



Stichwortverzeichnis

1password2john 147
 4-Way-Handshake 273
 7-Zip 38
 7z 145
 7z2john 147

A

Address Resolution Protocol 63
 AFP 134
 airdecap-ng (Tool) 264
 aireplay-ng (Tool) 245, 250
 airmon-ng (Tool) 244
 airodump-ng (Tool) 248
 andOTP 145
 Android 33
 AndroidBackup 145
 androidbackup2john 147
 Anmeldedaten 50
 Arch Linux 391
 ArchStrike 393
 argon2 145
 ARM 32
 ARP 63
 Poisoning 301
 Spoofing 301
 arp-scan (Tool) 66
 arping (Tool) 63
 arpspoof (Tool) 302
 ASN 78
 Asterisk 134
 Autonomous System Number 78
 Autopsy (Tool) 362

B

Backbox 392
 Backdoor 97
 BackTrack 31
 Bare Metal 32
 bcrypt 145
 Beacon Flooding 268
 Beacons 247
 Benutzernamen 50
 berate_ap (Tool) 271
 bettercap (Tool) 256, 311
 Bildmanipulation 355

Bildrauschen 356
 Bitcoin 102, 145
 bitcoin2john 147
 BitLocker 145
 bitlocker2john 147
 Bitwarden 145
 bitwarden2john 147
 BlackArch 391
 Brute Force 128, 135, 151, 231
 BSSID 248
 Bulk Extractor (Tool) 339
 Burp Suite (Tool) 182

C

Cache 180
 CAINE 392
 CeWL (Tool) 121
 checkfy 105
 cisco2john 147
 CMS 172, 204
 Command Injection 213
 commix (Tool) 223
 Computer-Forensik 321
 Container 33
 Content Security Policy 223
 Content-Management-System 172, 204
 Cookie 177, 195
 http-only 223
 CRC32 145
 Cross-Site-Scripting 191, 212
 crunch (Tool) 116
 CUPP (Tool) 125
 CVS 137, 140

D

Datenbankmanagementsystem (DBMS) 216
 DB Browser for SQLite (Tool) 371
 DBMS 216
 dc3dd (Tool) 328
 dd (Tool) 327
 DDNS 84
 ddrescue (Tool) 340
 Deauthentication 250

Debian 31, 394
 Dev Tools (Tool) 178
 DHCP 48
 Digitale Forensik 32, 321
 dirb (Tool) 165
 dirbuster (Tool) 166
 Directory-Enumeration 168
 diskcryptor2john 147
 Displaygröße 52
 Distributionen 391
 dmesg (Tool) 243
 dmitry (Tool) 84
 DNS 79, 141
 A-Record 81
 AAAA-Record 81
 MX-Record 80
 NS-Record 80
 Records 80
 SOA-Record 80
 TXT-Record 81
 DNSDumpster (Tool) 83
 dnsmap (Tool) 82
 dnsmasq 271
 DNSRecon (Tool) 79
 Domain Name System (DNS) 79
 domainfy 105
 Downgrade-Attack 201
 Driftnet (Tool) 308
 dsniff (Tool) 302
 dumpzilla (tool) 370
 DVWA 57
 Dynamische IP-Adresse 84
 DynDNS 84

E

E-Mail-Adressen 99
 EAP-TLS 280
 EAP-TTLS 280
 EAPHammer (Tool) 279
 Ethereum 145
 ethereum2john 147
 Evil Twin 271
 ExifTool (Tool) 348, 352
 exiv2 (Tool) 352
 Exploit 96
 Ext-Dateisysteme 340





406 Stichwortverzeichnis

Ext-Dateisysteme 340
extundelete (Tool) 340

F

FCrackZip (Tool) 127
fdisk (Tool) 326
Fedora 393
Fedora Security Lab 392
ffuf (Tool) 227
File Carving 334
File Transfer Protocol (FTP)
134
Firefox 370
Firewall 95
Foremost (Tool) 336
Forensics 388
Forensics Mode 325
Forensische Sicherung 328
fping (Tool) 68
FQDN 169
fsck (Tool) 340
FTP 134, 137, 140, 141
Fully qualified domain names
169
Fuzzer 226

