

STICHWORTVERZEICHNIS

O

0-days	696
2-Factor-Authentication.....	863

A

Absender über Verbindungsverbot inf.....	158
Absenderadresse fälschen	237
Absenderadresse festlegen	238
access	860
ACK	597
ACK-Mapping	292
ACK-Mapping, Firewalls umgehen	292
Acknowledge	277
ACK-Segmente	170, 277, 341
ACK-Segmente, Filterung.....	294
ACK-Segmente, willkürliche	597
Active Server Pages	449
Address mask request-Fragmentierung	465
Address Resolution Module.....	255
Admin, Paßwort	877
Adreßauflösungen in lok. Cache vermerken	257
Adressen, relative in absolute umwandeln	855
Adreßklassen	138
Adreßlänge von verschied. Medien.....	254
Adreßumwandlung, dynamische.....	254
AJAX	804
Aktive Systeme erkennen	201
Alternative Portnummern	595
alternative Portzugriffe, Webbrowser	612
amap	413
amap, Funktionsweise	413
amap, Response-Datei.....	415
amap, Suchmuster.....	416, 417
amap, Trigger	413f, 415
Amplifizierung durch Broadcasting	564
Analyse d. Arbeitsplatzrechner.....	51
Analyse d. Perimeter-Systeme	50
Analyse d. Server-Systeme.....	50
Analyse d. Sicherheitssysteme	50
Analyse gefilterter Ports und Verbindungen.....	594
Analyse wichtiger Systeme	49
Analytisches Sniffing	127
Anfragen, überfluten mit	560
Angreiferquelle verschleiern	237
Angreifertypen	30
Angriff, realistische Voraussetzungen für.....	55
Angriffstools, Namen	680
Angriffsvektoren ermitteln.....	718
Anwenderfehler	671
Anwendungen ermitteln	491
Anwendungsprotokoll am Banner erkennen	422
Anwendungsschicht.....	605
Anwendungstechnologien erkennen.....	449
ANY-Regel.....	621
Anzahl d. zu puff. Byte f. Übertragung	353
Apache, Port	120
Apache, Statusmeldungen-Datei.....	537
Apache, überlange URLs	533

appdefs.resp	415
appdefs.trig	413
Application Fingerprinting	491, 678
Application Gateway.....	603
Application Gateways umgehen	609
Application Inspection untergraben	612
Application Level Proxies.....	601
Application Mapping	395, 413, 492, 678
Application Mapping mit amap.....	691
Application-Gateways, Schicht	605
Applikationsbanner.....	494
Applikationsserver.....	46
arp who-has.....	130, 231
ARP	137, 211, 254, 579
ARP-Anfragen	579
ARP-Auflösung für Gateway	211
ARP-Auflösung untersuchen.....	220
ARP-Auflösung, erfolgreiche anzeigen	231
ARP-Auflösung, Internet	211
ARP-Auflösung, LAN	211
ARP-Broadcast	211
ARP-Cache anzeigen.....	257
ARP-Cache, Lebensdauer.....	257
ARP-Einträge manipulieren	269
ARP-Einträge überschreiben	270
ARP-Flooding	272
arping	257, 579
arping, Parameter	264
arping, Quelladressen fälschen.....	264
arping-Zugriffe, Wartezeit dazwischen.....	261
ARP-Kill	269
ARP-Mapping	253
ARP-Mapping, lokales Netz	272
ARP-Mapping, passives	270
ARP-Paket in Ethernet, Aufbau.....	254
ARP-Ping	258
ARP-Ping m. gefälschter Abs-Ethernetadr.....	267
ARP-Ping m. gefälschter Absender-IP-Adr.....	264
ARP-Spoofing	548
ARP-Sturm	232
ARP-Tabelle, lokale überwachen.....	266
ARP-Verbindungen m. fehlerh. Inform.	579
ARP-Verkehr prüfen	266
arpwatch	266
arp-who-has-Anfragen, Abstand zwischen.....	261
Array	835
ASL-Patterns für Webapplikationen	690
ASP, Session-Cookie	449
ASP, Status-Management	449
Asset-Definition	41
Asset-Berechnung.....	42
Assets erster Priorität	44
Assets zweiter Priorität	44
ATK (Attack Tool Kit).....	687f.
attrib.exe	731
Audit, konzeptioneller	57
Audit, organisatorischer	56
Audit, technischer	57
Auditoren-Team.....	67
Audits auf konzept. u. organisat. Ebene	55
Audits, zyklische	55

Audit-Verzeichnis70
 Ausführrechte, erweiterte wg. Direktzugriff..... 768
 Ausgabeumleitung74
 Authentifizierung 863
 Authentifizierung, Benutzergruppe.....866
 Authentisierung mitlesen..... 878
 Authentisierung, biometrische..... 884
 Authentisierung, schwache.....862
 Authentisierung, Single Sign-on 863
 Authentisierungen, zentraler Punkt 862
 Authentisierungsmechanismen umgehen..... 887
 Authentisierungs-Mechanismen, Angriff auf..... 863
 Authentisierungsmechanismus, PHP 799
 Automatische Begrüßung419
 Automatisches Schließen der Sitzung 410
 Automatisierter Vulnerability Scan..... 683
 Automatisiertes Mapping 309

