

Index

Symbols

3Com, MACs (Machine Address Codes), 72

A

Abhay Narayan Medical Center, storage security case study, 504-509

acceptance charts, risk management, 5

access controls, NFS (Network File System), 18

Ace Tomato Company, storage security case study, 510-515

Active Directory, Kerberos authentication, 212-213

address spoofing, FLOGI/PLOGI, 54-55

addresses, Fibre Channel

FLOGI (Fabric Login) process, 52-55

NLOGI (Node Login) process, 54

PLOGI (Port Login) process, 53-55

weaknesses, 52-70

administrators

iSCSI, 26, 28

NAS devices, enumeration, 24-26, 176-177

SANs, 20-23

AH (Authentication Headers), 340

IPSec, 417

anonymous connections, NAS devices, 172

architectures

iSCSI storage architecture, 278, 303

NAS (Network Attached Storage), 150-151

NAS devices using CIFS, 164-165

attacks

address spoofing, FLOGI/PLOGI, 54-55

e-port replication, 16, 136-139

entry points, 19-20

enumeration phase, 36

f-port attacks, 16

Layer 2 Fibre Channel attacks, defending against, 339-342

LUN (Logical Unit Number) subversion, 16
storage controllers, 87-101

management attacks, 16

MITM (Man-in-the-Middle) attacks, 16, 59-64

Fibre Channel, 55-57, 64-69

IP (Internet Protocol), 57-59

name server pollution, 64-65, 69-70

name server pollution, 15

NAS (Network Attached Storage), 16

CIFS (Common Internet File System) attacks, 17

iSCSI (Internet SCSI) attacks, 18-19

NFS (Network File System) attacks, 17-18

penetration phase, 37

SANs, 15

session hijacking, 15

Fibre Channel SANs, 43-51

ISN (Initial Sequence Number), 41

soft zone attacks, 124-128

spoofing

MACs (Machine Address Codes), 79-84

WWNs (World Wide Names), 73-74, 76-84

storage, 15-16

switch management attacks, 140-144

timelines, 37

World Wide Name spoofing, 15

zone hopping, 16, 108-112, 131

performing, 115-124

INDEX

- auditing, 6, 9-10, 451
 - SANs, 32
 - SNAP (Storage Network Audit Program), 452
 - iSCSI SANs, 461-462
 - NAS, 458-461
 - SANs, 452-458
 - storage networks, 432-433
 - authentication, 6, 8
 - CIFS (Common Internet File System), 165
 - Cisco MDS 9000 switches, configuration options, 481-482
 - IPSec, AH (Authentication Headers), 417
 - iSCSI, 18
 - iSNS (iSCSI Storage Name Servers), 411-413
 - Kerberos, 211-212
 - Active Directory, 212-213
 - NAS devices, 241, 252-257
 - CIFS (Common Internet File System), 183-223, 371-375
 - default authentication, 250-251
 - Kerberos, 211-223
 - LM (LANMAN), 189-190, 194-211
 - NFS (Network File System), 249-257, 384-386
 - NTLM (NT LANMAN), 191-211
 - plain-text passwords, 188-189
 - share-level authentication, 183-187
 - NFS (Network File System), 17
 - SANs, 32
 - Fibre Channel, 343-349, 357-358
 - iSCSI, 279-280, 301-314, 403-411, 422-423
 - Authentication Headers (AH), 340
 - IPSec, 417
 - authorization, 6-9
 - CIFS (Common Internet File System), 166
 - NAS devices, 225-226, 258-270
 - CIFS (Common Internet File System), 223-226, 376-377
 - NFS (Network File System), 17, 257-270, 386-389
 - SANs, 32
 - iSCSI, 19, 314-326, 423
 - authorized groups, NAS devices, enumeration, 171-175
 - availability, SANs, 6, 14, 32
- B**
- BeatLM, passwords, cracking, 202-204
 - best practices (security), xxiv
 - block data, file data, compared, xx-xxi
 - BlueArc storage devices, securing, 463
 - Brocade storage devices, securing, 463
 - brute-forcing, CIFS shares, 184-187
 - BS17799, 445
 - Burns, Jesse, 204
- business requirements
 - Abhay Narayan Medical Center case study, 505-509
 - Ace Tomato Company case study, 511-512
 - PlayTronics case study, 497-499
- C**
- Cain and Abel
 - iSNS servers, Man-in-the-Middle attacks, 290, 293-300
 - NAS devices, Man-in-the-Middle attacks, 193-203, 215-223
 - California Senate Bill 1386, 4, 443-444
 - case studies, storage security
 - Abhay Narayan Medical Center, 504-509
 - Ace Tomato Company, 510-515
 - PlayTronics, 496-502
 - CHAP (Challenge Handshake Authentication Protocol), 279
 - iSCSI Sans
 - authentication, 301-302, 403-411
 - CHAP authentication method, 296-298
 - message challenges, 407-408
 - message reflection attacks, 18
 - mutual authentication, 306-309, 409-411
 - offline password brute-forcing, 18
 - username sniffing, 19
 - CIFS (Common Internet File System), 149, 163, 369-370, 392
 - attacks, 17
 - authentication, 371-375
 - authorization, 376-377
 - encryption, 378-381
 - IPSec encryption, 377-381
 - enumeration, limiting, 370-371
 - management protocols, 392-393
 - monitoring, 394-396
 - NAS devices, 153, 156-157, 163
 - architectures, 164-165
 - authentication, 165, 183-223
 - authorization, 166, 223, 225-226
 - command syntax, 158-160
 - communication, 165
 - encryption, 166, 226-234
 - enumeration, 167-182
 - shares, 166, 177-182
 - NetApp filers, configuration options, 469-470
 - Network Appliance filers, 376-377
 - security options, 399
 - tape security, 397-398
 - vFilers (Virtual Filers), 396-397
 - Cisco MDS 9000 switches, configuring, 475-480
 - authentication, 481-482
 - iSCSI, 489-490
 - IVR, 484

