

Stichwortverzeichnis

Symbole

3DES – *siehe* Triple-DES

A

ACID 362, 364, 495, 509-510, 514
 Archivierung 512, 538
 Grafik 542
 Korrelation 535
 Rechte 517
 Volltextsuche 541
 Address Resolution Protocol 693
siehe auch ARP
 Adleman, Leonard 783
 ADOdb 514
 Adore – *siehe* Rootkit
 Advanced Encryption Standard 782
 AES – *siehe* Advanced Encryption Standard
 Aho-Corasick 258
 AirCERT 510
 Aktualisierung der Richtlinien 166
 Alarmierung, E-Mail 117, 126, 150, 168, 231,
 376, 422, 435, 447, 492
 Analyse 89, 593, 603
siehe auch Reaktion *und* Wiederher-
 stellung des Systems
 Dokumentation 605
 flüchtige Daten 604, 607
 Arbeitsspeicher 608, 611
 Kernel 608
 Netzwerkkonfiguration 609
 offene Dateien 611
 Prozesse 609
 Rootkit 611
 Uhrzeit 608
 forensische 586, 603
 nicht flüchtige Daten 604, 616
 Datei 619
 Dateisystem 616
 Partitionsschema 617
 RPM-System 620
 Analysis Console for Intrusion Databases
 – *siehe* ACID
 Angriffe
 Firewalking 755
 Fragmentierung 237, 668
 gespoofter Portscan 763
 kodierter Angriff 238
 Mitnick-Angriff 760
 Phonebook-Angriff phf 236

Segmentierung in TCP-Paketen 238, 675
 Session Hijacking 762
 SMURF 751
 Streamreassemblierung 300
 SYN-Flood 756, 760
 SYN/FIN 236, 284, 312, 660
 Anomalie 35
 Erkennung – *siehe* Erkennung
 Anomaly – *siehe* Anomalie
 Anonymisierung 59
 arachNIDS 275
 Arbeitsspeicher – *siehe* Analyse: flüchtige Da-
 ten
 Arkin, Ofir 747
 ARP 752
 Cache 610, 752
 Reply 752
 Request 752
 Spoofing – *siehe* Spoofing
 ARPAnet 725
 arpd 693
 ARPwatch 235, 311, 376
 ASCII 303
 Assigned Number Authority 732
 asymmetrische Kryptografie
 – *siehe* Kryptografie
 Attribute 265
 Aufruf – *siehe* Alarmierung
 AusCERT 29, 86, 589
 Authentifizierung 775
 Autopsy 628, 642

B

Backofficer Friendly 684
 BackOrifice 311
 Bakos, George 685, 689
 Barnyard 338, 344, 366-367, 495, 519, 547
 Installation 501
 Konfiguration 505
 BASH History 606
 BDSG – *siehe* Gesetze
 Beihilfe zu einer Straftat 686
 Beltane 187
 Benutzerordnung 46, 578-579
 Benutzerrichtlinie – *siehe* Benutzerordnung
 Betriebsvereinbarung 579
 Biatchux 616
 Biondi, Philippe 422
 Blackhat Briefings 599

- Blowfish 782
- Body-Datei 632
- BPF-Filter 106
- Bridging 711
- Broadcast 732
- Brute-Force 774, 780, 783
- BSI-CERT – *siehe* CERT-Bund
- Bufferoverflow 37, 45, 50, 285, 324, 449
- Bugtraq 275, 288

- C**
- CA – *siehe* Zertifikatsautorität
- Caesar-Code 773
- Capabilities 427
- Carrier, Brian 628
- CAST 781
- CERT – *siehe* Computer Emergency Response Team
- CERT-Bund 78, 590
- CERT/CC 30, 78, 88, 510, 589
- Cesare, Silvio 770
- Chaos Computer Club 599
- Cheswick, Bill 681
- Chkrootkit 138, 622
- chroot 352, 562
- CIDR – *siehe* Classless Internet Domain Routing
- Ciphertext 774
- Clam Antivirus 470
- ClamAV – *siehe* Clam Antivirus
- Classless Internet Domain Routing 263
- Cohen, Fred 685
- Computer Emergency Response Team – *siehe* Notfallteam
- Computer Security Institute 86
- content 350
- Critical Path 239
- Cryptcat 617
- CSI – *siehe* Computer Security Institute
- CVE 275

