

3DES, 46
802.1x limited access enforcement, 99

A

Access control, 9–10
Access control list (ACL), 34
Accounting, definition of, 20
Account lockout
 definition of, 71
 settings, 76–77
Active Directory
 definition of, 25
 domain controllers, 25–26
 groups, 31–33
 Kerberos, 26–27
 multimaster replication, 26
 network services, 25
 NTLM, 26
 objects, 28–33
 organizational units, 27–28
 schema, 29
 web server authentication, 33–34
Active Directory Administrative Center, 26
Active Directory Domains and Trusts, 26
Active Directory Sites and Services, 26
Active Directory Users and Computers, 25
ADMIN\$, 42
Administrative share, 42
Advanced Encryption Standard (AES), 46
Adware, 135
AES ciphers, 46
AGDLP, 32–33
AGUDLP, 33
Application attack surface, 7
Application layer (four-layer model), 92
Application layer (layer 7), 92
Application-level firewall, 94.
 See also Firewall
Applications, third-party, 6
ARP spoofing, 119
Asymmetric encryption, 46
Attack methods
 network, 121–123
 password, 80–82
Attack surface
 application, 7
 components of, 6–7
 definition of, 6
 employee, 7
 network, 7

Auditing
 auditors, 63
 change management system, 63
 definition of, 20, 60
 enabling, 61–62
 files and folders, 63
 site security, 10
 Syslog, 62
 ticket system, 63
 user account, 29
Authentication
 anonymous, 33
 basic, 33
 biometrics, 22–23
 Client Certificate Mapping, 34
 definition of, 20
 digest, 34
 digital certificates, 22
 IEEE 802.1x process, 125–126
 Integrated Windows, 34
 methods, 20–24
 multifactor, 21
 Network Access Protection (NAP), 99
 passwords, 21–22
 personal identification numbers (PINs), 22
 RADIUS, 23–24
 run as administrator, 24
 security tokens, 22
 site security, 10
 smart cards, 22
 TACACS+, 23–24
 VPNs, 59
 web server, 33–34
Authentic Header (AH), 58, 114
Authorization
 definition of, 20
 Network Access Protection (NAP), 99
Availability, 3

B

Backdoor, 135
Back door attack, 122
Base64-encoded X.509, 48
Bayesian filters, 149
Biometrics, 22–23
BitLocker
 data recovery agents, 56–57
 versus EFS, 51
 enabling, 55–56
 modes, 54–55

 system requirements of, 54
 TPM, determining whether you have it, 55
 turning on, 55–56
BitLocker To Go, 57
Block cipher, 46
Brute force attack, 21, 45, 46, 80
Buffering, 91
Buffer overflow attack, 123, 135
Built-in groups, 33

C

Caching, 94
Certificate authority (CA), 47, 49
Certificate chain, 49–50
Certificate revocation list (CRL), 47
Challenge Handshake Authentication Protocol (CHAP), 59
Circuit-level firewall, 94. *See also* Firewall
Client computers
 locking down, 147
 malware, protecting from, 134–138
 offline files, 146–147
 User Account Control (UAC), 140–143
 Windows Firewall, 143–147
 Windows Update, 138–140
Computer accounts, 31
Computers, types, 12
Computer security
 keyloggers, 14–15
 mobile devices, 12–13
 removable devices and drives, 13–14
Confidentiality
 data classifications, 2–3
 definition of, 2
 technologies that support, 2
Connectionless protocol, 91
Connection oriented protocol, 91
Content zones, 152
Cookie
 definition of, 149
 deleting, 149–150
Cracked password, 81
Cross-site scripting attack, 123
Cryptographic Message Syntax Standard (PKCS #7), 48

D

Data Encryption Standard (DES), 46
Data link layer (layer 2), 90
Data packet inspection
 stateful, 96–97
 stateless, 96

