

Stichwortverzeichnis

Symbols

7-zip 128
/etc/passwd« 142

A

Abschlussbericht 70
Access Control List (ACL)
 263
AccessEnum 209
Active Directory 224
Active Server
 Pages (ASP) 314
Acunetix Web Vulnerability
 Scanner 41, 205, 300, 319,
 331
Advanced EFS Data Recovery
 209
Advanced Office Password
 Recovery 328
Advanced Persistent Threat
 (APT) 172
Advanced SQL Password
 Recovery 326
Adware 215
AES (Advanced Encryption
 Standard) 132, 189, 192
AfriNIC 85
Aircrack-ng 181, 187, 352
airodump 188
AirWatch 215
Aktenvernichter 102
Angewandte
 Sozialwissenschaften 87
Angriff 34
 Anwendungen 36
 Betriebssystem 36
 Directory Traversal 301
 nicht-technischer 35
 planen 53
 Standardskripte 314
Angriff
 Netzwerkinfrastruktur 35
Angriffsbaum 61
Angriffserkennungssystem 70

Anmeldung, unsichere im
 Web 316
Anreiz 357
AP (Access Point) 181
APNIC 85
AppDetectivePro 329
AppSpider 313
Archive Password
 Recovery 131
ARIN 86
ARP 167
 Poisoning 166–167
 Poisoning mit Cain & Abel
 168
 Spoofing 166–167
 Tabellen 167
AT-Befehl 352
Auditierung 32
Auftragshacker 50
Authentifizierung
 schwache 121
 umgehen 121

B

Backdoor 94
Bandbreitenblockade 275
Banner-Grabbing 157
 Gegenmaßnahmen 158
Barracuda Networks 278, 322
Bastille UNIX 269
Benutzer, böswilliger 31
Bericht erstellen 342
Berichtswesen 339
Bildschirmaktion aufzeichnen
 64
Bildschirmsperre 213
Biometrisches
 Erkennungssystem 110
BIOS-Kennwörter 136
BitLocker 112, 213
BKA-Trojaner 101
Black Hat 30
Black Hat Conference 49
Blast 175
Blindtest 71

Blooover 186
Blue Hat 49
Bluelog 186
BlueScanner 186
Bluesnarfer 186
BlueSniper rifle 187
Bluetooth 186
Bot 55
Brute-Force-Angriff 125
Brutus 122–123, 290, 316
BSD (Berkeley Software
 Distribution) 261
BSD-r-Befehl 262
Btscanner 187
Buffer Overflow 266, 306, 329
Bulk Eraser 113
Bundestag 97
Burp Proxy 300, 306, 309

C

C|EH 32
Cain & Abel 121–122, 134,
 147, 161, 167, 288, 294, 326
 ARP-Poisoning 168
Cain and Abel 111
Camtasia 70
Camtasia Studio 64
CAPTCHA 278
Car Whisperer 187
Cb Protection 133
CCMP 189
Challenge-Response-
 Verfahren 137
Checksum Tool 67
Cheops-ng
 (Zeichenprogramm) 350
Cisco 330
Client Hyper-V 72
Cloudflare 322
Code Injection 309
Cofense 98
CommView 175
Common Gateway Interface
 (CGI) 261
CommView 135, 161, 296