- D**
- Daemen, Joan 782
- Data Encryption Standard 776, 781
- datagramm 732
- Datensysteme
 - bsdi 642
 - ext2fs 628
 - fat 642
 - fat12 642
 - fat16 642
 - fat32 642
 - freebsd 642
 - linux-ext2 642
 - linux-ext3 642
 - ntfs 642
 - openbsd 642
 - solaris 642
- Dateizugriff
 - ablehnen 434
 - anhängen 434, 441
 - nur lesen 434
 - schreiben 434
- Daten, personenbezogene 577
- Datenschutz 73, 577, 579
- Datenschutzbeauftragter 577
 - Fachkunde 578
 - Zuverlässigkeit 578
- Deception Toolkit 685
- DefCon 599, 770
- DEMARC Puresecure 510
- Denial of Service 57, 294, 749, 751, 756
 - distributed 97
 - /dev/kmem 428, 770
- DES – *siehe* Data Encryption Standard
- DFN-CERT 78, 590
- diff 99
- Differentiated Services – *siehe* ECN
- Diffie-Hellmann-Schlüsselaustausch 773, 776, 778
- Digital Millennium Copyright Act 719
- Digital Signature Algorithm 784
- Digitale Signatur – *siehe* Kryptografie
- Directory Traversal 45
- DMCA – *siehe* Digital Millennium Copyright Act
- DNS, Reverse-Lookup 590
- Doppelwort 727
- DoS – *siehe* Denial of Service
- Dreamcast-Spielekonsole 683
- DSA – *siehe* Digital Signature Algorithm
- dsniff 719
- DTK – *siehe* Deception Toolkit

- E**
- e2tools 705, 718
- ECN 738, 744
 - Congestion Experienced 745
 - Congestion Window Reduced 745
 - ECN-Echo 745
- Einbruch 87
- Einbruchserkennung – *siehe* Erkennung
- Einbruchsmeldung 586
- ElGamal 150, 784
- Erkennung 87, 683
 - Anomalie 38, 239, 320

Einbruch 38
 Missbrauch 38
 Ethernal 670, 674
 Explicit Congestion Notification – *siehe* ECN

F

falsch-negativ 49, 347
 falsch-positiv 49, 270, 291, 300, 305, 307, 311, 347, 628
 Farmer, Dan 628
 Fast Logging Project – *siehe* FLoP
 FBI – *siehe* Federal Bureau of Investigations
 Federal Bureau of Investigations 86
 fehlerhafte Anmeldung 118
 Fernmeldegeheimnis 74, 578
 Festplattencache 700
 FIA – *siehe* File Integrity Assessment
 file 655
 File Integrity Assessment – *siehe* Integritätstest
 find 99
 Fingerabdruck 235, 779
 Fingerprinting 362
 Firewalking 729
 siehe auch Angriffe
 Firewall 41, 86, 112, 594, 596, 678, 755
 Paketfilter 42, 284
 Proxy 42
 FIRST – *siehe* Forum of Incidents and
 Response Teams
 FLoP 367
 Follow-Up 91, 595
 Forensic Challenge 620, 627, 787
 Forum of Incident Response and Security
 Teams 599
 Forum of Incidents and Response Teams 590
 fpg 371
 Fragmentierung 237, 298, 727
 fragroute 678
 fragrouter 667
 Fwlogwatch 121

G

Gateway-IDS 465
 Gericht 73
 German Unix Users Group 598
 Geschichte der Intrusion Detection 33
 Gesetze 73
 Bundesdatenschutzgesetz 73, 577
 Teledienstedatenschutzgesetz
 (TDDSG) 73
 Teledienstegesetz (TDG) 73
 Telekommunikationsgesetz 74, 578