- Data recovery agents
 - BitLocker, 56–57
 - Encrypting File System, 53
 - Decryption, 44
 - Defense in depth, 8, 9–10
 - Demilitarized zone. *See* DMZ
 - Denial of service/distributed denial of service (DoS/DDoS) attacks, 121
 - DER-encoded binary X.509, 48
 - Desktop computers, 12
 - DHCP limited access enforcement, 100
 - Dictionary attack, 21, 80
 - Digital certificate
 - acquiring, 48–59
 - authentication, 22
 - definition of, 48
 - exporting, 49
 - formats, 48
 - importing, 49
 - Public Key Infrastructure (PKI), 47–49
 - X.509 version 3, 48
 - Digital signature, 50
 - Distance vector-based routing protocol, 105–106
 - DMZ
 - definition of, 109
 - sandwich, 110
 - services and servers found on, 111
 - single firewall, 110
 - DNS poisoning, 122
 - DNS Security Extensions (DNSSEC), 118–119
 - DNS spoofing, 119
 - Docking stations, 13
 - Domain controller
 - definition of, 25
 - Microsoft management console (MMC) snap-ins, 25–26
 - Domain local group scope, 32
 - Domain user, 29–30
 - Drives and folders, sharing, 40–42
 - Dynamic DNS, 157
 - Dynamic NAT, 112
- E**
- Effective permissions, 36–39
 - E-mail
 - address honeypot, 109
 - encryption, 51
 - open relay honeypot, 109
 - relaying, 149
 - relay servers, 111
 - social engineering, 7
 - spam, 147, 148–149
 - Employee attack surface, 7
 - Encapsulating Security Payload (ESP), 58, 114
 - Encrypting File System (EFS)
 - versus BitLocker, 51
 - certificate, backing up, 53
 - folder or file, decrypting, 52
 - folder or file, encrypting, 52
 - recovery agents, adding users as, 53
- Encryption**
- algorithm, 45
 - asymmetric, 46
 - definition of, 44
 - disks, in Windows, 54–57 (*see also* BitLocker)
 - email, 51
 - files, with EFS, 51–53
 - hash function, 46
 - keys, weak, 122
 - symmetric, 45–46
 - types, 45–46
 - with VPN technology, 58–60
- Error checking, 90**
- Espionage, 14**
- Explicit permissions, 36–38**
- Extensible Authentication Protocol**
- Microsoft CHAP version 2 (EAP-MS-CHAPv2), 59
- External perimeter security, 10, 11**
- F**
- FAT16, 35
 - FAT32, 35
 - Federal Information Processing Standard (FIPS), 46
- Files**
- auditing, 63
 - copying and moving, 39
 - decrypting or encrypting, 52
 - ownership, taking, 40
- File systems**
- FAT16, 35
 - FAT32, 35
 - NTFS, 35–39
- Firewall**
- application level, 94
 - circuit level, 94
 - definition of, 88
 - hardware, 92–95
 - hardware versus software, 95–96
 - host, 95
 - network, 95
 - packet filtering, 93, 96
 - personal, 95
 - Secure Content Management (SCM) appliance, 95
 - stateful multilevel, 94
 - stateful versus stateless inspection, 96–97
 - Unified Threat Management (UTM), 95
- Flash drive, 14**
- Flow control methods, 91**
- Folders**
- auditing, 63
 - decrypting or encrypting, 52
 - ownership, taking, 40
 - sharing, 40–41

- G**
- Generic Routing Encapsulation (GRE), 118
 - Global group scope, 32
 - Globally unique identifier (GUID), 28
 - Group Policy Management Console (GPMC), 26
 - Group Policy Object (GPO), 77
- Groups**
- Active Directory, 31–33
 - built-in, 33
 - definition of, 6, 31
 - distribution, 31
 - objects, 31–33
 - rights and permissions, assigning, 6, 32–33, 36
 - scopes, 32–33
 - security, 31
 - types, 31
- H**
- Hardware firewalls versus software firewalls, 95–96
 - Hardware routers versus software routers, 103–104
 - Hash function, 46, 50
 - Health policy servers, 99
 - HKEY_CLASSES_ROOT, 43
 - HKEY_CURRENT_CONFIG, 43
 - HKEY_CURRENT_USER, 43
 - HKEY_LOCAL_MACHINE, 43
 - HKEY_USERS, 43
 - Honey net, 108
 - Honeypot
 - definition of, 108
 - email address, 109
 - email open relay, 109
 - production, 108
 - research, 108
 - spam, used to combat, 109
 - types, 108–109
 - Host-based IDS (HIDS), 107
 - Host firewall, 95. *See also* Firewall
 - HTTPS, 114
- I**
- IEEE 802.1x, 125–126
 - Inherited permissions, 36–37
 - Inspection, stateful versus stateless, 96–97
 - Integrity, 3
 - Internal perimeter security, 10–11
 - Internet Explorer
 - content zones, 152–154
 - cookies, 149–150
 - phishing and pharming, 154–155
 - pop-up blocker, 151–152
 - privacy settings, 150–151
 - security levels, 153
 - web content zone, 152–153
 - Internet Information Server (IIS), 33