- CommView for WiFi 181, 184, 195, 198
 - Compliance 32
 - Content Management System (CMS) 299, 314
 - COPS 265
 - Cracker 30
 - cracklib 142
 - Crawler 302
 - Cross-site Scripting (XSS) 101, 312
 - prüfen auf 312
 - CryptoLocker 173
 - CryptoWall 173
 - Cyberterrorist 50
 - Cylance 173
- D**
- Daemon 251
 - auskommentieren 258
 - suchen 256
 - Dark Web 53
 - Datenbank 325
 - Kennwörter knacken 327
 - Schwachstellen 329
 - Werkzeuge 326
 - Datenschutz-
 - Grundverordnung 368
 - Datenschutzrichtlinie 86
 - Debian 270
 - Deep Freeze Enterprise 133
 - Deep Web 53
 - Demilitarisierte Zone 147, 204, 331
 - Denial of Service 35, 174
 - Angriff 174
 - Angriff,
 - Gegenmaßnahmen 175
 - E-Mail-Anhänge 274
 - Kondition 274
 - Testwerkzeuge« 175
 - DHA 280
 - Dial-by-Name 96
 - Dienstblockade 35
 - DIN 32757 102
 - Dipolantenne 181
 - Directory-Harvest-Angriff 280
 - Directory Traversal 301
 - Gegenmaßnahmen 305
 - disallow-Eintrag 84
 - Display-Sperre 219
 - Distributed DoS (DDoS) 174
 - DLP (Data Loss Prevention) 352
 - DNSstuff 85
 - Domain Factory 85
 - DoS 35
 - dpkg 270
 - Dropbox for Business 276
 - DSGVO 368
 - dsniff 167
 - DumpSec 140, 235
 - Dumpster Diving 35, 88, 95
 - Dumpstern 88
- E**
- E-Commerce 278
 - Ecora Patch Manager 348
 - Effective File Search 332
 - EICAR 289
 - Eingabeaufforderung 243
 - Eingabefilter 312
 - Eingabepprüfung 305
 - Elcomsoft Advanced SQL Password Recovery 328
 - Elcomsoft Distributed Password Recovery 122, 328
 - Elcomsoft Forensic Disk Decryptor 213
 - Elcomsoft Phone Password Breaker 218
 - Elcomsoft System Recovery 122, 208
 - Elcomsoft Wireless Security Auditor 181, 190
 - E-Mail
 - Angriffe 274, 290
 - Banner-Angriffe 278, 280
 - Bomben 274
 - Firewalls 278
 - Header 287
 - Malware 289
 - Postfix 291
 - gmail 291
 - Sendmail 291
 - Sicherheitskontrollen 278
 - SMTP 280
 - Tarpit 278
 - Teergrube 278
 - Verkehr abfangen 288
 - E-Mail-Header 76
 - EmailVerify 282
 - Enterprise Full Disk Encryption 113
 - Essential NetTools 147, 155, 282
 - Ethereal 161
 - ettercap 161
 - EU-DSGVO 52
 - EWSA 190
 - Exploit 35, 70
- F**
- Face Unlock 219
 - FAQ (Frequently Asked Questions) 41
 - Fedora 270
 - Fehler 404 75
 - Fernsteuerung 88
 - Fernwartungsprogramm 111
 - Festplattenverschlüsselung 212
 - FIFO-Puffer 163
 - FileLocator Pro 133, 331–332
 - FileVault 113
 - FileVault2 210, 213
 - findstr 133
 - Fingerabdruckscanner 241
 - Fingerbewegung 219
 - Display-sperre 219
 - Firefox Web Developer 300, 306
 - Firemon Risk Analyzer 159
 - Firewall 160
 - E-Mail 278
 - Regeln 158
 - testen 158
 - FMEA (Failure Mode and Effects Analysis) 61
 - Footprinting 71
 - Fortinet 322, 330, 335
 - Fortres 101 133
 - fping 73
 - FREAK (Factoring Attack on RSA-EXPORT Keys) 176
 - Free Kevin 50
 - Freigabeberechtigung 237
- G**
- Gantt 63
 - Gebäude 105
 - Angriffspunkte 105
 - Gegenmaßnahmen 106
 - Versorgung 107

Gebäudeschwachstelle 106
 Gesichtserkennung 219
 Getif 148, 155
 GFI EventsManager 353
 GFI LanGuard 71, 77, 185,
 205, 226–227, 230, 238,
 246–247, 270, 348
 GFI LANguard 148
 GHDB 304
 Glassdoor 82
 GNU MAC Changer
 171, 202
 Google 304
 erweiterte Suche 304
 suchen mit 83
 Google Drive 36
 Google Hack Honeypot
 305
 Google Kontakt 304
 GPS (Global Positioning
 System) 369
 Gray Hat 31, 49
 grep 133

H

H.323 294
 Hacken
 Abläufe automatisieren
 351
 ethisches 23
 Hacken, ethisches
 Richtlinien 33
 Hacker 29–30
 Denkweise 46
 Fähigkeiten 48
 geläuterter 356
 klassifizieren 45
 Hacktivist 49
 Hash 122
 Heartbleed 176
 Hintertür 94
 Hörgerät 96
 Hotspotter 198
 htaccess 305
 htdocs 305
 httpd.conf 305
 HTTP (Hypertext Transfer
 Protocol) 301
 HTTrack Website Copier
 83, 302
 Hyper-V 72