- logging, 493-494
 - port security, 487-488
 - security services, 490-493
 - VSANs, 482, 484
 - zoning, 485-486
 - clear-text communication, Fibre Channel, 35-38
 - client nodes, LUN (Logical Unit Number)
 - masking, 89-90
 - clients, Kerberos, 211
 - COBIT standards, 446-450, 512
 - command syntax
 - CIFS (Common Internet File System), 158-160
 - NFS (Network File System), 160
 - Common Internet File System (CIFS). *See* CIFS (Common Internet File System)
 - Common Transport (CT) authentication, Fibre Channel SANs, 348-349
 - communication
 - CIFS (Common Internet File System), 165
 - iSCSI, 279, 295
 - NAS (Network Attached Storage), 152
 - NFS (Network File System), 239-241
 - compliance, 430-432
 - audits, 432-433
 - California Senate Bill 1386, 443-444
 - COBIT standards, 446-447, 449-450
 - GLBA (Gramm-Leach Bliley Act), 441-442
 - HIPAA (Health Insurance Portability and Accountability Act), 437-441
 - international regulations, 445
 - NERC Standard 1200/1300, 444
 - Sarbanes-Oxley requirements, 429-430, 433-436
 - configuration
 - Cisco MDS 9000 switches, 475-480
 - authentication, 481-482
 - iSCSI, 489-490
 - IVR, 484
 - logging, 493-494
 - port security, 487-488
 - security services, 490-493
 - VSANs, 482-484
 - zoning, 485-486
 - NetApp filers, 463-474
 - connections
 - anonymous connections, NAS devices, 172
 - DumpSec connections, NAS devices, 173
 - control activities, COBIT standards, 447, 449-450
 - CRC checksums, iSCSI, 417
 - CT (Common Transport) authentication, Fibre Channel SANs, 348-349
 - cut-through switching, Fibre Channel switches, 139
- D**
- Data ONTAP, Network Appliance filers, security setting, 463-475
 - Details tab (Emulex HBA), 74
 - DH-CHAP (Diffie Hielman CHAP), 32
 - discovery domains, iSNS (iSCSI Storage Name Servers), 326-327, 415-416
 - domain hopping attacks, 328-331
 - Discovery tab (Emulex HBA), 74
 - domain hopping attacks, iSCSI, 326-331
 - domains, iSNS (iSCSI Storage Name Servers), 326-327, 415-416
 - domain hopping attacks, 328-331
 - DumpSec, NAS devices
 - connections, 173
 - enumeration, 173
 - username leaks, 172-175
- E**
- E-port replication, 16
 - Fibre Channel switches, 134-139
 - Electronic Protected Health Information (EPHI), 437
 - EMC Control Center management consoles, 71
 - EMC storage devices, securing, 463
 - Emulex, WWNs (World Wide Names), 72
 - Emulex HBAs, 74
 - Encapsulating Security Protocol (ESP), 340
 - IPSec, 417
 - encryption, 6, 12-13
 - CIFS (Common Internet File System), 166
 - iSCSI, 19
 - NAS devices, 18, 227-234, 242, 270-272
 - CIFS (Common Internet File System), 226-234, 377-381
 - NFS (Network File System), 270-272, 389-391
 - SANs, 32
 - Fibre Channel, 365-367
 - iSCSI, 331-333, 417-421
 - entry points, attacks, 19-20
 - enum.exe, NAS devices, local system account enumeration, 176-177
 - enumeration
 - CIFS (Common Internet File System), 167-175
 - administrators, 176-177
 - authorized groups, 171-175
 - open shares, 177-182
 - port scans, 168-171
 - target version, 168
 - usernames, 171-175
 - Fibre Channel switch enumeration, 132-134
 - NAS
 - CIFS, 370-371
 - NFS, 381-384