B

Backdoor 557, 597
 Backlog-Queue aufbrauchen 573
 Bandbreite 194f.
 Banner abgreifen 685
 Bannerausgabe, gefälschte..... 686
 Bannerausgabe, lückenhafte..... 686
 Bannerausgabe, unterdrückte..... 685
 Bannerauswertung 448
 Banner-Grabbing nicht möglich.....411
 Banner-Grabbing.....404, 493, 684
 Banner-Grabbing, Informationen 404
 base64_decode 795
 BBcode..... 796
 Bedrohung herausfinden29
 Bedrohungsfluß 634
 Befehle von Server nicht verarbeiten lassen..... 277
 Befehle, kritische 711
 Beglaubigte TCP-Sitzg. d. Flags vortäusch. 597
 Begrenzte TCP Backlog Queue..... 676
 Begrüßung durch Banner 404
 Begrüßung 579
 Benutzerauthentisierung in PHP..... 889
 Benutzereingabe, Argumente als Char..... 699
 Benutzereingabe, Argum. als Fließkommaz..... 699
 Benutzereingabe, negative Werte..... 700
 Benutzereingabe, reservierte Sonderzeichen 700
 Benutzereingabe, zu hohe Zahlenwerte..... 700
 Benutzereingaben, PHP..... 712
 Benutzernamen..... 866
 Benutzername/Paßwort-Kombinationen 876
 Benutzername, Footprinting 867
 Bereichsüberschreitung 838
 Bestehende Verbindung betrachten 118
 Betriebssystem anpingen nicht möglich 454
 Betriebssystem des Zielsystems ermitteln..... 448
 Betriebssystem vortäuschen 212
 Bibliotheken manipulieren 698
 Binäre Dienste..... 406, 410
 Birthday-Attacken.....33
 Black Hat Hacker.....54
 Blackbox-Verfahren58
 Blacklist 748
 Blacklist-Filter..... 751
 Blacklist für Eingaben 791
 Blacklist umgehen 609
 Blacklist-Überprüfung des Webbrowsers..... 803
 Blind SQL Injection 819
 Botnet 557
 Brandschutzmauer 585
 Breakpoints..... 715
 Bridge..... 190
 British Standards Institute37

Broadcast-Adresse 136, 140
 Broadcast-Adressen als Amplifier 566
 Broadcast-Adressen ermitteln 138
 Broadcast-Adressen privater IP-Bereiche 142
 Broadcast-Anfrage 129
 Broadcast-Anfragen, Reaktion 455
 Broadcasting..... 136
 Broadcast-Ping.....140, 233, 455
 Broadcast-Zugriff 140
 Broken by design..... 668
 Browser, Inhalte der gleichen Domain
 nachladen 803
 Browser-Schwachstellen ausnutzen 807
 Browsing-Frontend.....49
 Bruteforce-Attacken..... 385
 BSS-Overflow 836
 Bundesamt für Sicherheit in der Informatik.....37
 Byte-Ordering 833

C

Caches, lokale..... 376
 Carriage Return 543
 cat.....74
 CGI-Scan 739
 CGI-Scanner..... 691
 CGI-Scanning mit Nikto 691
 Challenge-Response-Protokoll 863
 chargen 369
 chargen, Überflutung mit 566
 Char-Input-Verarbeitung 427
 chmod 729, 860
 chown 860
 CIA-Dreieck 42
 Clark-Wilson-Modell 42
 Clientseitige HTTP-Abfragen..... 804
 Clogging..... 560
 Close-Verhalten..... 427
 Code Injection..... 759
 Codierung..... 611, 752
 Command Injection..... 759
 Common Point of Trust.....391, 640, 862
 Common Point of Trust, fehlender 642
 Computercluster..... 645
 Computersystem zum Absturz bringen.....32
 Concurrent Nutzung e. Kontos..... 883
 Content-Management-System 744
 Controlling82
 Cookie anzeigen 784
 Cookie auslesen 780
 Cookies definieren 784
 Cracker54
 Critical Infrastructure.....44
 Cross Site Request Forgery 800
 Cross Site Scripting..... 773
 CSRF-Attacke 801
 C-Strings 711
 CVE..... 680
 CVE-Kompatibilität..... 681

D

Data Tracing..... 714
 Datei herunterladen 424
 Datei sperren 860
 Datei vorhanden, Prüfung auf..... 860
 Datei-/Verzeichnisrechte 727
 Dateiattribut 730
 Dateihandle 860
 Dateisystem, navigieren im..... 742
 Dateiumleitung74
 Dateizugriffe..... 713

Daten absichtlich fragmentieren	573
Daten puffern.....	483
Datenaufkommen der Schnittstelle analys.	556
Datenaufkommen im Netzwerk verstärken.....	564
Datenbank, flache	811
Datenbank, Kommandozeilenbefehle	828
Datenbank, Paßwort-Authentisierung.....	822
Datenbanken, Datentypen.....	823
Datenbanken, erweiterte Zugriffsrechte	820
Datenbanken, Fehlerausgaben unterdrücken.....	819
Datenbanken, Ressourcen aufbrauchen	829
Datenbankzugriffe.....	713
Datenfluß drosseln.....	391
Datenpakete einlesen	128
Datensätze aus Datenbank exportieren	826
Datenströme mitlesen	144
Datenteil einer Anfrage analysieren	459
Datentypen einer Datenbank ermitteln.....	824
Datenübertragungsanalyse	193
Datenverkehr mitlesen	270
daytime	369, 429
dclient	553
DDNS	553
DDoS.....	557
Debugging	665, 666, 714f.
Decoy-Funktion	392
Defacements.....	32
Default Gateway	134
default.asp.....	449
Default-Gateway sperren lassen.....	661
Delta-Technik.....	177
Denial of Service.....	32, 144, 547
Denial of Service-Attacken auf Datenbanken.....	829
Denial-of-Service-Attacke, versehentliche.....	269
deny	157
Deny-Regeln.....	591
Design Errors.....	669
Desktop-Firewalls.....	214
Destruktive Attacke.....	547
Developer-Mailingliste.....	678
DF-Bit.....	173, 485
DHCP discover-Nachricht.....	129
DHCP-Einstellungen auswerten.....	141
DHCP-Informationen auswerten.....	129
Dial-up-Verbindungen	643
Dictionary Attacks	870
Dienst, Funktionsweise erkennen	413
Dienst, Schließverhalten.....	428
Dienste auswerten	440
Dienste ermitteln.....	315, 395
Dienste über NetBIOS	442
Dienste, fehlerhafte Eingaben verwerfen	423
Dienste, laute und aktive.....	390
dig	109
Directed Broadcast	138, 140
Directory-Traversal-Attacken, typische Zeichen.....	694
Directory-Traversal-Schwachstelle	675, 720, 741
Directory-Traversal-Schwachstelle ausnutzen mit POST-Anfrage	720
Directory-Traversal-Schwachstelle ausnutzen	688
Direct-Parameter-Access-Technik.....	852
Direktverbindungen provozieren.....	118
Disassembler	666
Discard-Dienst	276
Distanz von einem Host zu anderen	146
Distributed Denial of Service.....	557
Division durch Null	700
DMZ durch zwei Firewall-Systeme	649
DNS Zonentransfer ohne zusätzliche Scanning-Tools.....	108
DNS Zonentransfers	108

