
ZigBee, 407, 414, 702
ZigBee Alliance, 702
zombies, 220, 657, 702
zoning, private networks, 492–493
zooming, 702
Z-Wave, 407, 702