GNU GPL – *siehe* GNU GENERAL PUBLIC
 LICENSE
 GNU GENERAL PUBLIC LICENSE 795
 GnuPG 341, 607, 783
 grave-robber 629, 633
 grep 655
 Grsecurity 414
 Grub 426
 GUUG – *siehe* German Unix Users Group

H

Hash 777, 779, 784
 HAVAL 785
 Header 235
 HIDS – *siehe* Host Intrusion Detection System
 Hogwash 355
 Honeyd 414, 416, 685-686, 689, 693
 Honeynet 686
 Honeynet Project 465, 470, 472, 598, 605, 620, 681, 684, 711, 717, 729, 787
 Honeypot 29, 416, 681, 720
 Festplatten 700
 Festplattencache 700
 Firewall-Konfiguration 715
 Nachteile 682
 NAT (Network Address Translation) 713
 Routing 711
 Vorteile 682
 Host Intrusion Detection System 717
 Hotzone 685
 HTTP 281, 294, 296, 302, 671
 Proxy 305
 hunt 762

I

IANA – *siehe* Assigned Number Authority
 icat 638
 ICMP 263-264, 267, 279, 295, 540, 664, 729, 746
 Address Mask Request 751
 Code 540, 747
 Destination Unreachable 748
 Echo-Reply 664, 750
 Echo-Request 750
 Header 747
 Identifikationsnummer 540, 750
 Parameter Problem 750
 Prüfsumme 540
 Redirect 750
 Router Solicitation und Advertisement
 752
 Sequenznummer 540, 750
 Source-Quench 742, 749

- Time Exceeded 749, 755
 - Timestamp Request 751
 - Tunnel 665
 - Type 540, 747
 - icmpquery 751
 - IDEA – *siehe* International Data Encryption Algorithm
 - IDS 678
 - siehe auch* Intrusion Detection System
 - IDSG – *siehe* Intrusion Detection Sub Group
 - ils 638, 642
 - IMAP-Server 288
 - Incident 38
 - Incident Response – *siehe* Reaktion und Wiederherstellung des Systems
 - Incident Response Team – *siehe* Notfallteam
 - inetd 690
 - Integrität 775
 - Integritätstest 49, 147, 477
 - International Data Encryption Algorithm 781
 - Internet Protocol – *siehe* IP
 - Intrusion 35
 - Intrusion Detection 35
 - Intrusion Detection Sub Group 35, 38
 - Intrusion Detection System 29, 46, 86, 577, 603
 - Host Intrusion Detection System 47, 99, 111
 - Network Intrusion Detection System 50, 101
 - Intrusion Prevention System 53, 57, 465
 - Intrusion Response 59
 - IP 263, 725, 747
 - Adresse 263, 265, 540, 673, 730
 - DF-Bit 266, 298, 728, 748
 - Fragmentoffset 540, 728
 - Heade, Länge 727
 - Header 540, 726
 - Identifikationsnummer 266, 540, 662, 727
 - Länge 540
 - MF-Bit 266, 299, 728
 - Optionen 678, 730
 - Loose Source Routing 731
 - No Operation 730
 - Record Route 731
 - Router Alert 731
 - Security Options 731
 - Strict Source Routing 731
 - TimeStamp 731
 - Paketlänge 727
 - Prüfsumme 540, 729
 - reservierte Bits 266
 - Time to Live 540, 678, 729, 749, 755
 - Type of Service 540, 727
 - Version 727
 - ipchains 610
 - IPS – *siehe* Intrusion Prevention System
 - iptables 97, 610
 - itunnel 667
- J**
- JPGraph 513
- K**
- Kenntnisnahme 580
 - Kernel Intrusion System – *siehe* Rootkit
 - Kernel-Ereignis 228
 - Kernel-Module, 428, 615
 - Kim, Gene 148
 - KIS – *siehe* Rootkit
 - Kismet 374
 - Klartext 774
 - Klogd 560
 - Knark – *siehe* Rootkit
 - Kornblum, Jesse 654
 - Kossakowski, Klaus-Peter 590
 - Krauz, Pavel 763
 - Kryptoanalyse 774
 - siehe auch* Wiederherstellung des Systems
 - Kryptografie 773
 - asymmetrische 776, 783
 - digitale Signatur 777
 - öffentlicher Schlüssel 776
 - privater Schlüssel 776
 - symmetrische 776, 780
 - kstat 611
- L**
- Latenzzeit 742
 - lazarus 629, 635
 - ldd 655
 - LD_PRELOAD 413
 - Libnet 363
 - libpcap 102, 240, 246, 331, 381, 672, 674
 - Libsafe 69, 412
 - LIDS 71, 414, 421, 477
 - Aktualisierung der Regeln 442
 - Capabilities 432
 - DNS-Server 445
 - E-Mail-Alarmierung 447
 - Firewall/Snort-Sensor 446
 - Grundregeln 442
 - LIDS-Protokollierung 447
 - lids.net 435
 - lids.pw 435
 - lidsadm 430