DNS.....	46, 105, 188, 442, 588
DNS, Port.....	105
DNS-Server.....	105
Domänen-Abfrage	97
Don't Fragment-Flag.....	22, 485, 571
Don't Fragment	173
Don't-Fragment-Bit.....	190
DoS	547
DoS, Dienst deaktivieren	550
DoS, Fehlerhafte Verarbeitung ausnutzen.....	550
DoS, Ressourcen verbrauchen	549
Download automatisieren	555
Downstream.....	551
Downstream, Auslastungsangriff.....	556
Drei-Wege-Handschlag/Handshake	275, 277, 340
Drei-Wege-Handschlag zurücksetzen	286
Drei-Wege-Handschlag, Umkehr.....	341
drop	157
Drop-Regeln.....	591
Dual-Homed Host.....	152, 531
Durchsatz, maximaler	195
Dynamische Adreßumwandlung.....	254
Dynamische DNS-Systeme.....	553
Dynamische Routen erkennen	177
Dynamische Zugriffe	261
Dynamischer DNS-Dienst	553

E

echo, Überflutung mit	566
Echo-request-Datenteil.....	456
Eigene Ports	401
Eingabe ignorieren	410
Eingabe provoziert unvorherseh. Zustände	699
Eingabe, falsche.....	423
Eingabe, statisch	746
Eingabefilter umgehen m. altern. Schreibw.	791
Eingabefilter, statische umgehen	751
Eingabekonstellationen erzwingen	769
Eingabemaske	828
Eingaben manipulieren	697
Eingaben, GUI-Anwendungen.....	705
Eingabeüberprüfung	759
Eingabeüberprüfung, clientseitig	766
Eingabeüberprüfung, serverseitig.....	769
Eingabeungültigkeit	817
Eingabevorgaben umgehen.....	766
Eingeh. ICMP echo request-Anfr. ignorieren	215
Eingehenden Verkehr verwerfen	157
Eingelesene Pakete anzeigen	309
Eingetragene Nameserver abfragen	97
Einsatzzweck e. Systems ableiten	441
Einzelzeichen-Eingabe.....	426
Elektronischer Pförtner	585
E-Mail, Absender und Empfänger.....	508
Endanwender, Schutz vor	31
End-to-End-VPN	655
Erfolgreiche Authentisierung mitlesen	878
Erfolgskontrolle	84
Erkennungsmuster verändern	793
err.....	852
Erreichbarkeit eines Hosts prüfen.....	274
Erreichbarkeit eines Systems prüfen.....	73
Erstes Fragment e. Anfrage	174
/etc/hosts.....	226
/etc/passwd, Leserechte.....	748
eth0	23
EtherApe	129
Ethernetadresse des Zielsystems ermitteln.....	211
Ethernetadresse ermitteln	270
Ethernetadrezuweisung überwachen.....	266
Ethernet-Broadcasts.....	272

Ethernet-Schnittstelle23
 Ethernet-Versionen..... 172
 Ethertype.....172
 Eventbasiertes Fuzzing 705
 Event-Handler 796
 Event-Handler umgehen..... 795
 Exploit667, 717, 725
 Exploit, Ziele 719
 Exploiting..... 59, 683
 Exploit-Zustand herstellen 693
 XPN..... 514
 Exponierteste Komponenten45
 Externe Sicherheitsmechanismen83
 Externes Bild in E-Mail..... 124

F

Failover-Lösung65
 False Negatives 685
 Faultinjection..... 696
 Fehlende Ausgabe falsch entdeckter Dienste 594
 Fehler, Definition 667
 Fehlerbehaftete Funktionen 711
 Fehlerhafte Eingaben, Reaktion auf 427
 Fehlerhafte Verarbeitg. v. TCP-Verbindg..... 563
 Fehlerklassen..... 675
 Fehlermeldungen..... 203, 493
 Fehlermeldung zurückschicken 410
 Fehlermeldungen provozieren 495
 Fehlerquellen..... 667
 Fehlersuche..... 665
 Fernsteuerungs-Utility 402
 Filter erkennen..... 607
 Filter mit Codierung umgehen..... 752, 794
 Filter umgehen 748
 FIN 276, 597
 FIN, Rückantwort..... 592
 find..... 400
 Fingerabdruck fälschen 885
 Fingerprint-Datenbank 447
 Fingerprinting 439, 682
 FIN-Flag..... 345
 FIN-Mapping..... 295
 FIN-Mapping, untypische Ports 298
 FIN-Scan..... 340, 341
 FIN-Scan auf geschlossenen Port..... 342
 FIN-Scan auf offenen Port 342
 Firewall Ruleset..... 615
 Firewall umgehen 587
 Firewall verstecken 633
 Firewall, 150 Regelsätze 636
 Firewall, Antwort verweigern 591
 Firewall, automatischer Gegenangriff 661
 Firewall, automatisches Lockout 660
 Firewall, bekannte Dienste 593
 Firewall, beliebte Angriffsziele..... 594
 Firewall, fragmentierten Anfragen erkennen 599
 Firewall, gesprächige Dienste..... 593
 Firewall, Hostnamen 588
 Firewall, IP-Fragmentierung 598
 Firewall, Kommunikationsbez. visualisieren 633
 Firewall, korruptes Vorgehen erkennen..... 660
 Firewall, Logging..... 658
 Firewall, Portbereiche 630
 Firewall, Redundanz 644
 Firewall, Regelwerkgröße..... 636
 Firewall, Sperrliste 660
 Firewall, statuslos 294
 Firewall, Strike-Back-Mechanismen 660
 Firewall, verbindungsabbau sofort d. Server 594
 Firewall, virtuelle Gruppenbildung 636
 Firewall, VPN-Endpunkte..... 655