INDEX

- NFS (Network File System), 242
 - exports, 246-249
 - port scans, 244-246
 - target versions, 243-244
- SANs, iSCSI, 283-300
- enumeration phase (attacks), 36
- EPHI (Electronic Protected Health Information), 437
- EqualLogic storage devices, securing, 463
- ESP (Encapsulating Security Protocol), 340
 - IPSec, 417
- Ethereal
 - iSCSI targets, spoofing, 318-322
 - iSCSI usernames, capturing, 311-313
- exports
 - NAS devices, enumeration, 246-249
 - NFS (Network File System), 239-240
 - exports, security options, 389
- F**
- f-port replication, 16
- Fabric Attributes tab (Emulex HBA), 74
- FC-AL (Fibre Channel arbitrated loop), 33
- FC-SP (Fibre Channel Security Protocol), 32, 340, 343-346
- FCAP (Fibre Channel Authentication Protocol), 32, 346-347
- FCPAP (Fibre Channel Password Authentication Protocol), 347-348
- Feinstein, Diane, 443
- Fibre Channel Authentication Protocol (FCAP), 32, 346-347
- Fibre Channel Password Authentication Protocol (FCPAP), 347-348
- Fibre Channel Protocol, 4
- Fibre Channel SANs, 337-339
 - addresses, weaknesses, 52-70
 - AH (Authentication Headers), 340
 - authentication, 343-349
 - CT (Common Transport) authentication, 348-349
 - FC-SP (Fibre Channel Security Protocols), 343-346
 - FCAP (Fibre Channel Authentication Protocol), 346-347
 - FCPAP (Fibre Channel Password Authentication Protocol), 347-348
 - switch-to-switch authentication, 357-358
 - Cisco MDS 9000 switches, configuring, 475-494
 - clear-text communication, 35, 37-38
 - ESP (Encapsulating Security Protocol), 340
 - FC-AL (Fibre Channel arbitrated loop), 33
 - FLOGI (Fabric Login) process, 52-53
 - address spoofing, 54-55
- frames, 33
 - headers, 34-35
 - layers, 33-34
 - sequences, 40-43
 - session hijacking, 43-51
 - weaknesses, 40-51
- Layer 2 security, 339-342
- LUN masking, 360-361
- MITM (Man-in-the-Middle) attacks, 55-64
 - name server pollution, 64-70
- name server queries, 361
- NLOGI (Node Login) process, 54
- PlayTronics case study, 496-502
- PLOGI (Port Login) process, 53-54
 - address spoofing, 54-55
- port locking, 355-357
- port type locking, 359-360
- security options, 367-368
- security risks, 33
- soft zone attacks, 124-128
- storage tape encryption, 365-367
- switch management, 362-365
- switched Fibre Channel, 33
- switches
 - cut-through switching, 139
 - E-port replication, 134-139
 - management attacks, 140-144
 - security risks, 105
 - switch enumeration, 132-134
 - zone hopping, 108-112
- VSANs (Virtual SANs), 353-355
- WWNs, 349
 - identification, 350-351
 - zone hopping, 115-124
- zoning, 106-108, 351
 - hard zoning, 110-111, 128-131, 351-352
 - memberships, 111
 - port-based zoning, 352-355
 - soft zoning, 110-111, 113-115
- Fibre Channel Security Protocol (FC-SP), 32, 340, 343-346
- file data, block data, compared, xx-xxi
- Financial Audits with General Computer Controls, 445
- Financial Modernization Act, 441-442
- firewalls, NAS (Network Attached Storage), 154
- Firmware tab (Emulex HBA), 74
- FLOGI (Fabric Login) process, Fibre Channel, 52-53
 - address spoofing, 54-55
- frames, Fibre Channel, 33
 - headers, 34-35
 - layers, 33-34
 - sequences, 40-43
 - weaknesses, 40-51

G

Gates, Bill, 3
gateways, NAS (Network Attached Storage), 151
General tab (Emulex HBA), 74
GLBA (Gramm-Leach Bliley Act), 441-442
governmental regulations, 430-432
 audits, 432-433
 California Senate Bill 1386, 443-444
 GLBA (Gramm-Leach Bliley Act), xxiii, 425, 441-442
 HIPAA (Health Insurance Portability and Accountability Act), 437-441
 international regulations, 445
 Sarbanes-Oxley requirements, 429-430, 433-436
Gramm-Leach Bliley Act (GLBA), xxiii, 425, 441-442
groups, NAS devices, enumeration, 171-175