I

IceWarp 277
 ICMP 151
 IdentityFinder 334
 Idera 330
 IDS (Intrusion
 Detection Systems) 63
 IMAPS 290
 Imperva 330
 Inferenz 120
 Informationsbeschaffung 71
 Initialisierungsvektor (IV) 187
 inSSIDer 184
 Internetbanking 133
 Internet der Dinge 54, 220
 Internet Information Services
 Manager 305
 Internet of Things 220
 Internetquellen 280
 Intrusion Detection System
 (IDS) 70–71
 Intrusion Prevention System
 (IPS) 54, 63, 71, 152, 155
 iOS
 Kennwörter knacken 215
 iOS Forensic Toolkit
 Verwendung 215
 IoT 220
 IoT (Internet der Dinge)
 299
 IoT (Internet of Things) 54
 IP Personality 322
 IPS (Intrusion Prevention
 System) 352
 IPv6-Adresse 73
 IRC 53
 Iriscanner 241
 ISO/IEC 27001:2017 58

J

Jeep Cherokee 220
 John the Ripper 122, 127, 352

K

Kali Linux 181, 251, 294
 KeePass Password Safe 138
 Kennwort
 Schwachstellen 116
 Social Engineering 119
 Speicherort 124

suchen 133
 zurücksetzen 137
 Kennwortablage
 Linux/Unix 124
 unsichere 133
 Windows 124
 Kennwort knacken 41, 115,
 118, 125
 BIOS 136
 Datenbank 327
 iOS 215
 Laptops 208
 Linux 129, 210
 Netzwerkanalysator 134
 pwddumpx 127
 Rainbow 127
 Software 122
 Unix 129, 210
 Windows 127
 Wörterbuch 125
 Kennwortphrase 115
 Kennwortverschlüsselung
 123
 KeyGhost 132
 Keylogger 115, 132
 Keystroke Logging 132
 Kismet 180, 196
 Knoppix 210
 Kontensperrung 140

L

LACNIC 86
 LanGuard 71
 last | head 268
 LastPass 138
 Linux
 Aktualisierungsverwaltung
 270
 Dateiberechtigungen 264
 Dienst deaktivieren 258
 Distributionen
 aktualisieren 270
 hosts.equiv 261
 Kennwort knacken 129, 210
 Patches 269
 .rhosts 261
 Schwachstellen 250
 Werkzeuge 250, 257
 Linux Mint 270
 Linux Security Auditing
 Tool 269

Lippenleser 96
 Live-CD 181
 Local File Inclusion 307
 Lösegeldzahlung 173
 LoveBug (Wurm) 94
 LSAT 269
 LUCY 98
 Lumension Patch and Remediation 246

M

MaaS360 215
 MAC-Adresse 167, 182, 202
 fälschen mit SMAC 171
 manipulieren mit ifconfig 170
 Spoofing 170
 Spoofing,
 Gegenmaßnahmen 172
 MAC-Spoofing 200
 Gegenmaßnahmen 204
 MafiaBoy 174
 Mailsnarf 288
 Malwarebytes 173
 ManageEngine 270
 master.mdf 328
 maxsize 306
 MBSA 225, 248
 MD5 123
 Media Access Control (MAC) 167, 200
 Metasploit 78, 224, 226, 266, 290, 294, 301
 Editionen 244
 Metasploit Console 241
 verwenden 241
 Microfocus Data Collection 353
 Microsoft Baseline Security Analyzer 225, 248
 Microsoft BitLocker 212
 Microsoft BitLocker Administration and Monitoring 113
 Microsoft Visio 61
 Microsoft-Werkzeuge 225
 Microsoft Windows Defender 173
 MITM-Angriff 167
 Mitnick, Kevin 50
 Mülltauchen 35, 88, 95
 MXToolBox 85