Firewall, Zonen..... 639
 Firewall-Administration..... 67, 657
 Firewall-Element als Gateway 642
 Firewall-Elemente erkennen..... 155
 Firewalling 152
 Firewall-Regel, optimale..... 620
 Firewall-Regelwerk analysieren 614
 Firewall-Regelwerk normalisieren 618
 Firewall-Regelwerk, Aufbau..... 619
 Firewalls umgehen 292
 Firewalls, Namenskonventionen..... 588
 Firewall-Systeme b. traceroute-Zugr. umgeh 166
 Firewall-Systeme..... 585
 Firewall-Systeme, ICMP-Typ-3-Fehlerrm 593
 Firewall-Systeme, mehrstufige 646
 Firewall-Systeme, Namenskonventionen 107
 First Line of Defense 864
 Flags einer erlaubten Verbindung..... 597
 Flags, manipulative 597
 Flawfinder 712
 Flooding..... 560
 Fokussierter Portscan..... 318
 Footprinting..... 87
 fopen..... 860
 Format-String 848
 Format-String, Funktionen 852
 Format-String-Schwachstellen..... 712
 Formatumwandlungen, PHP 795
 Formularauswahl 766
 Forward Acknowledgement..... 480
 fraggle.c 566
 Fraggle-Angriffe..... 566
 Fragment eines Fragmentierungszugs..... 173
 Fragment, Total Length..... 173
 Fragment, welches Teil des Originalpakets 575
 Fragmente ablegen 571
 Fragmente logisch überlappen lassen..... 576
 Fragmentierter Datenverkehr..... 485
 Fragmentierung ausgehender Pakete best..... 174
 Fragmentierung 172, 569
 Fragmentierung, hohe 572
 Fragmentierungen vorbeugen 190
 Fragmentierungen vortäuschen 575
 Fragmentierungs-ID 173
 Fragmentierungs-Optionen von hping3..... 573
 Fragmentierungs-Queue verstopfen 572
 Fragmentierungszug zusammenbauen..... 570
 Fragment-Reassemblierung..... 174
 Fragmentverlust..... 173
 Frame 172
 Frame, Maximallänge..... 570
 Framegröße 172
 Framelänge ohne Fragmentierung 173
 Freizügige Banner 407
 Freizügige Dienste 406
 Frontend für Ping-Zugriffe 241
 FTP Bounce Scan 358
 FTP-Relays, offene finden 359
 FTP-Server als Zwischenstation für Portscans 359
 FTP-Server am Banner erkennen..... 422
 FTP-Server, anonymer Zugriff erlaubt? 359
 FTP-Server, Datenaustausch zwischen 358
 FTP-Server, überlange Paßworteingabe..... 835
 FTP-Uploads 556
 Full-connect TCP-Mapping 281
 Full-connect TCP-Scan 276, 317, 323
 Funktion, Zugriff auf in Windows 841
 Funktionen für Erlangen erweiterter Rechte..... 712
 Funktionsaufrufe, gefährliche 712
 fuzz-aqua 705
 Fuzzing 701
 Fuzzing als Bruteforce..... 703

Fuzzing, Testdauer	706
Fuzzy Search	116

G

Gast-Konto	736
Gefälschte Absenderadresse	237
Gefälschte Quell-IP-Adresse	599
Gefilterter Port	316
Gegenmaßnahmen	57, 84
Gegenmaßnahmen überprüfen	84
Gegenmaßnahmen vorschlagen	82
Geldanlage	42
Geräte ersetzen	670
Geschlossener Port	283, 316
Geschlossener Port, Fehlermeldung	284
Geschlossener Port, Window Size	353
Geschlossener Port, Zugriff auf	290
Geschlossener TCP-Port	328
Geschlossener UDP-Port	366
Geschützter Bereich, Webanwendung	890
Gesichtserkennung	885
GET	424
GET- und HEAD-Anfragen	533
GET-Parameter in der URL	891
\$_GET	775
gets	712
GFI LANguard	402
GID	734
Global Offset Table manipulieren	855
Google Hacking	738
Google, Usenet-Suche	92
Google-Suche optimieren	114
GOT	855
GOT-Adressen überschreiben	855
grep	400, 712
Grey Hat Hacker	75
Grundlegende Fehler	675
GUI-Anwendungen	705

H

Hacker	54
Halboffene Verbindungen	561
Halboffener Port	333
Half-open SYN-Scan	286, 333, 380
Half-open SYN-Scan, Entdeckungsgefahr	336
Half-open TCP-Mapping	286, 289
Half-open TCP-Mapping, geschlossener Port	289
Half-open TCP-Mapping, offener Port	286
Half-open TCP-Scans	317
Header-Length-Feld, Größe	184
Heap Overflow	838
Heise-DoS	830
HELO/EHLO-Statuscodes	506
HELP	424
Hexeditoren	666
Hintertür	557
Hintertür einrichten	801
Hintertür für Fernsteuerungs-Programme	402
Höchste IP-Adresse	140
Hochverfügbarkeit	644
Höflicher Verbindungsabbau	278, 279
Home-Verzeichnis	742
Home-Verzeichnis als Freigabe für Webs.	728
Honeypot	120
Hook	705
Hop	125
Hop, ausgehende Pakete verbieten	157
Hop, ein Paket pro Hop	149
Hop, eingehende Pakete verbieten	157
Hop, erster der Route	589

Hop, stiller	155
Hops ermitteln	144
Hops, Anzahl der	146
host	98, 107, 109
Host	21
Host, Erreichbarkeit	274
Host, Funktionen	447
Hostfunktion anhand offener Ports erkennen. 447	
Hostname	447
Hostnamen analysieren	187
Hostnamen zu IP-Adressen auflösen	105
Hostnamen, Namenskonventionen	106
hosts-Datei, lokale	226
Host-to-Host-VPN	655
hping3	238, 287, 353
hping3, Fragmentierungs-Optionen	573
hping3, Optionen	170
HP-UX ermitteln	455
HTML Injection	773
HTML	93
HTML, ausnutzen fehlerhafter Tags	807
HTML, Copyright	94
HTML, Generator	94
HTML, statisches injizieren	774
HTML-Dokument, Body analysieren	94
HTML-Dokumente, Infos ü. Authentisierungs-Mechanismen	95
htmlentities	796
HTML-Injection	762
HTML-Mail mit Internet-Referenz	123
HTML-Quelltext durchsuchen	93
HTTP	93
HTTP verkapseln	613
HTTP, OPTIONS	540
HTTP, überlange Eingaben	533
http_protocol.c	537
HTTP-Anfrage senden	213
HTTP-Cookies	780
HTTP-Fingerprinting	530
HTTP-Proxies, ausgehende, Port	604
httpprint	530
HTTP-Rückantwort, Formatierungen	541
HTTP-Rückantwort, Headerzeilen	537
HTTP-Statuscodes 200 bis 299	531
HTTP-Statuscodes 500 bis 599	531

