



Markus
Kammermann

Markus
a Campo



CompTIA Security+

Vorbereitung auf die Prüfung SY0-301

Stichwortverzeichnis

Numerisch

3DES 47
802.11a 220, 221
802.11b 220, 221
802.11g 220, 221
802.11h 221
802.11i 228
802.11n 221
802.11p 222
802.11s 222
802.1x 204, 230

A

AAA-Protokoll 206
Access Control List 64, 155
Ad-hoc-Netzwerk 222
Administrative Richtlinie 38
Adware 109
AES 47
AH 209
Annual Loss Expectancy 299
Application Gateway 260, 262
Application Level Gateway 257
Archivierung 144
Asymmetrische Verschlüsselung 48, 56
Aufbewahrungspflicht 144
Aufgabenteilung 127
Ausfallszenario 298
Authentifizierung 65
Authentifizierungsmethode 65
Autorisierung 63

B

Backdoor 194
Badge 76, 77
Baselinemanagement 245
Bastion Host 260
Bauliche Maßnahme 75
Bell La Padula 154
Benutzerverwaltung 38
Bildschirm Sperre 102
Biometrisches Erkennungssystem 78

Black Hats 196
Black-Box-Test 273
Blockverschlüsseler 43
Blowfish 47
Bluejacking 236
Bluesnarfung 236
Bluetooth 235
Boot-Virus 113
Botnet 114, 215
Brandklasse 83
Brandschutz 82
Broadcast 159
BSI 34
Business Continuity Management 146

C

CCMP 229
CERT 175
CHAP 72
Chassis Intrusion Detection 99
CIA 33
CIFS 171
Circuit Level-Firewall 260
Clean Desk Policy 124
Cloud 195
Cluster 296
Clustering 295
CO2 83
Cold Site 302
Command-Injection 183
Common Criteria 33, 100
CompTIA Security+-Zertifizierung 17
Cookie-Manipulation 184
CRL 67
Cross Site Scripting 182
CSMA/CA 220

D

DAC Siehe Zugriffssteuerung
Data Loss Prevention 151
Datenschutzgesetz 124, 144
Datensicherung 143, 147

Datensicherungskonzept 146
Datensicherungsmedium 143
Dedizierte Firewall 256
Denial of Service 176, 187
DES 46
Diebstahlsicherung 98
Differenziell Siehe Datensicherung
Diffie-Hellman 50
Digitale Signatur 55
Directory-Traversal 181
Disaster Recovery 38, 147, 296
Distributed Denial of Service 188
DLP 151
DMZ 255
DNS 168
Drehschleuse 79
Drive-By-Angriff 186
Drive-By-Pharming 134
dual-homed 257
duplexing 294

E

EAP 231
EAP-TLS 205
ECC 54
Echtzeitüberwachung 119
EICAR 120
EICAR-Code 121
Einbruchschutz 81
Elektrostatische Entladung 85
ElGamal 50
EMP 91
Energieversorgung 86
Enigma 42
ESD 85, 86
ESP 209
Evil Twin 235
Exploit 272

F

FDE 100
Fehler
 kritischer 104
 sicherheitskritischer 104
Fingerprinting 271
Firewall 255
 dedizierte 256
Footprinting 271
FORM-Field 184

FTP 167
Full Disk Encryption 100

G

Generationenprinzip Siehe Datensicherung
Gerätename 236
GPS-Tracker 102
Grayware 109
Grey Hats 196
Grundsäule
 der Informationssicherheit 33
Gruppenrichtlinie 95

H

Hardware-Firewall 256
Hardware-Sicherheitsmodul 100
Hash 72
Hash-Wert 50
HIPAA 125, 145
HMAC 53
Hoax 117
Hochwasserschutz 82
Honeynet 264
Honeypot 264
Hot Site 302
Hotfix 105
HSM 100
HTTP 169
Hybride Verschlüsselung 56

I

IaaS 195
Identifizierung 65
Identität 63
IDS 264, 265, 266
IEEE 802.11 219
IKE 211
Implementation
 Implementierung 162
Implicit Deny 64
Incident Response 278
Informationsklasse 123
Informationsrichtlinie 38
Informationssicherheit
 Grundsäulen 33
Infrastrukturnetzwerk 222
Inkrementell Siehe Datensicherung
Integrität 31
IP-Protokoll 162

IPsec 208, 211
 IPv6 165
 ISO/IEC 27001 34
 IT-Grundschutz 35, 36
 IT-Grundschutzkatalog 36
 ITSEC 33
 IV-Attacke 227

J

Job Rotation 127

K

Kensington 98
 Kerberos 70
 Keycard 76
 Keylogger 186
 Klassifizierung 123
 Koppelung Siehe Bluetooth
 Kritischer Fehler 104
 Kryptografie 41

L

L2TP 207
 Lastwert 245
 LDAP 171
 LDAP-Injection 183
 Least Privileges 157
 Leistungsüberwachung 246
 Loadbalancing 295
 Logische Bombe 116
 LoMAC 154

M

MAC Siehe Zugriffssteuerung
 MAC-Adresse 250
 MAC-Filter 224
 Mail Spoofing 140
 Malware 110, 114
 Man in the Middle 189, 215
 Man Trap 79
 mandatory vacations 127
 Mannschleuse 79
 Maßnahme
 bauliche 75
 MD4 52
 MD5 51
 MIMO 220
 mirror 291
 Modus 1 Siehe Bluetooth