H

hard zoning, 110-111, 128-131
 Fibre Channel SANs, 351-352
hashes, NTLM hashes, producing, 191-194
HBAs (Host Bus Adapters), 71
 Emulex, 74
 NICs (Network Interface Cards), compared, 72
 WWNs (World Wide Names), 72-73
 spoofing, 72-74, 76-84
 WWN-based zoning, 72
 authorization, 32
 LUN masking, 86-88
headers
 Fibre Channel frames, 34-35
 NAS (Network Attached Storage), 151
HIPAA (Health Insurance Portability and Accountability Act), xxiii, 425, 437-441
Host Attributes tab (Emulex HBA), 74
Host Bus Adapters (HBAs). *See* HBAs (Host Bus Adapters)
hostnames, spoofing, winrelay, 225-226

I

iGroups, iSCSI, 316-326
IKE (Internet Key Exchange), iSCSI IPSec, 417
Information Systems Audit and Control Association (ISACA), COBIT standards, 446-450
Initiator Node Names, iSCSI, 314-315
initiator software, iSCSI, 281, 286-289
integrity, 6, 11-12
integrity checking, SANs, 32
Internet Key Exchange (IKE), iSCSI IPSec, 417
Internet Small Computer Systems Interface (iSCSI). *See* iSCSI (Internet Small Computer Systems Interface)

IP (Internet Protocol), 4
 MITM (Man-in-the-Middle) attacks, 57-59
IP addresses
 MACs, displaying, 293-294
 spoofing, winrelay, 225-226
IPSec
 AH (Authentication Headers), 417
 ESP (Encapsulated Payload), 417
 IKE (Internet Key Exchange), 417
 encryption
 SCSI SANs, 417-421
 NAS devices, 377-381
 NFS NAS devices, 389-391
iQN values, iSCSI SANs, 423
ISACA (Information Systems Audit and Control Association), COBIT standards, 446-450
iSCSI (Internet Small Computer Systems Interface), 4, 275
 administrators, common questions, 26-28
 architecture, 303
 attacks, 18-19
 CHAP (Challenge Handshake Authentication Protocol), 279, 296-298, 301-302
 password hash, 298-299
 usernames, 297-298
Cisco MDS 9000 switches, configuring for, 489-490
communication, 295
iSNS (iSCSI Storage Name Servers)
 authentication, 411-413
 discovery domains, 415-416
 security management, 414-415
NetApp filers, configuration options, 472
node names, 314-315
packets, 275
SANs, 276-278, 401-402
 auditing, 461-462
 authentication, 279-280, 301-314, 403-411, 422-423
 authorization, 314-326, 423
 CRC checksums, 417
 communication, 279
 domain hopping attacks, 326-331
 encryption, 331-333, 417-421
 enumeration, 283-300
 iGroups, 316-326
 Initiator software, 281, 286-289
 iSNS server, 282, 424
 Man-in-the-Middle attacks, 289-300
 mutual authentication, 306-309
 regulations and standards, 445
 security options, 424
 storage architecture, 278
 WinTarget, 282-283
storage devices, 513
usernames, capturing, 311-313

INDEX

iSCSI Qualifier Name (IQN) spoofing, 18
 iSNS (iSCSI Storage Name Servers), 282-283
 authentication, 411-413
 discovery domains, 326-327, 415-416
 domain hopping attacks, 328-331
 enumeration, 284-289
 Man-in-the-Middle attacks, 289-291
 queries, authentication and
 authorization, 424
 security management, 414-415
 ISO17799, 445

J-K

Karlsson, Patrik, 184
 KDC (Kerberos Distribution Center), 211
 Kerberos, 211
 Active Directory, 212-213
 authentication process, 212
 clients, 211
 iSCSI SANs, authentication, 422-423
 KDC (Kerberos Distribution Center), 211
 NAS devices, authentication, 211-223
 service tickets, 211
 TGS (Ticket Granting Server), 211
 Kingsley, Ben, 1

L

Layer 2 Fibre Channel attacks, defending against, 339-342
 layers, Fibre Channel frames, 33-34
 Lefthand storage devices, securing, 463
 LM (LAN Manager), authentication
 CIFS, 371-375
 NAS devices, 189-190, 194-211
 local system administrators, NAS devices, enumeration,
 176-177
 logging, Cisco MDS 9000 switches, configuring for,
 493-494
 Los Alamos National Laboratory, shut
 down of, 4
 ls -al command, 258
 LSILogic, WWNs (World Wide Names), 72
 LUN (Logical Unit Number) masking
 Fibre Channel SANs, 360-361
 iSCSI, 316-326
 storage controllers, 85-87
 attacks, 87-101
 client nodes, 89-90
 disabling, 90
 WWNs (World Wide Names), 86-88
 switches, 95-96
 third-party software, 95-96
 LUN (Logical Unit Number) subversion, 16,
 87-101