I

IANA Port Numbers Assignment	396
ICMP address mask	244, 250
ICMP address mask request	455
ICMP destination unreachable fragmentation required-Fehlermeldung	485
ICMP destination unreachable-Meldung	316
ICMP echo	465
ICMP echo reply	206
ICMP echo reply-Rückantworten	206, 453
ICMP echo reply-Rückantwort provozieren	220
ICMP echo reply-Rückantworten unterdrücken	215
ICMP echo request-Anfragen erzwingen	127
ICMP echo request-Anfragen	161, 453
ICMP echo request-Anfragen ignorieren	237
ICMP echo request-Anfragen kommentarlos verwerfen	453
ICMP echo request-Anfragen, Länge setzen	222
ICMP echo request-Datagramm, Länge	221
ICMP echo request-Paket	456
ICMP echo request-Paket als Reiz versenden	453
ICMP echo-Nachrichten	125
ICMP information request	244, 251, 455
ICMP port unreachable-Fehlermeldung	204, 366
ICMP time exceeded in-transit	

Fehlermeldungen.....	203
ICMP timestamp.....	244, 465
ICMP timestamp request.....	455
ICMP time-to-live exceeded in transit.....	125
ICMP, Fehlermeldungen für UDP.....	304
ICMP-Anfrage m. gefälschtem Abs. an Broadcast-Adresse senden.....	564
ICMP-Anfragetypen.....	456
ICMP-Codes.....	204, 205
ICMP-Datagramme, verlorene.....	217
ICMP-Fehlermeldung.....	304
ICMP-Fehlermeldung, fehlende, Gründe für.....	373
ICMP-Fehlermeldungen, Rechte.....	371
ICMP-Fingerprinting.....	452
ICMP-information-Paket, Aufbau.....	251
ICMP-Mapping.....	203
ICMP-Mapping, Ergänzung.....	274
ICMP-Pakete.....	161
ICMP-Pakete, Zwischenstationen.....	183
ICMP-Rückantwort.....	206
ICMP-Sturm.....	564
ICMP-timestamp-Anfrage erstellen.....	246
ICMP-timestamp-Paket, Aufbau.....	245
ICMP-traceroute.....	160
ICMP-Typ-3-Fehlermeldungen.....	593
ICMP-Typen differenziert behandeln.....	215
ICMP-Typen ignorieren.....	249
ICMP-Typen.....	204, 205, 366
ICMP-Typen, alternative.....	244
ICMP-Typ-Feld.....	204
ICMP-Verhaltens e. Zielsystems auswerten.....	453
ICMP-Verkehr beobachten.....	208
Identification Field.....	173, 469
Identifikationsnummer eines Systems.....	104
Identitätsnachweis des Nutzers.....	863
Idle-Scan.....	355
ifconfig.....	130
ifconfig, MTU-Einstellungen.....	192
img-Tag.....	124
Inbound-Rules.....	631
index.php.....	449
Indexieren.....	89
Indirekte Identitäten.....	600
Indirekte Referenzierg. auf JavaScript-Dat.....	793
Infinites zyklisches NOP.....	432
Informationen zusammentragen.....	55, 62, 87
Informationen, verwertbare zurückschicken.....	410
Informationsaustausch.....	579
Inhaltsfilter.....	608
Initial Sequence Number.....	477
Initial Window Size, Größe.....	484
Injection.....	759
Inline-Firewalling.....	152
Insertion-Evasion.....	793
Institute for Security and Open Methodologies.....	38
Integrated Security Management System.....	56
Integrator.....	669
Integrität.....	43
International Organization for Standardization.....	37
Internetanbindung.....	46
InterNIC.....	96
Interrupt 80h.....	841
Intrusion-Detection-Regel für Portscans.....	386
IP Source Routing.....	181
ip_glue.....	576
IP-Adreßauflösung.....	98
IP-Adreßbereich ermitteln.....	111
IP-Adreßbereiche festlegen.....	250
IP-Adreßbereiche, Infos zu.....	98
IP-Adresse eines Hostnamens ermitteln.....	107

IP-Adresse.....	21, 64
IP-Adresse, falsche in TCP-Segmenten.....	562
IP-Adresse, höchste.....	140
IP-Adresse, Hostteil.....	250
IP-Adresse, Netzteil.....	250
IP-Adressen des Zielsystems.....	98
IP-Adressen herausfinden.....	104
IP-Adressen in Hostnamen umwandeln.....	46
IP-Adressen in Mailheadern.....	118
IP-Adressen zu Hostnamen auflösen.....	105
IP-Adreßvergabe, dynamische.....	553
IP-Adreßzuweisung überwachen.....	266
ipconfig.....	130, 192
IP-Datagramm mit best. TOS-Wert senden.....	462
IP-Fragmentierung.....	469, 569
IP-Header, Flags.....	173
IP-ID bei Protokollwechsel.....	474
IPID bekannter Systeme.....	471
IP-ID, gleiche.....	473
IP-ID-Generierung.....	469
IPIDs auswerten.....	355
IP-IDs, gleiche f. unterschied. Protokolle.....	474
IP-Paket, Route bis zum Ziel.....	125
IP-Pakete, Header.....	125
IP-Spoofing.....	237, 548, 599
iptraf.....	118, 128, 271
ISIC.....	703
ISO 17799, 20000.....	37
ISP.....	67
IT Infrastructure Library.....	37

J

java.util.Random.....	892
JavaScript.....	778
JavaScript injizieren.....	779
JavaScript, Rechte.....	808
JavaScript-Angriffe.....	786