lidsconf 431
 Proxy-Server 445
 Syntax 438
 Webserver 444
 Lilo 425
 Linux Rootkit Fünf – *siehe* Rootkit
 Linux-Intrusion-Detection-System – *siehe* LIDS
 LKM – *siehe* Kernel-Module
 Local-Key 171
 Logcheck 134
 LogSentry – *siehe* Logcheck
 LogSnorter 535
 Logsurfer 112
 Logwatch 130

M

MAC-Adresse 758
 MAC-Zeitstempel 633
 mactime. 629
 Mailingliste 592-593, 598
 Man-in-the-Middle 719
 ManTrap 685
 Maximum Segment Size 362
 siehe auch MSS
 Maximum Transmission Unit 298, 362
 siehe auch MTU
 McAfee 275
 MD5 341, 571, 607, 620, 766, 784
 md5deep 654
 md5sum 101, 607, 621
 Message Authentication Code – *siehe* Hash
 Missbrauch 35
 Missbrauchserkennung – *siehe* Erkennung
 Misuse – *siehe* Missbrauch
 Mitnick, Kevin 30, 738, 760
 mmap-libpcap 246, 343
 Morris-Wurm 449
 Mount-Optionen, noexec,ro 622
 MS SQL- 335
 MSS 732
 Msyslogd – *siehe* Syslogd
 MTU 733, 741, 748
 siehe auch Maximum Transmission Unit
 Mu-Wanber 258
 Mudpit 338, 364, 367, 501
 Multicast 732
 MySQL 335, 495, 501, 511, 563, 569
 Erzeugung der Datenbank 336, 512, 570
 Schema 512

N

NAT – *siehe* Network Address Translation
 National Institute of Standards and
 Technology 784
 nc – *siehe* Netcat
 Nessus 341
 Netcat 324, 605, 617-618, 675
 Netfilter 121, 689, 716
 siehe auch iptables
 Netstumbler 374
 Network Address Translation 730, 749
 Network Intrusion Detection System 235,
 495, 659, 675, 717
 siehe auch Intrusion-Detection-System
 Network Time Protocol 560, 572
 Neuinstallation 593
 ngrep 108
 Nichtabstreitbarkeit 775
 NIDS – *siehe* Network Intrusion Detection
 System
 NIST – *siehe* National Institute of Standards
 and Technology
 Nmap 268, 285, 313, 685, 693, 763
 NOP Sled 50, 288, 326
 Notfallplan 79, 585
 Notfallteam 77, 585, 597
 NTP 575
 siehe auch Network Time Protocol
 ntpd 573
 ntpdate 573
 NVP 729

O

objdump 655
 Oinkmaster 357, 470
 OpenSSL 520
 Optyx 770
 Oracle 335
 OSI-Modell 725
 Oudot, Laurent 415
 Out-Sourcing 597

P

p0f 362
 Packetstorm 289
 Paketfilter – *siehe* Firewall
 Path MTU Discovery 299, 748
 Perl Compatible Regular Expression 417
 PHP 511
 PHPLOT 513
 Ping 279
 of Death 728

