

Stichwortverzeichnis

Symbols

7-zip 127
/etc/passwd 141

A

Abschlussbericht 70
Access Control List (ACL) 261
AccessEnum 207
Active Directory 222
Active Server Pages (ASP) 309
Acunetix Web Vulnerability Scanner 41, 202, 296, 314, 327
Advanced EFS Data Recovery 207
Advanced Office Password Recovery 324
Advanced Persistent Threat (APT) 171
Advanced SQL Password Recovery 322
Adware 212
AES (Advanced Encryption Standard) 131, 186, 189
AfriNIC 85
Aircrack-ng 179, 185, 348
airodump 185
AirWatch 212
Aktenvernichter 101
Angewandte Sozialwissenschaften 87
Angriff 34
 Anwendungen 36
 Betriebssystem 35
 Directory Traversal 297
 Netzwerkinfrastruktur 35
 nicht-technischer 35
 planen 53
 Standardskripte 309
Angriffsbaum 61
Angriffserkennungssystem 70
Anmeldung, unsichere im Web 311
Anreiz 352
AP (Access Point) 179
APNIC 85
AppDetectivePro 325
AppSpider 308

Archive Password Recovery 130
ArcSight Data Platform 349
ARIN 85
ARP 166
 Poisoning 164, 166
 Poisoning mit Cain & Abel 167
 Spoofing 164, 166
 Tabellen 166
AT-Befehl 348
Auditierung 32
Auftragshacker 50
Authentifizierung
 schwache 121
 umgehen 121

B

Backdoor 93
Bandbreitenblockade 273
Banner-Grabbing 156
 Gegenmaßnahmen 157
Barracuda Networks 276, 318
Bastille UNIX 266
Benutzer, böswilliger 31
Bericht erstellen 338
Berichtswesen 335
Bildschirmaktion aufzeichnen 64
Bildschirm Sperre 210
Biometrisches Erkennungssystem 110
BIOS-Kennwörter 135
BitLocker 112, 211
BKA-Trojaner 101
Black Hat 30
Black Hat Conference 49
Blast 174
Blindtest 71
Blooover 184
Blue Hat 49
Bluelog 184
BlueScanner 184
Bluesnarfer 184
BlueSniper rifle 184
Bluetooth 184
Bot 55
Brutus 121, 123, 287, 312
BSD (Berkeley Software Distribution) 258
BSD-r-Befehl 259
Btscanner 184

Buffer Overflow 263, 301, 325
Bulk Eraser 113
Bundestag 97
BURP Proxy 296, 302, 306

C

Cain & Abel 111, 121–122, 133, 147, 160, 166, 286, 292, 322
 ARP-Poisoning 167
Camtasia 70
Camtasia Studio 64
CAPTCHA 275–276
Car Whisperer 184
Cb Protection 132
CCMP 186
C|EH 32
Challenge-Response-Verfahren 136
Checksum Tool 67
Cheops-ng (Zeichenprogramm) 346
Cisco 326
Client Hyper-V 72
Cloudflare 318
Code Injection 305
Cofense 97
Common Gateway Interface (CGI) 259
CommView 133, 160, 174, 294
CommView for WiFi 179, 182, 193–194
Compliance 32
Content Management System (CMS) 295, 309
COPS 263
Cracker 30
cracklib 141
Crawler 298
Cross-site Scripting (XSS) 101, 307
 prüfen auf 308
CryptoLocker 172
CryptoWall 172
Cyberterrorist 49
Cylance 172