- Internet Key Exchange (IKE), 114
- Internet Key Exchange version 2 (IKEv2), 59
- Internet layer, 92
- Intrusion detection system (IDS), 107–108
- Intrusion prevention system (IPS), 107–108
- IP address spoofing, 120, 121–122
- IPC\$, 42
- IP Security (IPsec)
 - components, 114
 - definition of, 57, 113
 - limited access enforcement, 99
 - protocols, 58
 - modes, 57, 114, 117
 - security services, 113–114
 - versus SSL/TLS, 115
 - transport mode, 57, 114, 117
 - tunnel mode, 57, 114, 117
 - Windows, 58
- Isolation
 - DMZs, 109–111
 - honeypots, 108–109
 - intrusion detection systems (IDSs), 107–108
 - intrusion prevention systems (IPSs), 107–108
 - IPsec, 113–114
 - Network Address Translation (NAT), 111–112
 - routing, 102–107
 - server and domain, 116–117
 - VLANs, 101–102
 - VPN protocols, 114–116
 - VPNs, 112–113
- K**
- Kerberos, 25, 26–27
- Key
 - based security mechanisms, 125–126
 - definition of, 45
 - Registry, 43
 - weak encryption, 122
 - wireless LAN, 125–126
- Keylogger
 - computer security, 14–15
 - definition of, 14, 80
 - physical, protection against, 15
 - software, protection against, 15
- L**
- Laptop, security, 13
- Layer 2 Tunneling Protocol (L2TP), 58, 118
- Lightweight Directory Access Protocol (LDAP), 25
- Link layer, 92
- Link state routing protocol, 106–107
- Local area network (LAN), 101
- Local user account, 29
- Logical Link Control (LLC) sublayer, 90
- Loss, 14
- M**
- MAC address, 90
- MAC filter, 126
- Malicious software, 134. *See also* Malware
- Malware
 - identifying, 135–136
 - precautions against, 136–137
 - removing, 137–138
 - security updates, 136
 - types, 134–135
 - Windows Defender, 136
- Man in the middle attacks, 122
- Media Access Control (MAC) sublayer, 90
- Member server, 26
- Microsoft Baseline Security Analyzer (MBSA), 156
- Microsoft CHAP version 2 (MS_CHAPv2), 59
- Mobile computers, 12
- Mobile devices
 - definition of, 12
 - security, 12–13
- Multifactor authentication, 21
- N**
- Network Access Protection (NAP)
 - authentication, 99
 - authorization, 99
 - definition of, 97
 - health policy compliance, 97
 - health policy servers, 99
 - health state validation, 97
 - how it works, 98–100
 - limited access mode, 98
 - purpose of, 97–98
 - remediation servers, 100
 - requirements for, 100–101
 - versus server and domain isolation, 116
 - system health agents, 98
 - system health validators, 98
- Network Address Translation (NAT)
 - definition of, 111
 - dynamic, 112
 - security implications, 112
 - static, 112
 - uses for, 112
- Network attack methods, 121–123
- Network attack surface, 7
- Network-based IDS (NIDS), 107
- Network firewall, 95. *See also* Firewall
- Network layer (layer 3), 90
- Network security
 - firewalls, dedicated, 88–97
 - isolation, 101–117
 - Network Access Protection (NAP), 97–101
 - protocol security, 117–123
 - wireless, 123–127
- Network sniffing, 120–121
- Nonrepudiation, 20
- NTFS
 - definition of, 35
 - effective permissions, 36–39
 - explicit permissions, 36–37
 - inherited permissions, 36–37
 - permissions, 35–36, 41
 - permission types, 36
- NTLM, 26
- O**
- Objects
 - Active Directory, 28–33
 - computers, 31
 - globally unique identifier (GUID), 28
 - groups, 31–33
 - users, 29–30
- Offline files, 146–147
- Open Systems Interconnect (OSI) model
 - application layer (layer 7), 92
 - data link layer (layer 2), 90
 - definition of, 89
 - network layer (layer 3), 90
 - physical layer (layer 1), 89
 - presentation layer (layer 6), 91
 - session layer (layer 5), 91
 - transport layer (layer 4), 90–91
- Organizational units
 - Active Directory, 27–28
 - definition of, 27
 - delegate control, 28
- OSI model. *See* Open Systems Interconnect (OSI) model
- Owner, definition of, 39
- Ownership, file and folder, taking 40
- P**
- Packet filtering, 93, 96
- Padded cell, 108
- Password(s)
 - account lockout, 71
 - authentication, 21–22
 - complexity, 21, 70
 - controls, using a default domain policy to enforce, 78–80
 - controls, using a Group Policy to enforce, 78
 - cracked, 81
 - definition of, 21, 69
 - guessed, 82
 - history, 71
 - leaked, 81
 - length, 71
 - maximum age, 72
 - minimum age, 72
 - settings, reviewing, 72–77
 - shared, 81
 - strength, 70
 - time between changes, 72