- Plac 616
 Port 668, 673
 offen 663
 Portmapper – *siehe* RPC Portmapper
 Portscan 37, 51
 gespooft 763
 PortSentry 134
 POSIX-Capabilities – *siehe* Capabilities
 PostgreSQL 335, 563
 Prävention 85
 Prelude 111, 201, 204
 Snort 408
 Protokolle
 Analyse 48, 111, 121, 130, 559, 572
 Dekodierung 52, 238
 Kontext 115
 Rotation 120, 233, 328, 429, 441
 Verkettung 341, 571
 Protokollierung 578
 Provos, Niels 414, 685, 693
 Proxy – *siehe* Firewall
 ProxyARP 711
 Prozesse – *siehe* Analyse: flüchtige Daten
 Prüfsumme 777, 779
- Q**
- Quality of Service 727
- R**
- Random Early Detection 745
 Ranum, Marcus 68, 684
 RC5 781
 Reaktion 88, 276, 583, 683
 Reassemblierung 670
 Record Route 266
 Recovery – *siehe* Wiederherstellung
 des Systems
 RED – *siehe* Random Early Detection
 Red Hat 122, 150, 252, 511, 563, 699
 Red Hat 513-514
 regulärer Ausdruck 116, 569
 Return On Investment 60
 Return on Security Investment 60
 Rijmen, Vincent 782
 Rijndael 782
 RipeMD-160 435, 571, 785
 Rivest, Ron 781, 783
 Roesch, Marty 239, 681
 ROI – *siehe* Return On Investment
 Rootkit 48, 57, 207, 421, 611, 614, 623, 765
 Adore 211, 614, 768
 Erkennung 207
 Kernel Intrusion Rootkit 428
 Kernel Intrusion System 765, 770
 Kernel Intrusion-System 615
 Knark 767
 Linux Rootkit Fünf 765
 T0rnkit 765
 ROSI – *siehe* Return On Security Investment
 Routing Information Protocol 750
 RPC Portmapper 692
 RSA 783
 rsync 486, 495
- S**
- Samhain 69, 111, 148, 187, 412
 Chroot 217
 Stealth-Modus 189
 SANCP 547
 SANS Institute 599
 Sasser 449
 Satori 765
 Scan
 ACK 662
 FIN 663
 SYN/FIN 660
 Schlüssel 775
 Schlüssellänge 780, 783, 786
 Schneier, Bruce 782
 script 606
 Sebek 717
 Secure Shell 486
 Sensor
 Barnyard-Installation 501
 Barnyard-Konfiguration 505
 Hardware 496
 Netzwerkkonfiguration 500
 Partitionierung 500
 Snort-Installation 500
 Snort-Konfiguration 501
 Software 499
 Standort 495
 Sequenznummer 756
 servsock 370
 Sguil 364, 511
 SHA 785
 SHA-1 571
 Shamir, Adi 783
 Sheffield, Keith 718
 Sicherheits-Audit 594
 Sicherheitslücke 593
 Sicherheitsrichtlinie 80, 595-596
 sid-msg.map 275
 Signatur-Erkennung 51
 Silent Host 764
 Site-Key 171