D

Daemon 249
 auskommentieren 256
 suchen 253

Dark Web 53
 Datenbank 321
 Kennwörter knacken 323
 Schwachstellen 325
 Werkzeuge 321
 Datenschutz-Grundverordnung 364
 Datenschutzrichtlinie 86
 Debian 267
 Deep Freeze Enterprise 132
 Deep Web 53
 Dell KACE Systems 268
 Demilitarisierte Zone 147,
 176, 201, 327
 Denial of Service 35, 172
 Angriff 172
 Angriff, Gegenmaßnahmen 174
 E-Mail-Anhänge 272
 Kondition 272
 Testwerkzeuge 174
 DHA 278
 Dial-by-Name 96
 Dienstblockade 35
 DIN 32757 101
 Dipolantenne 179
 Directory-Harvest-Angriff 278
 Directory Traversal 297
 Gegenmaßnahmen 300
 disallow-Eintrag 84
 Display-Sperre 216
 Distributed DoS (DDoS) 173
 DLP (Data Loss Prevention) 348
 DMZ 176
 DNSstuff 85
 Domain Factory 85
 DoS 35
 dpkg 267
 Dropbox for Business 274
 DSGVO 364
 dsniff 166
 DumpSec 139, 233
 Dumpster Diving 35, 87, 95
 Dumpstern 87

E

E-Commerce 275
 Ecora Patch Manager 344
 Effective File Search 328
 EICAR 286
 Eingabeaufforderung 240
 Eingabefilter 307
 Eingabepprüfung 301
 Elcomsoft Advanced SQL
 Password Recovery 323
 Elcomsoft Distributed Password Recovery 122, 323

Elcomsoft Forensic Disk
 Decryptor 211
 Elcomsoft Phone Password
 Breaker 216
 Elcomsoft System Recovery 122, 206
 Elcomsoft Wireless Security
 Auditor 179, 187
 E-Mail
 Angriffe 272, 287
 Banner-Angriffe 276–277
 Bomben 272
 Firewalls 276
 Header 285
 Malware 286
 Postfix 289
 qmail 289
 Sendmail 289
 Sicherheitskontrollen 276
 SMTP 278
 Tarpit 276
 Teergrube 276
 Verkehr abfangen 285
 E-Mail-Header 76
 EmailVerify 280
 Essential NetTools 147, 155,
 280
 Ethereal 161
 ettercap 161
 EU-DSGVO 52
 EWSA 187
 Exploit 35, 70

F

Face Unlock 216
 FAQ (Frequently Asked
 Questions) 41
 Fedora 267
 Fehler 404 74
 Fernsteuerung 88
 Fernwartungsprogramm 111
 Festplattenverschlüsselung 210
 FIFO-Puffer 162
 FileLocator Pro 132, 327–
 328
 FileVault 112
 FileVault2 207, 211
 findstr 133
 Fingerabdruckscanner 238
 Fingerbewegung 216
 Display-sperre 216
 Firefox Web Developer 296
 Firefox Web Developer 302
 Firemon Risk Analyzer 159
 Firewall 159
 E-Mail 276
 Regeln 158
 testen 158

FMEA (Failure Mode and Effects Analysis) 61
 Footprinting 71
 Fortinet 318, 326, 331
 Fortres 101 132
 fping 72
 FREAK (Factoring Attack on
 RSA-EXPORT Keys) 175
 Free Kevin 49
 Freigabeberechtigung 234

G

Gantt 63
 Gebäude 105
 Angriffspunkte 105
 Gegenmaßnahmen 106
 Versorgung 106
 Gebäudeschwachstelle 106
 Gesichtserkennung 216
 Getif 148, 155
 GFI EventsManager 349
 GFI LanGuard 71, 77, 183,
 202, 224–225, 228, 235,
 244, 268, 344
 GFI LANguard 148
 GHDB 300
 Glassdoor 82
 GNU MAC Changer 170, 199
 Google 299
 erweiterte Suche 300
 suchen mit 83
 Google Drive 36
 Google Hack HoneyPot 301
 Google Kontakt 300
 GPS (Global Positioning
 System) 365
 Gray Hat 49
 Gray-Hat 30
 grep 133

H

H.323 291
 Hacken
 Abläufe automatisieren 347
 ethisches 23
 Hacken, ethisches
 Richtlinien 32
 Hacker 29–30
 Denkweise 46
 Fähigkeiten 48
 geläuterter 351
 klassifizieren 45
 Hacktivist 49
 Hash 122
 Heartbleed 175
 Hintertür 93
 Hörgerät 96
 Hotspotter 196
 htaccess 301

htdocs 301
 httpd.conf 301
 HTTP (Hypertext Transfer Protocol) 297
 HTTrack Website Copier 83, 298
 Hyper-V 72