Multifaktorauthentifizierung 69
 Multi-Level-Security 154

N

NAC 161
 NAS 206
 NAT 160
 NetBIOS 171
 Network Access Server 206, 231
 Netzwerkmonitor 249
 Netzwerküberwachung 248
 nicht sichtbar Siehe Bluetooth
 Nicht-Leugbarkeit 73
 NIDS 264
 NIPS 265
 Non-Repudiation 73
 Notfallplan 300
 Notstromaggregat 89
 NTLM 73

O

Öffentlicher Schlüssel 49
 One-Time-Pad 42
 Online Backup 149

P

Paketfilter 257, 258
 PAP 72
 Passwort Guessing 179
 Patch 105
 Patch Management 106
 PEAP 205
 PEAP-EAP-TLS 205
 Personal Firewall 256
 PGP 136
 Pharming 133
 Phishing 185
 PII 125
 PIN-Code 101
 Ping of Death 187
 PKI 56, 59
 Portnummer 166
 Portscanner 271
 PPTP 207
 Privater Schlüssel 49
 Proxy 262, 264
 PSK 212
 Pufferüberlauf 178
 Punkt-zu-Punkt-Verbindung 200

Q

Quarantänebereich Siehe NAC

R

Race-Condition 178
 RADIUS 205, 207, 230
 RAID 290
 RAID 0 290
 RAID 1 291
 RAID 10 293
 RAID 3 292
 RAID 5 292
 RAID Levels 290
 Rainbow-Tabelle 275
 RAS-System 203
 RBAC Siehe Zugriffssteuerung
 RC4 48
 Recovery-Agent 59
 Redundanz 301
 Registrierung 58
 Release-Notes 275
 Remote Sanitation 102
 Remote Wipe 102
 Remote-Access 199
 Remote-Access-VPN Siehe VPN
 Remote-Zugriff 199
 Replay-Angriff 192
 Richtlinie
 administrative 38
 RIPv4 53
 RMON 242
 Rogue Access Point 235
 Rollenbasierte Zugriffskontrolle 155
 Rollups 105
 Root-Zertifikat 58
 RSA 49

S

S/MIME 135
 SA 208, 211, 212
 SaaS 195
 Safe 81
 Salt 180
 Sandbox 263
 Scareware 109
 Schleuse 80
 Schließsystem 76, 77
 Schlüssel 76
 öffentlicher 49
 privater 49

Schutzbedarf 125
 Schutzbedarfsfeststellung 36
 SCP 167
 Segregation of Duties 127
 Service Pack 105
 Session-Hijacking 193
 SHA 52
 Sicherheitskritischer Fehler 104
 Sicherheitsrichtlinie 33
 Sicherungsverfahren Siehe Datensicherung
 Signatur
 digitale 55
 Site-to-Site Siehe VPN
 SMON 242
 SMTP Relay 139
 Smurf 187
 SNMP 168, 242
 Social Engineering 127, 129
 SOX 145
 Spam 140
 Spear Phishing 133
 Spit 186
 Spoofing 188, 215
 Spyware 109
 SQL-Injection 182
 SSH 167, 213
 SSID 222, 223
 SSL 170, 213
 Stack 178
 Stateful Inspection Firewall 257
 Stateful Packet Inspection 259
 Steganografie 195
 Stripes 292
 Stromverschlüsseler 44
 Stromverschlüsselung 45
 Subnettierung 158
 Subnetzmaske 158
 SY0-301 324
 Symmetrische Verschlüsselung 45, 55
 SYN-Flooding 187
 Systemhärtung 96
 Systemsicherheit 93
 Systemsicherheitsrichtlinie 38

T

TACACS 206
 TACACS+ 206
 TCG 99
 TCP 163
 TCSEC 33

Telnet 166
Terminalverbindung 166
TFTP 167
TKIP 229
TLS 170
Token 66
TPM 99
Transitive Zugriffe 184
Transport-Modus 210
Transportverschlüsselung 166
Triple-A 206
Trojaner 114
Trusted Platform Module 99
Tunnel-Modus 210
Twofish 48

U

Überwachung 242
UDP 164
Unified Threat Management 266
Update 105
UPS 87
URL-Manipulation 184
USV 87, 88
 Leistung 88
UTM 266

V

Venenscanner 68
Verfügbarkeit 31
Verschlüsselung 224
 asymmetrische 48
 hybride 56
 symmetrische 45, 55
Vertraulichkeit 31
Videoüberwachung 80
Viren 109, 118, 119
Virenbekämpfung 117
Virenschutzkonzept 120

Virenverantwortlicher 120
Virtualisierung 158
Vishing 133
VLAN 160
Vollbackup Siehe Datensicherung
Voraussetzung
 für Zertifizierungen 21
VPN 199
VPN Concentrator 202

W

Wachpersonal 76
WAP 232
War Chalking 219
War Driving 219
WEP 226
Whaling 133
White Hats 196
White-Box-Test 273
Wireshark 251
WPA 229
WPA2 229
Wurm 116

X

X.509 57, 212
Xmas-Attacke 187
XML-Injection 183
XTACACS 206

Z

Zeitsteuerung Siehe Rollen
Zertifikat 58
Zugriffskontrolle
 rollenbasierte 155
Zugriffsliste 64
Zugriffssteuerung 153
Zutrittsregelung 75