K

Kamikaze-Paket.....	347
Kanalkapazität.....	193
Kein NOP.....	432
Keine Begrüßung.....	419
Kernelzugriffe.....	841
Key Assets.....	44
Keyword-Filter umgehen.....	610
Klasse-1-Fehler.....	676
Klasse-2-Fehler.....	676
Klasse-3-Fehler.....	676, 696
Kommando an Zielenwendung senden.....	426
Kommando in Shell-Umgebung ausführen.....	761
Kommandoeingaben ausprobieren.....	424
Kommandos aneinanderreihen.....	769
Kommandos einschleusen.....	712
Kommandozeile, Sonderzeichen.....	771
Kommunikationsdiagramm f. Server-DMZ.....	629
Kompetenzen vergeben.....	67
Konfigurationseinstellungen erfragen.....	251
Konfigurationsfehler.....	670
Kryptographische Protokolle.....	862
Kryptographische Verfahren.....	655
Kurze Pings.....	221

L

Lamp Test Segment.....	345
LAN Station Monitor.....	271
land.c.....	563
Land-Attacken.....	563
Lastverteilung.....	175

Latenz einer Verbindung.....	194
Latenzanalyse.....	193, 196
Latenzzeiten in Netzwerk.....	146
Laufwerke freigeben.....	729
Lebensdauer eines Pakets.....	125
Legitimität der Kommunikation nach etablierter Sitzung überprüfen.....	595
Leserechte auf /etc/passwd.....	748
Lexikalisches Fuzzing.....	704
Limited Broadcasts.....	137
linbrutemax, linbrutemin.....	868
Line Feed.....	543
Link, manipulierter.....	747
Listiges Mapping.....	235
List-Ordering.....	540
Load-Balancing.....	175
Lockvogel.....	392
Logdateien für Zugriffe.....	333
Logging überlasten.....	390
Login pro Konto, Zahl der erlaubten.....	883
Login-Prozess.....	424
Logische Operationen.....	713
Logische Teilnetze.....	140
Log-Repository.....	122
Lokale ARP-Tabelle manipulieren.....	269
Lokale Netzwerkkonfiguration auswerten.....	129
Loose Source Routing.....	181

M

MAIL FROM.....	508
MAIL FROM-Statuscodes.....	509
Mailheader analysieren.....	117
Mailserver ermitteln.....	500
Mailserver, Namenskonventionen.....	107
Mailserver, Statuscodes 200 bis 299.....	524
Mailserver, Statuscodes 500 bis 509.....	524
Mailserver, Statuscodes 500 bis 599.....	524
Mailserver, Statuscodes 550 bis 559.....	524
Mailserver, Statuscodes.....	505
Makro-Recorder.....	706
Man-in-the-Middle-Attacken.....	144
Mapping.....	157, 201
Mapping, Netzwerkprotokolle.....	202
Maximum Segment Size.....	22
Maximum Transmission Unit.....	173
MBZ-Analyse.....	463f.
MBZ-Bit, Echo.....	464
Mehrere Systeme ansprechen.....	136
Metadaten-Injection.....	764
Meta-Suchmaschinen.....	89
Metazeichen.....	755
MF.....	173
Microsoft IIS 5.0.....	536
Microsoft IIS, Header-Order.....	539
Mitschnitt des Datenaustauschs.....	23
mktemp.....	860
More Fragments.....	173
More Fragments-Bit.....	570
MTU der lokalen Schnittstelle.....	191
MTU.....	173, 189, 569
MTU, minimale.....	190
MTU-Einstellungen anzeigen.....	192
MTU-Größe setzen.....	174
Multicasting.....	136
Multiple Routen.....	175, 176
Multi-Proxy.....	604
Multi-Routing.....	179
Multitasking, kooperativ.....	858
Multitasking, präemptiv.....	858
MultiOS-Shellcodes.....	843
mysql_connect.....	817

N

Namensauflösung unterdrücken.....	223
Namensauflösung.....	105
Namensauflösungen, verzichten auf.....	376
Namensauflösungen, Zeitdauer.....	226
Namensgebung.....	188
Nameserver.....	46, 105
NASL.....	691
Nessus.....	691
Nessus-NASL-Plugin.....	108
NetBIOS.....	442
NetBIOS, Laufwerke freigeben.....	729
NetBIOS/SMB.....	455
NetBIOS/SMB-Ports.....	323
NetCat.....	213, 319, 405, 684
NetCat, SuSE Linux.....	319
netstat.....	118, 556
Network Address Port Translation.....	401
Netzmaske.....	140, 250, 465
Netzmaske 0.0.0.0.....	466
Netzmaske erfahren.....	465
Netzmaske, aktuelle erfragen.....	250
Netzwerk in Zonen unterteilen.....	641
Netzwerkabfrage.....	98
Netzwerkanbindung auslasten.....	550
Netzwerkanpassungen.....	670
Netzwerkdaten beziehen, Ablauf.....	129
Netzwerkdiagnose mit EtherApe.....	129
Netzwerkelemente.....	46
Netzwerkelemente, Namenskonventionen.....	107
Netzwerkkonfiguration anzeigen.....	130
Netzwerkmaske eines Netzwerksegments ermitteln.....	203
Netzwerkmedium erkennen.....	186
Netzwerkmedium virtuell segmentieren.....	650
Netzwerkparameter dynamisch zuweisen.....	129
Netzwerkplan, Inhalt.....	63
Netzwerkschnittstelle.....	23
Netzwerkschnittstelle, Promiscuous-Mode.....	270
Netzwerkschnittstellen anpassen.....	192
Netzwerkverkehr auswerten.....	127
Netzwerkverkehr n. ARP-Paket untersuchen.....	270
Neue Fehler.....	675
Neuen Sicherheitslücke veröffentlichen.....	707
NFS.....	446, 730
Nicht abgeschlossene Fragmentierung.....	573
Nicht antwortende Zielsysteme.....	213
Nicht vorhandene Zielsysteme.....	210
Nicht-autoritativer Server, Namensauflösung.....	106
Nikto.....	691
nmap.....	214, 229, 299, 307, 324
nmap, Full-connect TCP-Scans.....	323
nmap, geschlossener TCP-Port.....	329
nmap, Mapping-Optionen.....	312
nmap, offener Port.....	324
nmap, Optionen.....	324
nmap, Ping-Suchlauf.....	230
nmap, Shared IP ID Sequence Boolean.....	473
nmap, Standardtyp für Portscans.....	325
nmap, Timing Policy Templates.....	387
nmap, Verbindungsabbau/-aufbau.....	326
nmap-os-fingerprints.....	447
NOOP-Sled.....	845
NOP.....	431
NOP-Verhalten.....	521
nslookup.....	107, 108
NTFS.....	732
Null, Exponent.....	700
Null-Byte.....	711, 837, 841
Null-Scan.....	341, 348