I

IceWarp 274
 ICMP 150
 IdentityFinder 330
 Idera 326
 IDS (Intrusion Detection Systems) 63
 IMAPS 288
 Imperva 326
 Inferenz 120
 Informationsbeschaffung 71
 Initialisierungsvektor (IV) 184
 inSSIDer 181
 Internetbanking 132
 Internet der Dinge 54, 217
 Internet Information Services Manager 301
 Internet of Things 217
 Internetquellen 278
 Intrusion Detection System (IDS) 70–71
 Intrusion Prevention System (IPS) 53, 63, 71, 152, 154
 iOS
 Kennwörter knacken 213
 iOS Forensic Toolkit Verwendung 213
 IoT 217
 IoT (Internet der Dinge) 295
 IoT (Internet of Things) 54
 IP Personality 317
 IPS (Intrusion Prevention System) 348
 IPv6-Adresse 73
 IRC 53
 Irisscanner 238
 ISO/IEC 27001\ 2017 58

J

Jeep Cherokee 217
 John the Ripper 122, 127, 348

K

Kali Linux 178, 248, 292
 Kennwort
 Schwachstellen 116
 Social Engineering 119
 Speicherort 123

suchen 132
 zurücksetzen 136
 Kennwortablage
 Linux/Unix 124
 unsichere 132
 Windows 123
 Kennwort knacken 41, 115, 118, 125
 BIOS 135
 Datenbank 323
 iOS 213
 Laptops 206
 Linux 128, 207
 Netzwerkanalysator 133
 pwdumpx 127
 Rainbow 126
 Software 121
 Unix 128, 207
 Windows 127
 Wörterbuch 124
 Kennwortphrase 115
 Kennwortverschlüsselung 123
 KeyGhost 132
 Keylogger 115, 131
 Keystroke Logging 131
 Kismet 178, 193
 Knoppix 207
 Kontensperrung 139

L

LACNIC 85
 LanGuard 71
 last | head 264
 LastPass 137
 Linux
 Aktualisierungsverwaltung 267
 Dateiberechtigungen 261
 Dienst deaktivieren 256
 Distributionen aktualisieren 267
 hosts.equiv 258
 Kennwort knacken 128, 207
 Patches 267
 .rhosts 258
 Schwachstellen 248
 Werkzeuge 248, 255
 Linux Mint 267
 Linux Security Auditing Tool 266
 Lippenleser 96
 Live-CD 178
 Local File Inclusion 302
 Lösegeldzahlung 172
 LoveBug (Wurm) 94
 LSAT 266

LUCY 97
 Lumension Patch and Remediation 244

M

MaaS360 212
 MAC-Adresse 166, 180, 199
 fälschen mit SMAC 170
 manipulieren mit ifconfig 169
 Spoofing 169
 Spoofing, Gegenmaßnahmen 171
 MAC-Spoofing 197
 Gegenmaßnahmen 200
 MafiaBoy 173
 Mailsnarf 286
 Malwarebytes 172
 ManageEngine 267
 master.mdf 323
 maxsize 301
 MBSA 223, 244
 MD5 123
 Media Access Control (MAC) 166, 197
 Metasploit 78, 222, 224, 263, 287, 291, 297
 Editionen 242
 Metasploit Console 239
 verwenden 238
 Microsoft Baseline Security Analyzer 223, 244
 Microsoft BitLocker 210
 Microsoft BitLocker Administration and Monitoring 112
 Microsoft Visio 61
 Microsoft-Werkzeuge 223
 Microsoft Windows Defender 172
 MITM-Angriff 166
 Mitnick, Kevin 49
 Mülltauchen 35, 87, 95
 MXToolBox 85

N

NAT 159
 National Vulnerability Database 118
 Nation-State-Angriff 171
 nbtstat 223, 228
 Nessus 297
 net 223
 NetBIOS (Network Basic Input/Output System) 228
 Hacks 228
 Hacks, Gegenmaßnahmen 230
 Ports 228