N

NAT 159
 National Vulnerability Database 118
 Nation-State-Angriff 172
 nbtstat 225, 230
 Nessus 301
 Nessus Pro 251
 net 225
 NetBIOS (Network Basic Input/Output System) 230
 Hacks 230
 Hacks, Gegenmaßnahmen 232
 Ports 230
 Netcat 158
 NetResident 166, 288
 NetScanTools Pro 73, 85, 147, 154–155, 185, 226–227, 251–252, 284
 Netsparker 41, 176, 257, 331
 netstat 225
 NetStumbler 184, 195, 200
 net view 235
 Network Address Translation (NAT) 177
 Network Analyzer Pro 181
 Network Attached Storage (NAS) 330
 Network File System (NFS) 263
 Hacks 263
 Network Multimeter 181
 Network Security Toolkit 181
 Netzwerkanalysator 135, 147, 160
 Empfehlungen 161
 entdecken 166
 Kennwort knacken 134
 OmniPeek 135
 Verteidigungsmaßnahmen 135
 Netzwerkinfrastruktur 147
 Ports scannen 149
 Scanner 147
 Schwachstellen 146
 Schwachstellenprüfung 148
 Testwerkzeuge 147
 Nexpose 77, 148, 174, 176, 185, 205, 226, 230, 239, 247, 252, 257, 284, 301, 326, 329, 331

NFS 263
 Nmap 73, 148, 151–152, 228, 251, 257, 331, 352
 NMap 76
 NMapWin 148
 npasswd 142
 Nping 185
 ntds.dit 124
 NT-Hash 127
 NTOSpider 313
 Null Session 233
 Gegenmaßnahmen 236
 zuordnen 233

O

Obskürität 321
 OmniPeek 41, 73, 135, 148, 181, 184, 195–196, 296
 OneDrive 36, 238
 OneDrive for Business 276
 OpenSSL 256
 Ophcrack 41, 122, 210
 ophcrack-Live-CD 110
 Oracle 327
 OS fingerprint 253
 Outlook Web Access (OWA) 291
 Outpost24 110
 Outsourcing 353–354

P

Palo Alto Networks 173, 322
 Partikelschnitt 102
 PASS 135
 Passphrase 138
 Passware 209
 Passware Kit Forensic 210, 213
 passwd+ 142
 passwd (Datei) 307
 Password Safe 138
 Patch 93, 239
 Verwaltung 246, 347
 Werkzeuge 347
 Payment Card Industry Data Security Standard (PCI DSS) 367
 Penetrationstest 23
 PGP (Pretty Good Piracy) 131
 PGP (Pretty Good Privacy) 43, 290