M

MAC Address Scanner, MAC addresses,
 enumerating, 293-294
 MAC addresses
 Enumerating, MAC Address Scanner,
 293-294
 NICs (Network Interface Codes), 72
 spoofing, 79-84
 Man-in-the-Middle attacks, 16, 55-64
 Fibre Channel, 64-69
 IP (Internet Protocol), 57-59
 iSCSI, 293-300
 iSNS servers, 289-291
 name server pollution, 64-65, 69-70
 NAS devices, 193-203, 215-223
 management attacks, 16
 iSCSI, 19
 management protocols, NAS devices, 392-393
 McData storage devices, securing, 463
 MD5 (Message Digest 5) algorithm, 11
 memberships, zoning, 111
 message challenges, CHAP, 407-408
 monitoring NAS devices, 394-396
 mount points, CIFS (Common Internet File System), 166
 mount utility, NFS exports, 252-257
 mutual authentication, iSCSI SANs, 306-309, 409-411

N

name server pollution process, 15
 MITM (Man-in-the-Middle) attacks, 64-65, 69-70
 name server queries, Fibre Channel SANs, 361
 NAS (Network Attached Storage), xvii, 2, 3, 149,
 369-370, 392
 administrators, common questions, 24-26
 architectures, 150-151
 attacks, 16
 CIFS (Common Internet File System) attacks, 17
 iSCSI (Internet SCSI) attacks, 18-19
 NFS (Network File System) attacks, 17-18
 timeline, 155
 auditing, SNAP (Storage Network Audit Program),
 458-461
 CIFS (Common Internet File System), 149, 153,
 156-157, 163, 370
 architectures, 164-165
 authentication, 165, 183-223, 371-375
 authorization, 166, 223-226, 376-377
 command syntax, 158-160
 communication, 165
 encryption, 166, 226-234, 377-381
 enumeration, 167-182, 370-371
 shares, 166, 177-182
 communication architecture, 152
 government regulations, 430-433
 audits, 432-433

- California Senate Bill 1386, 443-444
 - GLBA (Gramm-Leach Bliley Act), 441-442
 - HIPAA (Health Insurance Portability and Accountability Act), 437-441
 - Sarbanes-Oxley requirements, 433-436
 - head architecture, 151
 - management protocols, 392-393
 - monitoring, 394-396
 - NetApp Filer, security setting, 463-475
 - network filtering, reliance on, 154
 - NFS (Network File System), 149, 157-158, 238-239
 - authentication, 241, 249-257, 384, 386
 - authorization, 257-270, 386-389
 - command syntax, 160
 - communication, 239-241
 - encryption, 242, 270-272, 389-391
 - enumeration, 242-249, 381-384
 - exports, 239-240
 - operating system attacks, compared, 155
 - securing, 463
 - security, xix-xx
 - security options, 399
 - security risks, 149, 153
 - security standards, 153-155
 - storage devices, 506
 - tape security, 397-398
 - TCP/IP traces, 157
 - vFilers (Virtual Filers), 396-397
 - NDMP (Network Data Management Protocol), NAS
 - devices, monitoring, 394
 - NERC Standard 1200/1300, 444
 - NetApp Filer
 - Authentication, iSCSI, 404-411
 - security setting, 463-466, 468
 - CIFS options, 469-470
 - iSCSI options, 472
 - multi-protocol options, 470, 472
 - network options, 473-474
 - NFS options, 468
 - system services options, 474-475
 - Network Appliance filers, CIFS, 376-377
 - Network Attached Storage (NAS). *See* NAS (Network Attached Storage)
 - Network Data Management Protocol (NDMP), NAS
 - devices, monitoring, 394
 - network devices, security risks, 153
 - Network File System (NFS). *See* NFS (Network File System)
 - network storage
 - attacks, 15-16
 - future of, 4
 - risk management, 5-6
 - trend toward, 3
 - NFS (Network File System), 149, 237, 369-370, 392
 - attacks, 17-18
 - authentication, 384, 386
 - authorization, 386-389
 - encryption, 389-391
 - enumeration, 381-384
 - management protocols, 392-393
 - monitoring, 394-396
 - NAS devices, 153, 157-158, 237-239
 - authentication, 241, 249-257
 - authorization, 257-270
 - command syntax, 160
 - communication, 239, 241
 - encryption, 242, 270-272
 - enumeration, 242-249
 - exports, 239-240
 - NetApp filers, configuration options, 468
 - security options, 399
 - tape security, 397-398
 - vFilers (Virtual Filers), 396-397
 - NICs (Network Interface Cards)
 - HBAs (Host Bus Adapters), compared, 72
 - MACs (Machine Address Codes), 72
 - spoofing, 79-84
 - Nixon, Richard, 431
 - NLOGI (Node Login) process, Fibre Channel, 54
 - nmap, 169
 - iSNS servers, locating, 290
 - NAS devices, port scans, 169-171
 - node names, iSCSI, 314-315
 - node WWNs, port WWNs, compared, 112
 - nodes, client nodes, LUN Logical Unit Number) masking, 89-90
 - NPI (non-public personal information),
 - protection of, 441
 - NTLM (NT LAN Manager), authentication
 - CIFS, 371-375
 - NAS devices, 191-211
- O**
- Odhner, Chris, 463
 - open port scans, NAS devices, 168-171, 244-246
 - open shares, NAS devices, 177-182
 - Oracle databases, NFS (Network File System), 237
 - Oxley, Michael, 430
- P**
- Packets, iSCSI packets, 275
 - passwords
 - Fibre Channel, FCPAP (Fibre Channel Password Authentication Protocol), 347-348
 - plain-text passwords, CIFS authentication, 188-189