Netcat 158
 NetResident 164, 286
 NetScanTools Pro 72, 85,
 147, 153, 155, 174, 182,
 224–225, 249, 282
 Netsparker 41, 175, 254, 327
 netstat 223
 NetStumbler 181, 193, 197
 net view 233
 Network Address Translati-
 on (NAT) 176
 Network Analyzer Pro 179
 Network Attached Storage
 (NAS) 326
 Network File System (NFS)
 260
 Hacks 261
 Network Multimeter 179
 Network Security Toolkit
 178
 Netzwerkanalysator 133,
 147, 159
 Empfehlungen 160
 entdecken 166
 Kennwort knacken 133
 OmniPeek 133
 Verteidigungsmaßnahmen
 134
 Netzwerkinfrastruktur 147
 Ports scannen 149
 Scanner 147
 Schwachstellen 146
 Schwachstellenprüfung
 148
 Testwerkzeuge 147
 Nexpose 77, 148, 173, 175,
 183, 202, 224, 237, 244,
 250, 254, 282, 291, 297,
 322, 325, 327
 NFS 260
 Nmap 73, 148, 150, 152, 226,
 249, 255, 327, 348
 NMapWin 75, 148
 npasswd 141
 Nping 182
 ntds.dit 123
 NT-Hash 126
 NTOSpider 308
 Null Session 231
 Gegenmaßnahmen 233
 zuordnen 231

O

Obskürität 317
 OmniPeek 41, 73, 133, 148,
 179, 182, 193–194, 294
 OneDrive 36, 235
 OneDrive for Business 274
 OpenSSL 254
 ophcrack 122, 208

Ophcrack 41
 ophcrack-Live-CD 110
 Oracle 322
 OS fingerprint 251
 Outlook Web Access (OWA)
 289
 Outsourcing 349–350

P

Palo Alto Networks 172, 318
 Partikelschnitt 101
 PASS 134
 Passphrase 137
 Passware 207
 Passware Kit Forensic 207,
 211
 passwd+ 141
 passwd (Datei) 302
 Password Safe 137
 Patch 93, 236
 Verwaltung 244, 343
 Werkzeuge 343
 Payment Card Industry Data
 Security Standard (PCI
 DSS) 363
 Penetrationstest 23
 PGP (Pretty Good Privacy)
 42, 131, 288
 Phishing 39, 88, 97, 119
 durchführen 97
 Werkzeuge 97
 PHP (Hypertext Preproces-
 sor) 309
 PID 256
 Ping 72
 Ping of Death 173
 Ping Sweep 150
 ausführen 151
 pkgtool 267
 Poisoning 166
 POODLE (Padding Oracle On
 Downgraded Legacy En-
 cryption) 175
 POP3S 288
 Port
 offener 73
 scannen 149
 Port Address Translation
 (PAT) 176
 Portscan 146, 149
 Portscanner 73
 Funktionsweise 151
 PortSentry 251
 PPTP 189
 Privilege Escalation 325
 Proactive Password Auditor
 41, 122
 Proactive System Password
 Recovery 121–122, 207
 Probe-Request-Signal 182

PromiscDetect 134, 166
 Promiskuitiver Modus 160
 PROTOS 292
 PSK (Pre-Shared Key) 186
 Pufferüberlauf 263, 325
 PVS-Studio Analyzer 318
 pwddump3 122, 127
 pwddumpx 127
 Pwnie Express 110

Q

QualysGuard 77, 228, 249,
282

R

Rainbow 126
 RainbowCrack 122
 Rainbow-Tabelle 121–122
 Rangniedrigere 48
 Ransomware 31, 88, 172, 237
 RARP 196
 RC4 175, 184
 R-Dienste 254
 Real-Time Transport Proto-
 col (RTP) 291
 Reaver 190
 Reaver Pro 190
 Rechtheausweitung 325
 Red Hat 267
 Red Hat Package Manager
 (RPM) 267
 Red Team 59
 Regenbogenhautscanner 238
 Registrar-PIN 189
 Remailer 94
 Remote Cracking Utility 115
 Remote Desktop Protocol
 (RDP) 73
 Remoteverwaltung 154
 Reverse Address Resolution
 Protocol (RARP) 196
 RIAA (Recording Industry
 Association of America)
 52
 Richtlinienbeauftragter 24
 Richtmikrofon 96
 RIPE 86
 Risikoanalyse 60
 robots.txt 84, 301
 RPM 267