O

objdump, Parameter 856
Object-Spanning 630
Off-by-One-Pufferüberlauf 835
Offene Verbindungen unter Windows 119
Offenen Port erkennen 332
Offenen TCP-Port suchen 284
Offener Port 283, 316
Offener Port, Reaktion d. Zielsystems 284
Öffentlicher Teil, Webanwendung 890
Onlinebanking-System 45
Online-Frontend zu Ping, eigenes 241
Online-Hilfe auswerten 424
Onlinehilfe, Nennung des Systems 493
Online-Ping 240
Online-Tools für Netzwerkdagnosen 240
Opcodes 840
Open Source Security Testing Methodology Manual 38
Organisation, zentrale Objekte einer 44
Organisatorischer Sicherheitstest 53
Originalpaket erneut versenden 190
OS Command Injection 712
OS Fingerprinting 439, 678
OSSTMM 3.0 38
Outbound-Rules 631

P

Paketfilter, Kriterien für Weiterleitung 293
Paket auf dem Weg zum Ziel abgelaufen 204
Paket erreichte Ziel nicht 125
Paket verwerfen 125, 157
Paket, zu großes verwerfen 485
Pakete m. gesetztem ACK-Flag 294
Pakete verbieten 157
Paketfilter 587
Paketfilter umgehen mit altern. Portnummern 595
Paketfilter umgehen 170, 175, 292
Paketfilter, Anwendungsschicht 602
Paketfilter, Protokoll-Header 590
Paketgenerator 238
Paketgröße anpassen 195
Paket-Maximalgröße 485
Paketorientierte Kommunikation 21
Paket-Priorität 460
Paketverlust von 100 Prozent 210
Parameter-Injection 817
Passives ARP-Mapping 270
Passives FTP 425
Paßwort, Bruteforce-Attacken 867
Paßwort, schwaches 864
Paßwort, Stärke 864
Paßwort-Authentifizierung, Protokoll 865
Paßwort-Authentisierung über Datenbank 822
Paßwort-Datei auslesen 762
Paßwortdatei des Webservers anzeigen 772
Path MTU Discovery Mechanism 190
Path MTU zu Zielsystem ermitteln 191
Path MTU 173, 189, 190, 485, 569
pathchar 194
Pattern-Matching 88
pchar 194
Penetration Test 58
Penetration Test, Blackbox-Verfahren 59
Penetration Test, Definition 53
Penetration Test, Greybox-Verfahren 59
Penetration Test, Voraussetzungen 64
Penetration Test, Whitebox-Verfahren 59
Perimeter-Firewall 155

Perimeter-Systeme 50
Persil-Schein 63
Personal Firewalls 214
Personal Identification Number 864
Pfadangaben 741
Phishing 671
PHP 95, 767
PHP, at-Zeichen 819
PHP, Datentypen 750
PHP, Fehlermeldungen 819
PHP, Formatumwandlungen 795
PHP, include 890
PHP, Tags löschen 796
php.ini 819
PHP-Funktionen, kritische 711
PIN 863
Ping auf Betriebssystem nicht möglich 454
Ping in großen Netzwerken 227
Ping of Death 575
Ping 73, 203
Ping, ARP- 258
Ping, Linux 460
Ping, Route Record-Option 183
Ping, Windows 460
Ping, Zeitmessung 223
Ping-Anfragen, nur einige unbeantwortet 221
Ping-Implementierung, Eigenschaften eines anderen Systems vortäuschen 212
Ping-Mapping 206
Ping-Mapping, Ablauf 220
Ping-Pong-Verhalten 209
Ping-Suchlauf 227
Ping-Suchlauf mit gefälschter Absenderadresse 237
Ping-Suchlauf, großflächiger 233
Ping-Sweep 227
pingsweep.sh 227
Ping-Überprüfungen durch Online-Dienste 240
Ping-Verhalten kennzeichnen 220
Ping-Zugriff auf ein einzelnes System 206
Ping-Zugriff mit gefälschter Absenderadresse, Ablauf 238
Ping-Zugriff mit Hostnamen 224
Ping-Zugriff über versch. Netzwerke 213
Ping-Zugriff, Ablauf 206
Ping-Zugriff, Protokolle filtern 234
Platzhalter für Variablen 849
PLC 276
Policies 38, 56
Port 445, Windows 444
Port 80, 8000, 8080 594
Port reagiert nicht 316
Port, CLOSED-Status 316
Port, LISTENING-Status 316
Portbelegung 396
Portbelegung, Unix-System 445
Portbelegung, Windows 442
Portfilter 165
Port-Forwarding 120, 401
PORT-Kommando 361
Portlisten des Betriebssystems, lokale 399
Portmapper 446
Portnummer zu Dienst zuweisen 396
Portnummern, alternative 165, 595
Portnummern, Liste der z. Zt. vergebenen 397
Port-Redirection 603
Port-Redirection ausnutzen 611
Ports 0 bis 1023 397
Ports 1024 bis 49151 398
Ports 49152 und 65535 398
Ports auswerten 440
Ports bekannter Dienste 390
Ports des Firewall-Systems abtasten 592