- Phishing 39, 88, 97, 119
 - durchführen 97
 - Werkzeuge 98
 - PHP (Hypertext Preprocessor) 314
 - PID 258
 - Ping 73
 - Ping of Death 174
 - Ping Sweep 151
 - ausführen 151
 - pkgtool 270
 - Poisoning 167
 - POODLE (Padding Oracle On Downgraded Legacy Encryption) 176
 - POP3S 290
 - Port
 - offener 73
 - scannen 149
 - Port Address Translation (PAT) 177
 - Portscan 146, 149
 - Portscanner 73
 - Funktionsweise 152
 - PortSentry 255
 - PPTP 191
 - Privilege Escalation 329
 - Proactive Password Auditor 41, 122
 - Proactive System Password Recovery 121–122, 209
 - Probe-Request-Signal 184
 - PromiscDetect 135, 166
 - Promiskuitiver Modus 160
 - PROTOS 294
 - PSK (Pre-Shared Key) 189
 - Pufferüberlauf 266, 329
 - PVS-Studio Analyzer 323
 - pwdump3 122, 127
 - pwdumpx 127
- Q**
- Qualys Cloud Platform 77
 - QualysGuard 284
 - Quest KACE Systems 270
- R**
- Rainbow 127
 - RainbowCrack 123
 - Rainbow-Tabelle 121–122
 - Rangniedrigere 49
 - Ransomware 31, 88, 173, 239
 - RARP 199
 - RC4 176, 187
 - R-Dienste 256
 - Real-Time Transport Protocol (RTP) 293
 - Reaver 193
 - Reaver Pro 193
 - Rechtheausweitung 329
 - Red Hat 270
 - Red Hat Package Manager (RPM) 270
 - Red Team 59
 - Regenbogenhautscanner 241
 - Registrar-PIN 193
 - Remailer 94
 - Remote Cracking Utility 115
 - Remote Desktop Protocol (RDP) 74
 - Remoteverwaltung 155
 - Reverse Address Resolution Protocol (RARP) 199
 - RIAA (Recording Industry Association of America) 53
 - Richtlinienbeauftragter 24
 - Richtmikrofon 96
 - RIPE 86
 - Risikoanalyse 60
 - robots.txt 84, 305
 - RPM 270
- S**
- SAM (Security Account Manager) 122
 - SAM (Security Account Manager) 124
 - SANS 77
 - SavviusOmniPeek 161
 - SCADA (Supervisory Control And Data Acquisition) 60
 - Scan, authentifizierter 247
 - Schatten-IT 36
 - Schredder 102
 - Schwachstelle
 - bewerten 76
 - Datenbanken 329
 - Kennwörter 116
 - lokalisieren 105
 - Mobilgerät 207
 - Netzwerkinfrastruktur 146
 - Windows 224
 - Schwachstelle
 - Prioritäten 341
 - Schwachstellenscanner
 - Webanwendungen 300
 - Schwachstellentests
 - Arbeitsabläufe 38
 - Schwachstelle, physische identifizieren 104
 - Secure Shell (SSH) 74
 - Secur/Tree 61
 - sendmail 256
 - Sensitive Data Manager 334
 - ServerMask 322
 - Service Set Identifier (SSID) 183
 - Session Initiation Protocol (SIP) 293
 - SetGID 264
 - SetUID 264
 - SHA-1 176
 - SHA-2 177
 - SHA2 123
 - Shadow-Password-Datei 268
 - ShareFile 238
 - Share Finder 231
 - Shoulder Surfing 115, 118, 120
 - Sicherheit durch Unklarheit 321
 - Sicherheitsinfrastruktur prüfen 349
 - Sicherheitsschulung 100
 - Sicherheitsvorkehrung physische 103
 - SIEM (Security Incident and Event Management) 352
 - Simple Mail Transfer Protocol (SMTP) 280
 - Relay 284
 - Relay-Angriffe, Gegenmaßnahmen 287
 - sipsak 294
 - Site
 - Google Hacking Database (GHDB) 304

- Skript Kiddies 46
 - Fähigkeiten 48
 - Skriptvirus 94
 - Slackware 270
 - SMAC 171
 - SmartDraw 61
 - SmartWhois 85
 - SMB Scanner 227
 - SMB (Server Message Block) 227
 - S/MIME 290
 - Smishing 99
 - SMTP-Relays 276
 - SMTPS 290
 - smtpscan 279
 - SnagIt 70
 - SNARE 255
 - sniffdet 135, 166
 - Sniffer 160
 - SNMP (Simple Network Management Protocol) 155
 - scannen 155
 - Schwachstellen 155
 - Werkzeuge 155
 - SNMPUTIL 156
 - Snowden, Edward 31, 37
 - Social Engineering 35, 87
 - Angriff durchführen 94
 - Beispiele 88
 - Gegenmaßnahmen 99
 - Kennwörter knacken 119
 - umgekehrtes 93
 - SoftPerfect Network Scanner 157
 - SolarWinds Network Configuration Manager 159
 - Soziale Manipulation 35
 - Sozialtechniken 87
 - Spam Denylist 85
 - Spear-Phishing 88
 - Speichersystem 330
 - Testwerkzeuge 331
 - Spider 302
 - SPI Proxy 309
 - SPI (Stateful Packet Inspection) 160
 - Spoofing 93
 - ARP 167
 - Gegenmaßnahmen 172
 - MAC 200
 - MAC-Adresse 170
 - MAC, Gegenmaßnahmen 204
 - Sprachfreigabe 219
 - SQL-Einschleusung 310
 - SQL Injection 78, 310–311
 - SQLPing3 123, 326
 - SQL Power Injector 312
 - SQL Server 328
 - SSAE16 SOC 2 368
 - SSID 183
 - SSL Labs 177
 - SSL (Secure Sockets Layer) 35, 146, 176
 - Stateful Packet Inspection (SPI) 177
 - Storage Area Network (SAN) 330
 - Symantec 268, 278
 - SYN-Floods 174
 - Sysinternals 226
- T**
- Tablet
 - knacken 214
 - Task Scheduler 352
 - tcpdump 296
 - TCPView 226
 - TCP Wrappers 260
 - Telefon
 - Identität
 - verheimlichen 97
 - knacken 214
 - Telefonsystem 96
 - Telnet 158
 - Temporal Key Integrity Protocol (TKIP) 189
 - Test
 - Planung 57
 - Rahmenplan« 39
 - vorbereiten 69
 - Zeitplan 63
 - Teststandard 62
 - THC-Hydra 123, 317
 - theHarvester 282
 - Tiger 268
 - Tiger Team 59
 - TLS 290
 - Tool 67
 - Transmission Control Protocol (TCP) 149
 - Transport Layer Security (TLS) 176, 290, 302
 - Tripwire 263, 265
 - Trojaner 94
 - TrueCrypt 213
- U**
- Ubuntu 270
 - UDPFlood 175
 - UEFI (Unified Extensible Firmware Interface) 136, 213
 - Unified Threat Management (UTM) 71
 - Unix 250
 - Kennwort knacken 129, 210
 - MAC-Adressen manipulieren 170
 - up2date 270
 - Update-Manager 270
 - URL-Redirection 308
 - User Datagram Protocol (UDP) 149
 - USV 108
- V**
- VeraCrypt 213
 - Veratio Vision 132
 - Verizon Data Breach Investigations Report 346
 - Verschlüsselungstrojaner 173
 - VirtualBox 72
 - Virtual Network Computing (VNC) 74
 - Visio (Zeichenprogramm) 350
 - Visual Code Grepper 323
 - VLAN 293
 - VMware-Workstation 225
 - VNC 111
 - Voicemail 96–97
 - Voice over Internet Protocol (VoIP) 292
 - Gespräche aufzeichnen 294
 - Netzwerkanalysator 296
 - Schwachstellen 292, 294
 - Schwachstellen, Gegenmaßnahmen 296
 - Voice over IP 292
 - VoIP Hopper 293
 - vomit 296