S

SAM (Security Account Ma-
 nager) 122, 123
 SANS 76
 SavviusOmniPeek 160
 SCADA (Supervisory Control
 And Data Acquisition) 60
 Scan, authentifizierter 244

- Schatten-IT 36
 - Schredder 101
 - Schwachstelle
 - bewerten 76
 - Datenbanken 325
 - Kennwörter 116
 - lokalisieren 105
 - Mobilgerät 205
 - Netzwerkinfrastruktur 146
 - Prioritäten 336
 - Windows 222
 - Schwachstelle, physische identifizieren 103
 - Schwachstellenscanner
 - Webanwendungen 296
 - Schwachstellentests
 - Arbeitsabläufe 38
 - Secure Shell (SSH) 73
 - Secur/Tree 61
 - sendmail 254
 - Sensitive Data Manager 330
 - ServerDefender 318
 - ServerMask 317
 - Service Set Identifier (SSID) 181
 - Session Initiation Protocol (SIP) 291
 - SetGID 261
 - SetUID 261
 - SHA-1 175
 - SHA-2 176
 - SHA2 123
 - Shadow-Password-Datei 265
 - ShareFile 235
 - Share Finder 229
 - Shoulder Surfing 115, 118, 120
 - Sicherheit durch Unklarheit 317
 - Sicherheitsinfrastruktur prüfen 345
 - Sicherheitsschulung 100
 - Sicherheitsvorkehrung physische 103
 - SIEM (Security Incident and Event Management) 348
 - Simple Mail Transfer Protocol (SMTP) 278
 - Relay 281
 - Relay-Angriffe, Gegenmaßnahmen 284
 - sipsak 292
 - Site
 - Google Hacking Database (GHDB) 300
 - Skript Kiddies 46
 - Fähigkeiten 48
 - Skriptvirus 94
 - Slackware 267
 - SMAC 170
 - SmartDraw 61
 - SmartWhois 85
 - SMB Scanner 225
 - SMB (Server Message Block) 225
 - S/MIME 288
 - Smishing 98
 - SMTTP-Relays 274
 - SMTSPS 288
 - smtpscan 277
 - SnagIt 70
 - SNARE 251
 - sniffdet 134, 166
 - Sniffer 160
 - SNMP (Simple Network Management Protocol) 154
 - scannen 154
 - Schwachstellen 155
 - Werkzeuge 155
 - SNMPUTIL 155
 - Snowden, Edward 31, 37
 - Social Engineering 35, 87
 - Angriff durchführen 94
 - Beispiele 88
 - Gegenmaßnahmen 98
 - Kennwörter knacken 119
 - umgekehrtes 92
 - SoftPerfect Network Scanner 156
 - SolarWinds Network Configuration Manager 159
 - Soziale Manipulation 35
 - Sozialtechniken 87
 - Spam Blacklist 85
 - Spear-Phishing 88
 - Spector Pro 132
 - Speichersystem 326
 - Testwerkzeuge 327
 - Spider 298
 - SPI Proxy 304
 - SPI (Stateful Packet Inspection) 159
 - Spoofing
 - MAC 197
 - MAC, Gegenmaßnahmen 200
 - Spoofing 93
 - ARP 166
 - Gegenmaßnahmen 171
 - MAC-Adresse 169
 - Sprachfreigabe 216
 - SQL-Einschleusung 306
 - SQL Injection 78, 306
 - SQL Inject Me 307
 - SQLPing3 123, 322
 - SQL Power Injector 307
 - SQL Server 323
 - SSAE16 SOC 2 364
 - SSID 181
 - SSL Labs 175
 - SSL (Secure Sockets Layer) 35, 146, 175
 - Stateful Packet Inspection (SPI) 175
 - Storage Area Network (SAN) 326
 - Symantec 264, 276
 - SYN-Floods 173
 - Sysinternals 223
- ## T
- Tablet
 - knacken 211
 - Task Scheduler 348
 - tcpdump 294
 - TCPView 224
 - TCP Wrappers 258
 - Telefon
 - Identität verheimlichen 96
 - knacken 211
 - Telefonsystem 96
 - Telnet 157
 - Temporal Key Integrity Protocol (TKIP) 186
 - Test
 - Planung 57
 - Rahmenplan 39
 - vorbereiten 69
 - Zeitplan 63
 - Teststandard 62
 - THC-Hydra 122, 313
 - theHarvester 280
 - Tiger 266
 - Tiger Team 59
 - TLS 288
 - Tool 66
 - Transmission Control Protocol (TCP) 149
 - Transport Layer Security (TLS) 175, 288, 298
 - Tripwire 260, 263
 - Trojaner 93
 - TrueCrypt 211
- ## U
- Ubuntu 267
 - UDPFlood 174
 - UEFI (Unified Extensible Firmware Interface) 135, 211
 - Unified Threat Management (UTM) 71
 - Unix 248
 - Kennwort knacken 128, 207
 - MAC-Adressen manipulieren 169