- SIV – *siehe* System Integrity Verifier
- Skript-Kiddie 37
- Skytale von Sparta 773
- Sleuthkit 642
 - siehe auch* The @stake Sleuth Kit
- SMURF – *siehe* Angriffe
- SNARE 111, 226
- Sneeze 363
- Sniffer 587, 719
- SNMP 338
- Snort 67, 69, 235, 239, 408, 495, 674
 - Aktion 262, 359
 - Activate 262, 292-293
 - Alert 262, 292
 - Dynamic 262, 292-293
 - Eigene Definition 262
 - Log 262, 292
 - Pass 262, 292, 341
 - Anwendung
 - NIDS 250
 - Paketlogger 249
 - Paketsniffer 248
 - Anwendung bei einem Switch 356, 495
 - Attribute
 - ack 268, 347
 - activated_by 293
 - activates 293
 - asn1 270
 - byte_jump 271, 275
 - byte_test 272
 - classtype 276
 - content 272-275, 283, 308, 327, 346, 469
 - content-list 273, 296
 - count 293
 - depth 273-274, 347
 - distance 273, 275
 - dsize 267-268, 347
 - flags 267, 283, 347
 - flow 268, 283, 347
 - flowbits 269, 277, 294
 - fragbits 266, 347
 - fragoffset 267
 - icmp_id 267, 347
 - icmp_seq 267, 347
 - icode 267, 347
 - id 266, 347
 - ipopts 266, 347
 - ip_proto 266, 347
 - isdataat 273, 291, 348
 - itype 267, 281, 347
 - length 362
 - logto 275
 - msg 275, 280
 - nocase 274, 284
 - offset 274, 347
 - pcr 274, 292, 348
 - priority 276
 - quirks 362
 - rawbytes 274, 309
 - react 273, 278
 - reference 275
 - replace 469
 - resp 277, 295, 347
 - rev 276
 - rpc 274, 309
 - sameip 266, 347
 - seq 268, 347
 - session 276, 347
 - sid 275
 - stateless. 278
 - tag 270, 276, 294
 - tcpopts 362
 - tos 266, 347
 - ttl 266, 347, 362
 - uricontent 283, 308
 - window 268, 347, 362
 - within 275
- Ausgabeformat 243, 250
- automatischer Start 251
- Bleeding-Snort 361
- Chrooting Snort 351
- config 257
 - alertfile 257
 - alert_with_interface_name 257
 - bpf_file 257
 - checksum_mode 258, 302
 - chroot 257
 - classification 258, 276
 - daemon 258
 - decode_arp 258
 - decode_data_link 258
 - detection 258
 - disable_decode_alerts 259
 - disable_ipopt_alerts 259
 - disable_tcpopt_alerts 259
 - disable_tcpopt_experimental_alerts 259
 - disable_tcpopt_obsolete_alerts 259
 - disable_tcpopt_tcp_alerts 259
 - dump_chars_only 259
 - dump_payload 259
 - dump_payload_verbose 259
 - event_queue 258-259, 327, 349
 - interface 259
 - logdir 259

- min_ttl 259
- nolog 259
- no_promisc 259
- obfuscate 259
- order 260, 282
- pkt_count 260
- quiet 260
- reference 260
- reference_net 260
- set_gid 260
- set_uid 260
- show_year 260
- stateful 260, 300, 302
- umask 260
- utc 260
- verbose 261
- Content-Regel 283
- Detektionsmaschine 348
- diskrete Attribute 265, 346
- dynamische Regeln 293
- Event-Queue 327
- Event-Suppression 339
- flexible Antwort 294
- Konfigurationswerkzeuge 375
 - Win32 IDS Policy Manager 375
- Multi-Rule-Inspection-Engine 265, 346
- Output-Plug-In
 - alert_fast 327, 345
 - alert_full 328
 - alert_smb 330
 - alert_syslog 330
 - alert_unixsock 331
 - alert_unixsock_db 368
 - CSV 337
 - database 277, 335
 - IDMEF 333
 - log_null 339
 - log_tcpdump 331
 - mysql 362
 - Snort 368
 - trap_snmp 338
 - unified 338, 364, 505
 - xml 331
- Passregel 282
- Plug-In 241, 256
- Präprozessor 242, 256, 298
 - arpspoof 311
 - bo 311
 - conversation 312-313, 315
 - defrag 298-299
 - flow 313-315
 - flow-portscan 314-316, 320
 - frag2 240, 298, 345
 - httpflow 314
 - http_decode 302, 304
 - http_inspect 302, 304, 314
 - portscan 312, 546
 - portscan2 313, 316
 - rpc_decode 309
 - spade 320
 - stream4 240, 283, 300, 313, 345, 363, 469, 546, 678
 - stream4_reassemble 300
 - telnet_decode 300, 309
 - unidecode 302
 - uni_decode 304
- Präprozessoren
 - flow 277
 - http_decode 273
 - http_inspect 273
- Realtime Network Awareness 362
- Regel-Management 357
- Regelrumpf 261
- ruletype 293
 - siehe auch* Snort Aktion
- Stealth-Modus 354
- Testwerkzeuge 363
- Thresholding 339
- Variable 255
- Snort!(FP) 362
- snort-center 495, 526
 - ACID-Plug-In 533
- Snort-Inline 465, 716
 - Attribute, replace 469
- Snort-Wireless 371
 - Attribute
 - addr4 373
 - ssid 373
 - duration_id 373
 - fragnum 373
 - frame_control 372
 - from_ds 372
 - more_data 373
 - more_frags 373
 - order 373
 - pwr_mgmt 373
 - retry 373
 - seqnum 373
 - ssid 373
 - stype 372
 - to_ds 373
 - type 372
 - wep 373
- Präprozessor
 - Antistumbler 374
 - Authflood 374