INDEX

penetration phase (attacks), 37
 permissions, Unix, 257-258
 PHI (Protected Health Information), 437
 plain-text passwords, CIFS authentication, 188-189
 PlayTronics storage security case study, 496-504
 PLOGI (Port Login) process, Fibre Channel, 53-54
 address spoofing, 54-55
 Port Attributes tab (Emulex HBA), 74
 port locking, Fibre Channel SANs, 355-357
 port scanning
 iSNS servers
 Storage Scanner, 285
 StorScan, 285-286
 NAS devices, 168-171, 244-246
 port security, Cisco MDS 9000 switches,
 configuring for, 487-488
 Port Statistics tab (Emulex HBA), 74
 port type locking, Fibre Channel SANs, 359-360
 port WWNs
 membership attacks, 119-120
 node WWNs, compared, 112
 port-based zoning, Fibre Channel SANs, 352-353
 Protected Health Information (PHI), 437

Q

QLogic storage devices
 securing, 463
 WWNs (World Wide Names), 72
 QoS (Quality of Service), SANs, 32
 queries, iSNS queries, authentication and
 authorization, 424

R

regulations, 430-432
 Abhay Narayan Medical Center case study, 505-509
 Ace Tomato Company case study, 511-512
 audits, 432-433
 California Senate Bill 1386, 443-444
 GLBA (Gramm-Leach Bliley Act), 441-442
 HIPAA (Health Insurance Portability and
 Accountability Act), 437-441
 international, 445
 PlayTronics case study, 497-499
 Sarbanes-Oxley requirements, 429-430, 433-436
 storage security, xxiii
 risk management, 5-6
 Ritter, Jordan, 176

S

Samba CIFS, 156
 SANs (Storage Area Networks), 2-3
 administrators, common questions, 20-23
 attacks, 15
 entry points, 19-20
 auditing, 32
 SNAP (Storage Network Audit Program), 452-458

authentication, 32
 authorization, 32
 availability, 32
 encryption, 32
 Fibre Channel, 337-339
 address weaknesses, 52-70
 authentication, 343-349
 clear-text communication, 35-38
 CT (Common Transport) authentication, 348-349
 FC-AL (Fibre Channel arbitrated loop), 33
 FC-SP (Fibre Channel Security Protocols), 343-346
 FCAP (Fibre Channel Authentication Protocol),
 346-347
 FCPAP (Fibre Channel Password Authentication
 Protocol), 347-348
 FLOGI (Fabric Login) process, 52-55
 frame sequences, 40-43
 frame weaknesses, 40-51
 frames, 33-35
 hard zoning, 128-131
 Layer 2 security, 339-342
 LUN masking, 360-361
 MITM (Man-in-the-Middle) attacks, 55-70
 name server queries, 361
 NLOGI (Node Login) process, 54
 PLOGI (Port Login) process, 53-55
 port locking, 355-357
 port type locking, 359-360
 security options, 367-368
 security risks, 33
 session hijacking, 43-51
 soft zone attacks, 124-128
 storage tape encryption, 365-367
 switch management, 362-365
 switch-to-switch authentication, 357-358
 switched Fibre Channel, 33
 switches, 105
 VSANs (Virtual SANs), 353-355
 WWNs, 349-351
 zone hopping, 108-112, 115-124
 zoning, 106-115, 351-355
 government regulations, 430-433
 audits, 432-433
 California Senate Bill 1386, 443-444
 GLBA (Gramm-Leach Bliley Act), 441-442
 HIPAA (Health Insurance Portability and
 Accountability Act), 437-441
 meeting, 445
 Sarbanes-Oxley requirements, 433-436
 HBAs (Host Bus Adapters), 71-72
 Emulex, 74
 WWNs (World Wide Names), 72-74, 76-84
 integrity checking, 32