update 267
 Update-Manager 267
 URL-Redirection 303
 User Datagram Protocol
 (UDP) 149
 USV 108

V

Verizon Data Breach Investi-
 gations Report 342
 Verschlüsselungstrojaner
 172
 Versicherung 59
 VirtualBox 72
 Virtual Network Computing
 (VNC) 73
 Visio (Zeichenprogramm)
 345
 Visual Code Grepper 318
 VLAN 291
 VMware-Workstation 223
 VNC 111
 Voicemail 96
 Voice over Internet Protocol
 (VoIP) 289
 Gespräche aufzeichnen
 292
 Netzwerkanalysator 294
 Schwachstellen 289, 290,
 291
 Schwachstellen, Gegen-
 maßnahmen 294
 Voice over IP 289
 VoIP Hopper 291
 vomit 294

W

WannaCry 237
 WannaCry (Ransomware)
 225
 WatchGuard 318
 WatchGuard Technologies
 331
 Web
 Anmeldung, unsichere 311
 Buffer Overflow 301

Code Injection 305
 Cross-site Scripting 307
 Standardskripte 309
 URL-Manipulation 302
 verborgene Felder 304
 Web 2.0
 hacken 316
 Werkzeuge 316
 Webanwendung, Testwerk-
 zeuge 296
 Webcrawler 83
 Webcrawling 83
 Webproxy 302
 Webroot 172
 Webserver, Softwareversion
 74
 Websicherheit
 Crawler 298
 Google 299
 Wellenreiter 178
 WEP 184
 WEPCrack 185
 Werkzeug 40, 66
 Beispiele 42
 White Hat 30
 Whois 84
 WiEye 179
 Wi-Fi 177
 WiFi Analyzer 179
 WiFi Pineapple 182
 Wi-Fi Protected Access
 (WPA) 184, 186
 Wi-Fi Protected Setup (WPS)
 183, 189
 Angriffe 190
 Windows 221
 Freigaben 229
 Kennwort knacken 127
 MAC-Adressen fälschen
 170
 Null Sessions 231
 Portscan 225
 Schwachstellen 222
 System untersuchen 225
 Version herausfinden 226
 Werkzeuge 222
 Windows 10

Sicherheit 238
 Windows-Freigabe 234
 Windows Hello 238
 Winfo 224, 233
 WinHex 139, 207, 310
 WinMagic 264
 WinMagic SecureDoc 211
 WinMagic SecureDoc Full
 Disk Encryption 112
 WinNuke 173
 WinZip 127
 WIPS (Wireless Intruder
 Prevention System) 196
 Wired Equivalent Privacy
 (WEP) 184
 Wireless Intrusion Preventi-
 on System (WIPS) 196
 Wireshark 41, 73, 133, 148,
 161
 WLAN 177
 Antenne 179
 entdecken 179
 Verkehr, verschlüsselter
 184
 Verschlüsselungsproto-
 kolle 184
 WLAN-Angriffe
 Gegenmaßnahmen 182
 WordPress 311
 Wörterbuch
 Angriff mit 124
 Wörterbuchdatei 187
 Wortliste 124
 WPA2 186
 WPA3 186
 WPS 183
 WPS-PIN 190
 WSUS 244

X

XSS 307
 XSS-Me 308

Z

Zombie 55
 Zugriffskontrollliste 261