- Deauthflood 374
 - Macspoof 374
 - RogueAP 373
 - SnortConfig 470
 - Snot 363, 371, 396
 - Social Engineering 30, 88
 - sockserv 369
 - Song, Dug 667, 678, 719
 - Source Routing
 - Loose 731
 - siehe auch* IP-Optionen
 - Strict 731
 - Strict[/i] – *siehe* IP-Optionen
 - Sourcefire 362
 - Spafford, Eugene H. 148
 - Spitzner, Lance 416, 681
 - Spoofing 51, 665, 716, 757
 - ARP 310, 753, 757, 762
 - ARP-Spoofing 376
 - DNS 757
 - IP 757
 - ssh – *siehe* Secure Shell
 - sshmitm 719
 - SSL 519, 526, 530, 719, 759
 - StGB – *siehe* Strafgesetzbuch
 - Stick 363, 396
 - Stoll, Clifford 681
 - Stoppint – *siehe* Tripwire, Ausnahme
 - strace 655
 - Strafgesetzbuch 686
 - strings 655
 - stunnel 495, 519, 568
 - Suchmuster 116
 - sudo 491
 - SUSE 122, 150, 253, 511, 513-514, 563, 699
 - symmetrische Kryptografie
 - *siehe* Kryptografie
 - SYN-Cookies 756
 - SYN-Flood 95
 - siehe auch* Angriffe
 - SYN-Paket 236, 282
 - SYN/FIN-Paket 236
 - Syslogd 560, 757
 - BSD 563, 565
 - Modular 563
 - Msyslogd, PEO 571
 - System Integrity Verifier 187
 - siehe auch* Integritätstest
 - Systrace 414, 455, 658
- T**
- T0rnkit – *siehe* Rootkit
 - Tastaturlogging 717
 - TCO – *siehe* Total Cost of Ownership
 - TCP 236, 263, 267, 540, 568, 618, 729, 732, 734
 - Acknowledgement Timer 743
 - Acknowledgementnummer 268, 540, 738
 - Congestion Avoidance 742-743
 - Congestion Window 742-743, 745
 - Congestion Window Reduced 745
 - ECN-Echo 745
 - FIN 676
 - Flag 267, 540, 678, 739
 - ACK 284, 739, 746
 - FIN 739
 - PSH 739
 - RST 284, 739
 - SYN 284, 739, 746, 761, 763
 - URG 739-740
 - Flags, SYN 301
 - Flusskontrolle 742
 - Handshake 735, 761
 - Header 736
 - Länge 738
 - MRU 741
 - Optionen 741
 - End of Option List 741
 - MSS 741
 - No Operation 741
 - Selective Acknowledgment Data 741
 - Selective Acknowledgment
 - Permitted 741
 - Timestamp 742
 - Window Scale 740-741
 - Port 540, 737
 - Prüfsumme 540, 677, 740, 743
 - Receive Window 540, 740, 743
 - reservierte Bits 738
 - Reset 278, 295, 301, 673, 748
 - RST 676
 - Selective Acknowledgment 744
 - Sequenznummer 268, 540, 676, 678, 734-735, 737, 743, 760, 762
 - Slow Start 743
 - Streamassemblierung 300
 - Streamreassemblierung 238, 283
 - Streamreassemblierungs-Angriff 675
 - Urgent-Zeiger 540, 740
 - Vollduplex 736
 - tcpdump 102, 666, 674
 - snaplen 665
 - TCPflow 672
 - TCPshow 671
 - TCPtrace 673
 - TCT – *siehe* The Coroner's Toolkit
 - TDDSG – *siehe* Gesetze