G

Gentoo 392
Geo Location 85
GET 177
gobuster (Tool) 168
gpg 145
guymager (Tool) 330

H

Hardware-Write-Blocker 324
Hash 143, 328
hash-identifier (Tool) 144
hashcat (Tool) 149, 261
hcxtools (Tool) 260
Hops 76
hostapd 271
hping3 (Tool) 95
HTML 179
HTTP 134, 176
Body 176
GET 177
Header 176
Message-Body 177
POST 177
HTTP-Header 172, 177
HTTP-StatusCode 164

httponly 195
HTTPS 200
HTTPSServer 172
Hydra (Tool) 133
Hypervisor 35

I

ICMP 62
ICMP-Echo-Ping-Scan 72
IEEE 802.11, 241
IMAP 134, 137, 140, 141
Information Gathering 61,
379
Injection 191
Installer 34
Internet Control Message
Protocol 62
Internet-Sharing-Modus 273
IP-Adresse 84
IPGeoLocation (Tool) 85
iptables 304
IRC 134
IT-Forensik 320, 321
iw (Tool) 243

J

John the Ripper (Tool) 145
Joomla 210
JuiceShop 57

K

Kali Linux 31
Alternativen 391
Download 32
Installation 37
IP-Adresse 62
Update 56
KeePass 145
keepass2john 147
keystore 141

L

LDAP 134, 141
libreoffice2john 147
Login-Daten 50
Lokalisierung 85
lsusb (Tool) 243

M

MAC 65
MAC-Spoofing 269
mac2john 147

macchanger (Tool) 269
macOS 37
mailfy 105
Maltego (Tool) 109
Man-in-the-Middle (MitM)
274, 291
Maryam (Tool) 107
MASSCAN (Tool) 94
MD5 129, 281, 328
md5crypt 145
mdk4 (Tool) 251, 267
Media-Access-
Control-Adresse 65
Medusa (Tool) 139
MEMCACHED 134
Mentalist (Tool) 123
Meta-Packages 46
Metadaten 345
Metagoofil (tool) 349
Metasploit (Tool) 96
Metasploit-Framework 96
Metasploitable2 47
mitmproxy (Tool) 304
ModSecurity 171
MongoDB 134, 137, 145
Monitor Mode 244
Mozilla 145
Mozilla Firefox 370
mozilla2john 147
MQTT 137
MS-CHAPv2 281, 285
MSSQL 134, 137, 140, 141,
145
mtr (Tool) 77
MySQL 134, 137, 140, 141,
145

N

NAT-Netzwerk 48
Ncrack (Tool) 137
netdiscover (Tool) 69
NetHunter 33
NetInstaller 34
Network Security Toolkit
(NST) 393
Netzwerkconfiguration 48
Netzwerktopologieplan 74
nikto (Tool) 192
Nmap (Tool) 71, 88
Nmap Scripting Engine (NSE)
94
NNTP 134, 140