W

WannaCry (Ransomware)
 228, 239
 WatchGuard 322
 WatchGuard Technologies
 335
 Web
 Anmeldung, unsichere 316
 Buffer Overflow 306
 Code Injection 309
 Cross-site Scripting 312
 Standardskripte 314
 URL-Manipulation 307
 verborgene Felder 308
 Web 2.0
 hacken 320
 Werkzeuge 321
 Webanwendung,
 Testwerkzeuge 300
 Webcrawler 83
 Webcrawling 84
 Webproxy 306
 Webroot 173
 Webserver, Softwareversion
 75
 Websicherheit
 Crawler 302
 Google 304
 Wellenreiter 180
 WEP 187
 WEPCrack 187
 Werkzeug 41, 67
 Beispiele 42

White Hat 30
 Whois 85
 WiEye 181
 Wi-Fi 179
 WiFi Analyzer 181
 WiFi Pineapple 185
 Wi-Fi Protected Access
 (WPA) 187, 189
 Wi-Fi Protected
 Setup (WPS) 185, 193
 Angriffe 193
 Windows 223
 Freigaben 231
 Kennwort knacken 127
 MAC-Adressen fälschen 171
 Null Sessions 233
 Portscan 227
 Schwachstellen 224
 System untersuchen 227
 Version herausfinden 228
 Werkzeuge 225
 Windows 10
 Sicherheit 240
 Windows-Freigabe 237
 Windows Hello 241
 Winfo 226, 235
 WinHex 140, 209, 314
 WinMagic 268
 WinMagic SecureDoc 213
 WinNuke 174
 WinZip 128
 WIPS (Wireless Intruder
 Prevention System) 198

Wired Equivalent
 Privacy (WEP) 187
 Wireless Intrusion Prevention
 System (WIPS) 199
 Wireshark 41, 73, 135, 148,
 161
 WLAN 179
 Antenne 181
 entdecken 182
 Verkehr, verschlüsselter
 187
 Verschlüsselungsprotokolle
 187
 WLAN-Angriffe
 Gegenmaßnahmen 185
 WordPress 316
 Wörterbuch
 Angriff mit 125
 Wörterbuchdatei 190
 Wortliste 125
 WPA2 189
 WPA3 189
 WPS 185
 WPS-PIN 193
 WSUS 246

X

XSS 312

Z

Zombie 55
 Zugriffskontrollliste 263