- iSCSI (Internet Small Computer Systems Interface), 275-278, 401-402
 - authentication, 279-280, 301-314, 403-411, 422-423
 - authorization, 314-326, 423
 - communication, 279
 - domain hopping attacks, 326-331
 - encryption, 331-333, 417-421
 - enumeration, 283-289, 291-292, 294-300
 - iGroups, 316-326
 - Initiator software, 281, 286-289
 - iSNS queries, 424
 - iSNS server, 282
 - Man-in-the-Middle attacks, 289-291
 - mutual authentication, 306-309
 - packets, 275
 - security options, 424
 - storage architecture, 278
 - WinTarget, 282-283
- iSNS (iSCSI Storage Name Servers)
 - authentication, 411-413
 - discovery domains, 415-416
 - security management, 414-415
- SBR (Security and Business Risk) chart, 39-40
- securing, 463
- security risks, 32
- security weaknesses, 39
- storage controllers, 71, 84
 - LUN (Logical Unit Number) masking, 85-101
- storage management consoles, 71, 101-102
- storage switches, 71
- Sarbanes, Paul, 430
- Sarbanes-Oxley requirements, 425, 429-430, 433-436, 443-444
- SAS70, 445
- SBR (Security and Business Risk) chart, 39-40
- scanning ports
 - iSNS servers
 - Storage Scanner, 285
 - StorScan, 285-286
 - NAS devices, 168-171, 244-246
- ScoopLM, LM/NTLM hashes, sniffing, 201-202
- SCSI (Small Computer Systems Interface), 275
- security
 - auditing, 6, 9-10
 - authentication, 6, 8
 - authorization, 6, 8-9
 - availability, 6, 14
 - best practices, xxiv
 - encryption, 6, 12-13
 - integrity, 6, 11-12
- security management, iSNS (iSCSI Storage Name Servers), 414-415
- sequences, Fibre Channel frames, 40-43
- Server Message Block (SMB). *See* SMB (Server Message Block)
- service tickets, Kerberos, 211
- session hijacking, 15
 - Fibre Channel SANs, 43-51
 - ISN (Initial Sequence Number), 41
- SHA-1 (Secure Hash Algorithm 1), 11
- share-level authentication, NAS devices, 183-187
- shares
 - CIFS (Common Internet File System), 166
 - NAS devices, 177-182
- Showmount, NAS devices, export enumeration, 247-249
- Simple Network Management Protocol (SNMP), NAS devices, monitoring, 395-396
- Small Office/Home Office (SOHO), 4
- SMB (Server Message Block), 156, 163
 - NAS devices
 - architectures, 164-165
 - authentication, 165
 - authorization, 166
 - communication, 165
 - encryption, 166
 - enumeration, 167-182
 - shares, 166
- SMB Brute Forcer, CIFS shares, brute-forcing, 184-187
- SMBproxy, 204
- SmbShell, NAS devices, LM/NTLM hash presentations, 204-207
- SNAP (Storage Network Audit Program)
 - iSCSI SANs, auditing, 461-462
 - NAS, auditing, 458-461
 - SANs, auditing, 452-458
- Sneakers*, 1
- sniffing iSCSI, 291-292, 294-300
- SNMP (Simple Network Management Protocol), NAS devices, monitoring, 395-396
- soft zone attacks, 124-128
- soft zoning, 110-111
 - WWN-based membership, 113-115
- SOHO (Small Office/Home Office), 4
- spoofing
 - hostnames, winrelay, 225-226
 - IP addresses, winrelay, 225-226
 - MACs (Machine Address Codes), 79-84
 - WWNs (World Wide Names), 72-74, 76-84
- standards
 - COBIT standards, 446-447, 449-450
 - NERC Standard 1200/1300, 444
- Storage Area Networks (SANs). *See* SANs (Storage Area Networks)
- storage capacities, extension of, 3
- storage controllers, 71, 84
 - LUN (Logical Unit Number) masking, 85-87
 - attacks, 87-101
 - client nodes, 89-90
 - disabling, 90

INDEX

storage devices, securing, automated tools, 463

storage groups, 2

storage management consoles, 71, 101-102

Storage Network Audit Program (SNAP). *See* SNAP (Storage Network Audit Program)

storage networks, 1

Storage Scanner, iSNS servers, port scanning, 285

storage security, case studies

- Abhay Narayan Medical Center, 504-509
- Ace Tomato Company, 510-515
- PlayTronics, 496-502-504

storage switches, 71

storage tapes, Fibre Channel SANs, encryption, 365-367

StorScan, 169

- iSNS servers
 - locating, 290
 - port scanning, 285-286
- NAS devices, port scans, 169, 244-246

switch management, Fibre Channel SANs, 362-365

switch-to-switch authentication, Fibre Channel SANs, 357-358

switched Fibre Channel, 33

switches

- Cisco MDS 9000 switches, configuring, 475-494
- Fibre Channel switches
 - cut-through switching, 139
 - E-port replication, 134-139
 - management attacks, 140-144
 - security risks, 105
 - switch enumeration, 132-134
 - zone hopping, 108-112
 - zoning, 106-108, 110-111, 113-115
- LUN (Logical Unit Number) masking, 95-96