Stichwortverzeichnis 407

- NSE 94
Null-Scan 88
- O**
- OffSec* 31
office2john 147
Open Source Intelligence 99
openssl2john 147
Oracle 141
Organizationally Unique Identifier (OUI) 65
OS Detection 91
OSINT 99
OSRFramework (Tool) 105
OWASP 107
SamuraiWTF 393
- P**
- Packet Injection 245
ParrotOS 391
Partition 46
Passiver Scan 69
Password Attacks 379
Passwort 50
Passwortlisten 114
 Download 116
Patator (Tool) 141
pcanywhere 140
PDF 129, 145
 Owner Password 129
 User Password 129
pdf2john 147
PDFCrack (PDF) 129
PEAP 280
PEM 145
Penetrationstest 32
Pentest 32
Pentoo 392
pgsql 141
Phishing 275
phonefy 105
PhotoRec (Tool) 334
PHPSESSID 195
Ping 62
PMF 251
POODLE 201
POP3 134, 137, 140, 141
Port 87
 Scan 88
Portweiterleitung 49
POST 177
postgres 140, 145
- PostgreSQL 137
Probe Requests/Responses 247
Protected Management
 Frames 251
Proxy 182, 304
putty2john 147
- R**
- RADIUS 279
radius2john 147
rar2john 147
Raspberry Pi 32
Raw-MD4 145
Raw-MD5 145
Raw-MD5u 145
Raw-SHA1 145
Raw-SHA1-AxCrypt 145
Raw-SHA1-Linkedin 145
Raw-SHA224 145
Raw-SHA256 145
Raw-SHA3 145
Raw-SHA384 145
RC4 129
RDP 134, 137, 141
Redis 137
Regionseinstellung 245
Reverse Engineering 32
rexec 140
ripemd-128 145
ripemd-160 145
Rlogin 134, 140, 141
RockYou 115
Rogue Access Point 271
RSH 140
- S**
- SafeCopy (Tool) 341
Samurai Web Training Framework 393
sap2john 147
Scalpel (Tool) 338
Scan 88
 ICMP-Echo-Ping-Scan 72
 Null-Scan 88
 TCP-Ping-Scan 72
 TCP-SYN-Scan 88
 UDP-Scan 90
Schreibschutz 324
searchfy 105
Second-Level-Domain 82
- Secure Shell 137
securezip 145
SHA-256 280
SHA1 328
sha1crypt 145
SHA256 129, 328
sha256crypt 145
sha512crypt 145
Shellshock 193
Sicherungskopie 324
Siemens-S7 145
Signal 145
signal2john 147
SIP 134, 137, 145
SMB 134, 137, 141
smbnt 140
SMTP 134, 140, 141
smtp-vrfy 140
Sniffing 295
Sniffing & Spoofing 386
SNMP 134, 140, 141
Software-Write-Blocker 324
solarwinds 145
SpiderFoot (Tool) 101
SQL-Injection 211
SQLite 371
sqlmap (Tool) 214
SSH 134, 137, 140, 141, 145
SSL 200
sslsan (Tool) 204
SSLyze (Tool) 202
stat (Tool) 346
Steganografie 357
stegextract (Tool) 359
steghide (Tool) 358
Subdomain 82
Subversion 134
sudo 56
SVN 140
- T**
- Tastaturlayout 54
TCP 88
TCP-Ping-Scan 72
TCP-SYN-Scan 88
tcpdump (Tool) 295
Teamspeak (TS2) 134
Telegram 145
Telnet 134, 137, 140, 141

408 Stichwortverzeichnis

TestDisk (Tool) 342
 testssl (Tool) 200
 The Sleuth Kit (Tool) 367
 theHarvester (Tool) 99
 Tiger 145
 Time to live 76
 Timestamp 347
 TLS 200
 Top-Level-Domain 82
 Topology 74
 Traceroute 76
 TShark 300
 Tsurugi 392
 TTL 76

U

Ubuntu 392
 UDP 90
 UDP-Scan 90
 unzip 141
 Update 56
 URL 176
 urlsnarf (Tool) 307
 User Agent 169
 usufy 105

V

Virtual Machine 32
 VirtualBox 35
 Download 37
 Image 38

vmauthd 140
 VMware 35
 VMware-Auth 134
 VNC 134, 137, 141, 145
 vsFTPD 96

W

WAF 171, 207
 wafw00f (Tool) 171
 wapiti (Tool) 196
 Web Application Analysis 382
 Web Application Firewall 171, 207
 web-form 140
 Webservice 172
 Website Crawler 121
 wget 348
 whatweb (Tool) 172
 whirlpool 145
 Whois 81
 Wi-Fi 241
 wifphisher (Tool) 275
 Wireless Attacks 384
 Wireless LAN 241
 Wireshark (Tool) 264, 274, 299
 WLAN 241
 Beacon Flooding 268
 Beacons 247
 BSSID 248

Deauthentication 250
 Evil Twin 271
 Probs 247
 Rogue Access Point 271
 Sicherheit 253
 SSID 247
 WPA2 Enterprise 279

Wordlist 82, 114
 wordlists (Tool) 114
 WordPress 205
 WPA2 253
 Enterprise 279
 WPA3 251, 254
 WPScan (Tool) 205
 Write-Blocker 324
 Hardware 324
 Software 324
 Wörterbücher 114

X

Xfce 46
 XFCE4 54
 XSS 191, 212
 XSSStrike (Tool) 219

Z

Zeitstempel 347
 Zenmap (Tool) 73
 Zip 127
 zip2john 147
 Zwischenablage 53