- Password attack methods, 80–82
 - Password Authentication Protocol (PAP), 59
 - Password security, 21–22
 - Patch Tuesday, 139
 - PDC Emulator, 26
 - Permissions
 - definition of, 34
 - effective, 36–39
 - explicit versus inherited, 36–38
 - files, copying and moving, 39
 - files or folders, ownership, taking, 40
 - groups, 6, 36
 - hierarchy of precedence, 37
 - inherited, 36–37
 - NTFS, 35–36
 - principle of least privilege, 5–6
 - Registry, 44
 - versus rights, 34
 - share, 41
 - viewing, 37
 - Personal digital assistants (PDAs), 12, 13
 - Personal firewall, 95. *See also* Firewall
 - Personal identification number (PIN), 22
 - Personal Information Exchange (PKCS #12), 48
 - Pharming, 155
 - Phishing, 154
 - Physical attacks, 80
 - Physical layer (layer 1), 89
 - Physical security
 - computer, 12–15
 - site, 9–11
 - Point-to-Point Tunneling Protocol (PPTP), 58, 118
 - Pop-up blocker, 151–152
 - Pop-up window, 151
 - Portable devices. *See* Removable devices and drives
 - Presentation layer (layer 6), 91
 - Pretty Good Privacy (PGP), 51
 - Principle of least privilege, 5–6, 14
 - PRINT\$, 42
 - Protocols and ports, 93
 - Protocol security
 - DNS security extensions (DNSSEC), 118–119
 - spoofing, 119–120
 - tunneling, 118
 - Proxy servers, 94, 111
 - Public key infrastructure (PKI)
 - certificate authority (CA), 47
 - certificate chain, 49–50
 - definition of, 47
 - digital certificates, 47–49
 - digital signature, 50
 - registration authority (RA), 47
 - Secure Sockets Layer (SSL), 50–51
 - Transport Layer Security (TLS), 51
- R**
- RADIUS, 23–24, 99
 - RC4, 46
 - Recovery agents, adding users as, 53
 - Registration authority (RA), 47
 - Registry
 - definition of, 42
 - hives, 43
 - keys, 43
 - key types, 44
 - permissions, 44
 - Remote access, VPNs, 113, 115
 - Remote code execution attack, 123
 - Removable devices and drives
 - definition, 14
 - security, 13–14
 - Replay attack, 122
 - Replication, multimaster, 26
 - Residual risk, 5
 - Reverse proxy servers, 111
 - Rights
 - definition of, 34
 - groups, assigning, 32–33
 - versus permissions, 34
 - Risk
 - acceptance, 4–5
 - assessment, 3
 - avoidance, 4
 - definition of, 3
 - management, 3–5
 - matrix, 4
 - mitigation, 5
 - transfer, 5
 - Rootkit, 135
 - Routers, hardware versus software, 103–104
 - Routing
 - count to infinity issues, 106
 - definition of, 103
 - distance vector-based protocol, 105–106
 - how it works, 104–105
 - isolation, 102–107
 - link state protocol, 106–107
 - protocols, 105–107
 - network layer, 102–103
 - Run as, 24
- S**
- Sandwich DMZ, 110
 - Scope, group, 32–33. *See also* Groups
 - Secure areas, defining, 11
 - Secure Content Management (SCM)
 - appliance, 95
 - Secure Dynamic DNS, 157
 - Secure Multipurpose Internet Mail Extension (S/MIME), 51
 - Secure Shell (SSH), 115–116
 - Secure Sockets Layer (SSL)
 - versus IPsec VPNs, 115
 - Public Key Infrastructure (PKI), 50–51
 - VPN protocol, 114–115
 - Secure Sockets Tunneling Protocol (SSTP), 59
 - Security Account Manager (SAM), 29
 - Security Association (SA), 58
 - Segmentation, 90
 - Sender Policy Framework (SPF), 149
 - Servers
 - computer security, 12
 - definition of, 12
 - hardening, 155–157
 - placement, 155
 - Secure dynamic DNS, 157
 - Service addressing, 90
 - Service Set Identifier (SSID), 124–125
 - Session layer (layer 5), 91
 - Shared folder, 40–41
 - Shared-key WPA, 125
 - Share permissions, 41
 - Simple Mail Transfer Protocol (SMTP), 149
 - Single firewall DMZ, 110
 - Single sign-on (SSO), 25
 - Site security
 - access control, 9–11
 - auditing and authentication, 10
 - external perimeter, 10, 11
 - internal perimeter, 10–11
 - processes, 11
 - secure areas, 10, 11
 - Smart card, 22
 - Smartphones, 12, 13
 - Sniffer
 - definition of, 81
 - network and wireless, 81–82
 - wireless keyboard, defending against, 15
 - Social engineering
 - definition of, 7
 - email, 7
 - network attacks, 7–8, 122
 - Software
 - firewalls versus hardware firewalls, 95–96
 - routers versus hardware routers, 103–104
 - theft recovery, 13
 - vulnerability attack, 122
 - Spam, 109, 147–149
 - Special shares, 42
 - Split horizon, 106
 - Split horizon with poison reverse, 106
 - Split tunneling, 60
 - Spoofing, 119
 - Spyware, 135
 - SQL injection attack, 123
 - Stateful inspection, 96–97
 - Stateful multilevel firewall, 94. *See also* Firewall
 - Stateless inspection, 96
 - Static NAT, 112
 - Stream cipher, 46
 - Strong passwords, 70. *See also* Passwords
 - Symmetric encryption, 45–46
 - Syslog, 62