T

tapes, NAS devices, security, 397-398

Target Attributes tab (Emulex HBA), 74

targets, versions, enumeration, 168

TCP/IP traces, NAS (Network Attached Storage), 157

Telnet, NAS devices, managing, 228-229

TGS (Ticket Granting Server), 211

third-party software, LUN (Logical Unit Number) masking, 95-96

U

Unix permissions, 257-258

Urgent Action Standard 1200—Cyber Security, 445

usernames

- iSCSI, capturing, 311-313
- NAS devices, enumeration, 171-175

V

Veritas SANPoint, 71

versions, NAS devices, enumeration, 168

vFilers, NAS devices, segmenting, 396-397

Vindstrom, Arne, 179, 225

virtual architecture, NAS (Network Attached Storage), 151

VSANs (Virtual SANs), 353-355

- Cisco MDS 9000 switches, configuration options, 482, 484

W

wininfo.exe, NAS devices, share enumeration, 179-182

winrelay

- hostnames, spoofing, 225-226
- IP addresses, spoofing, 225-226

WinTarget, iSCSI, 282-283

Wood, Rose Mary, 431

World Wide Name spoofing, 15

World Wide Names (WWNs). *See* WWNs (World Wide Names)

WORM (Write Once Read Many) devices, 432

WWNs (World Wide Names)

- authorization, 32
- Fibre Channel SANs, 349
- identification, 350-351
- HBAs (Host Bus Adapters), 72-73
 - Emulex, 74
 - LUN masking, 86-88
 - spoofing, 72-84
 - WWN-based zoning, 72
- node WWNs, 112
- port WWNs, 112
 - membership attacks, 119-120

X-Z

Xircom, MACs (Machine Address Codes), 72

zone hopping, 16, 131

- Fibre Channel switches, 108-112
- performing, 115-124

zoning

- Cisco MDS 9000 switches, configuring for, 485-486
- Fibre Channel SANs, 106-108, 351
 - hard zoning, 110-111, 351-352
 - memberships, 111
 - port-based zoning, 352-353
 - soft zoning, 110-111, 113-115
- VSANs (Virtual SANs), 353-355



Register Your Book

at www.awprofessional.com/register

You may be eligible to receive:

- Advance notice of forthcoming editions of the book
- Related book recommendations
- Chapter excerpts and supplements of forthcoming titles
- Information about special contests and promotions throughout the year
- Notices and reminders about author appearances, tradeshow, and online chats with special guests

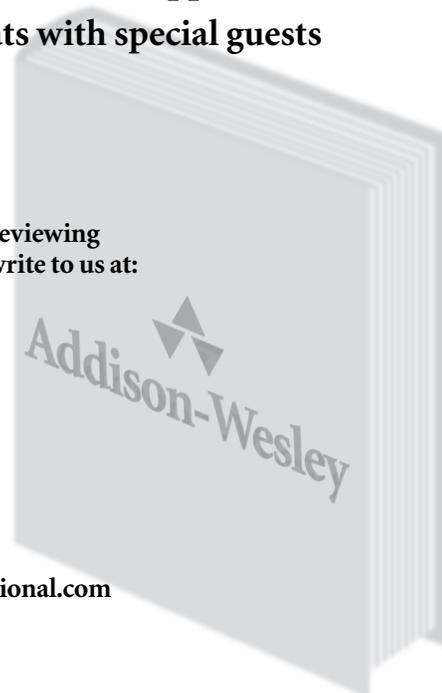


Contact us

If you are interested in writing a book or reviewing manuscripts prior to publication, please write to us at:

Editorial Department
Addison-Wesley Professional
75 Arlington Street, Suite 300
Boston, MA 02116 USA
Email: AWPro@aw.com

Visit us on the Web: <http://www.awprofessional.com>



The logo for InformIT, with 'inform' in a bold, lowercase sans-serif font and 'IT' in a larger, uppercase sans-serif font, both in black.The website address 'www.informit.com' in a white, lowercase sans-serif font, centered on a black horizontal bar.

YOUR GUIDE TO IT REFERENCE

The word 'Articles' in a white, bold, sans-serif font, centered on a black horizontal bar. To the left is a small image of a computer keyboard.

Keep your edge with thousands of free articles, in-depth features, interviews, and IT reference recommendations – all written by experts you know and trust.

The words 'Online Books' in a white, bold, sans-serif font, centered on a black horizontal bar. To the left is a small image of a book cover.

Answers in an instant from **InformIT Online Book's** 600+ fully searchable on line books. For a limited time, you can get your first 14 days **free**.

The logo for Safari Tech Books Online, featuring the word 'Safari' in a large, bold, serif font with a registered trademark symbol, and 'POWERED BY' in a smaller font above it. Below 'Safari' is the text 'TECH BOOKS ONLINE' in a smaller, all-caps sans-serif font.The word 'Catalog' in a white, bold, sans-serif font, centered on a black horizontal bar. To the left is a small image of a book spine.

Review online sample chapters, author biographies and customer rankings and choose exactly the right book from a selection of over 5,000 titles.