- TDG – *siehe* Gesetze
 Team Teso 667, 768
 The @stake Sleuth Kit 628
 The Coroner's Toolkit 585, 623
 THP – *siehe* Tiny Honeypot
 Tiger 111, 135, 190, 785
 Time Stamp 266
 Time to Live 266, 300
 Tiny Honeypot 685-686, 689
 TKG – *siehe* Gesetze
 Total Cost of Ownership 60
 traceroute 729, 749
 Traffic-Vis 674
 Transmission Control Protocol – *siehe* TCP
 Trinux 616
 Triple DES 781
 Tripwire 72, 111, 147, 187, 477, 623
 Aktualisierung der Datenbank 165, 493
 Attribut 178
 Ausdruck der Berichte 169
 Ausnahme 178
 CRC-32 172, 176, 186
 Direktive 181
 E-Mail 492
 Alarmierung 168
 Erzeugung der Datenbank 157, 490
 HAVAL 172, 177, 186
 Installation 150
 Klartextanzeige der Datenbank 159
 Kommentar 175
 Local-Key 153, 155, 486
 MD5 172, 176, 186
 Optimierung 173
 Regeln
 allgemein 479
 DNS-Server 483
 E-Mail-Server 480
 OpenLDAP-Server 484
 Proxy 479
 Samba-Server 483
 Syntax 175
 Webserver 482
 SHA 172, 177, 186
 Site-Key 153, 155, 485
 twadmin 155
 twcfg.txt 152, 478
 twpol.txt 152, 478
 Überprüfung der Datenbank 159, 490
 Variable 177
 Verschlüsselung der
 Konfigurationsdateien 150, 153, 156
 zentrale Auswertung 492

 Trojanisches Pferd 48
 TTL – *siehe* Time to Live
 twcfg.txt 170
 Twofish 782
 twpol.txt 170
 Type of Service 266

U
 UDP 236, 263, 540, 562, 568, 618, 729, 732, 757
 Destination Port 733
 Header 733
 Länge 540, 733
 Port 540
 Prüfsumme 540, 733
 Source Port 733
 UML – *siehe* UserModeLinux
 Unicode 303-304, 308
 UNIX epoch 505
 UNIX-Socket 562
 unixODBC- 335
 unrm 635
 unrm. 629
 uricontent 346, 350
 USENIX 599
 User Datagram Protocol – *siehe* UDP
 UserModeLinux 686, 699, 701, 706
 Erzeugung der Dateisysteme 707

V
 Venema, Wietse 608, 628
 Verbindungsdaten 74-75, 578
 Verschlüsselung 775
 siehe auch Kryptografie
 Konfigurationsdateien 170
 Virtuelles Privates Netzwerk 46
 VMware 686, 699, 701
 Festplattenpartitionen 704
 Netzwerk 701
 Suspend 705
 VPN – *siehe* Virtuelles Privates Netzwerk

W
 webmitm 719
 Weiterbildung 597
 Konferenzen 598
 Kurse 598
 Selbststudium 597
 Wesslowski, Boris 121
 Whois 591
 Wiederherstellung des Systems 90, 583
 Wurm 449

X

Xie, Huagang 422

xinetd 690

XMAS 312

xwd 607

Y

Yarochkin, Fyodor 747

Yule 187

Z

Zeitserver 560, 573

Sicherheit 574

Zertifikatsautorität 520

Ziegler, Robert L. 690

Zugriffsanalyse 49