T

- TACACS+, 23–24
- TCP/IP attributes, 93
- Theft, 14
- Theft recovery software, 13
- Threat, 3
- Time Service tool, 27
- Transport layer (four-layer model), 92
- Transport layer (layer 4)
 - flow control methods, 91
 - mechanisms, 90
 - protocols, 91
- Transport Layer Security (TLS), 51, 114–115
- Triggered updates, 106
- Triple DES, 46
- Trojan horse, 135
- Trusted Platform Module (TPM)
 - BitLocker Drive Encryption, 54
 - determining whether you have it, 55
- Tunneling, 118

U

- Unified Threat Management (UTM), 95
- Universal group scope, 32
- USB drives, 14
- User account
 - for administrators, multiple, 6
 - auditing, 29
 - domain, 29
 - guest, 29
 - local, 29
 - processes and procedures, 6
 - standardization, 6
- User Account Control (UAC)
 - client computers, 140–143
 - definition of, 140
 - enable or disable, 141
 - settings, 142–143

Users

- adding as recovery agents, 53
- examining, 29–30
- as objects, 29–30

V

- Virtual LANs
 - hosts, ways to assign, 102
 - IP subnet address, membership by, 102
 - isolation, 101–102
 - MAC address, membership by, 102
 - port, membership by, 102
 - protocol, membership by, 102
 - versus routed networks, 101
 - security, 102
- Virtual private network (VPN)
 - authentication, 59
 - definition of, 58, 112
 - encryption, 58–60
 - limited access enforcement, 99–100
 - protocols, 114–116
 - remote access, 113, 115
 - split tunneling, enabling, 60
 - SSL/TLS, 114–115
 - tunnel, creating, 59
 - tunneling protocols, 58–59
- Virus, 134, 135
- Virus hoax, 138

W

- W32Time service, 27
- Weak encryption keys, 122
- Web content zone, 152–153
- Web servers
 - authentication, 33–34
 - DMZ, 111
- Wi-Fi Protected Access
 - (WPA/WPA2), 125–126

Windowing, 91

- Windows Defender, 136
- Windows Firewall
 - with Advanced Security, 143
 - client computers, 143–147
 - definition of, 143
 - enable or disable, 144
 - ports, opening, 145–146
 - programs, allowing through, 145
- Windows Server Update Service (WSUS), 139
- Windows Update, 138–140
- Windows updates, 138
- Wired Equivalency Privacy (WEP), 125, 126
- Wireless LAN (WLAN)
 - definition, 123
 - keys, 125–126
 - MAC filters, 127
 - security types, 126–127
 - Service Set Identifier (SSID), 126–125
 - Wi-Fi Protected Access (WPA/WPA2), 125–126
 - Wired Equivalency Privacy (WEP), 125
- Wireless networks, security, 123–127
- Worm, 135

X

- X.509 version 3, 48

Z

- Zone, security
 - settings, modifying, 154
 - sites, adding, 153–154
- Zone, web content, 152–153