Ports eines Zielsystems, alle untersuchen.....	318
Ports für Hintertüren.....	398
Ports v. TCP-Diensten.....	285
Ports von bekannten Hintertüren	402
Ports, kurzlebige	398
Ports, NetBIOS-Dienste.....	443
Ports, private	398
Ports, typische eines Betriebssystems	441
Ports, wichtige für Sicherheitsüberprüf.	383, 384
Portscan für Proxy-Dienste	603
Portscan, Legalität	319
Portscan, Mapping unterdrücken.....	378
Portscan, Namensauflösungen.....	376
Portscan, Ressourcen- und Zeitminimierung....	327
Portscan, Zahl der Portzugriffe	386
Portscan-Methoden.....	316
Portscanner, Timing-Verhalten einstellen	386
Portscanner-Optimierungen	324
Portscanning mit nmap.....	691
Portscanning	315
Portscans verstecken	380
Portstati.....	316
POST-Abfragen, injizierte.....	804
POST-Zugriffe	806
Präsentation d. Ergebnisse	81
Precedence Bit TOS Echoing	460
Pre-shared Secret	122, 863
Primary Nameserver	105
printf.....	852
Private IP-Adressbereiche	142
Procedure Linkage Table	855
Professioneller Angreifer	35
Programmaufruf, überlange Zeichenkette übergeben	834
Programmausgaben festhalten.....	72
Programmausgaben speichern.....	69
Programmausgaben	713
Programmcode, ausführbaren einschleusen.....	777
Programmkonventionen verletzen.....	701
Programmquelltext	666
Projektzuschlag.....	62
Promiscuous-Mode	128
Promiscuous Mode, Protokoll-Analyzer.....	879
Proof-of-Concept	57, 58, 717
Protocol Analyzer	21, 666
Protocol-Tunnelling	603
Protokoll	21
Protokolldateien des Serversystems.....	122
Protokolle unterschiedl. Prod. vergleichen.....	659
Protokolle verkapseln	613
Protokolle, Ethertype-Codes	260
Protokollfamilie im Internet.....	21
Protokollstack	452
Provozierte Begrüßung.....	419
Proxy als Hop mißbrauchen.....	611
Proxy-Dienste, Portscan.....	603
Proxy-Hubs.....	600
Proxy-Mechanismen.....	603
Proxyspezifisches Application Mapping	605
Proxy-Verbindungen	358
Prozentzeichen	851
Prozessorbefehle aneinanderreihen	839
PScan	712
PSH	276
PSH-Flag	345
Pufferstand	484
Pufferüberlauf.....	712, 832
Pufferüberlauf, Off-by-One	835
Pufferüberlauf-Schwachstellen, stackbasiert	832
Punkt-zu-Punkt-Verbindungen	136
PUT- und DELETE-Anfragen	533

Q

Quellen vortäuschen.....	599
Quell-Ethernet-Adresse fälschen	267
Quellport, unschuldiger	389
Quell-Socket.....	22
Quelltext durchsuchen	712
Quelltext-Analyse.....	711
Queue-Überlastung	560
Queuing-Mechanismen	195
QUIT	424

R

Race Condition	712, 858
Race Condition, C-Funktionen.....	860
RARP	255
Rauschen vortäuschen.....	392
rawurdecode.....	795
Read-only	731
Reaktion auf ICMP echo request«-Anfragen.....	453
Reaktion auf unerwartete TCP-Anfragen.....	316
Real World Test	58
Re-Audit	85
Rechner vor Ping-Mapping verstecken.....	215
Rechnerverbund	557
Reconnaissance.....	103
Redirect	889
Regel, Akzeptanz.....	627
Regel, vertretbare.....	626
Regelattribute bewerten	622, 625
Regelattribute.....	620
Regeln grafisch auswerten	628
Regeln, verwaiste	621
Regelwerk exportieren	616
Regelwerk, dichtes	622
Regelwerk, unsichere Objekte.....	626
Reiz/Reaktion Proof of Concept	683
Reize versenden.....	195
Replay-Angriff.....	878
Report, Datenbankfelder für.....	79
Report, Inhalt, Aufbau.....	77, 79
Reset einer Verbindung	276
Ressourcen verteilen	175
Restriktive Hops	152
Reverse Engineering	666
Risiken, Abwesenheit von	36
Risikoberechnung, Aufwand	35
Risikoberechnung, Grundatz der.....	35
Risikobewertung eines Assets	42
robots.txt.....	677
root	734
root, Paßwort	877
Root-Server.....	106
Root-Verzeichnis.....	742
Round Robin.....	175
Round Trip Time von ICMP-echo- Verbindungen	197
Round-Trip-Time ermitteln.....	223
route	133
Route eines IP-Pakets bis zum Ziel	125
Route eines IP-Pakets erkennen.....	589
Route Record-Option	183
Route selbst definieren	181
Route, erster Hop	589
Router zwischen zwei Netzen.....	152
Router, ARP-Pakete	272
Route-Traceing.....	125, 144, 589
Routing	181
Routing-Informationen abfragen	97
Routing-Loop.....	145
Routing-Tabelle ausgeben	133

Routing-Tabelle auswerten.....	133
Routingwechsel.....	176
RPC.....	446
RSA SecurID.....	882
RST.....	276
RST-Antwort, ausbleibende.....	350
RST-Methode.....	328
RST-Nutzdaten.....	486
Rückantworten zu unterschiedl. Zeitpunkten.....	195
Rückantworten, Größe der.....	554
Rückkanal abhören.....	240
Rundlaufverfahren.....	175
Rundungen.....	701

S

Scan TCP Closed Minimum.....	328
Scan TCP Open Minimum.....	327
scanf.....	712
Scanning-Software.....	681
Scan-Resultate in Datei schreiben.....	389
Scan-Zugriffe, kurze zusammenführen.....	387
Scheduler.....	858
Schlüsselraum.....	865
Schlüsselraum durchlaufen.....	868
Schnittstelle.....	23
Schnittstelle in Promiscuous-Mode schalten.....	128
Schutzkriterien.....	42
Schutzverletzung.....	832, 834
Schwache WEP-Verschlüsselung.....	675, 676
Schwache Zufallszahlen.....	712
Schwachstelle beweisen.....	57
Schwachstelle gefunden, weiteres Vorgehen.....	57
Schwachstelle, Existenz ermitteln.....	687
Schwachstelle, Schweregrad berechnen.....	38
Schwachstellen ausnutzen.....	725
Schwachstellen, neue suchen.....	696
Schwachstellen, untersuchen auf.....	57
Screenshots.....	75
Scriptcode injizieren.....	777
Script-Injection.....	774
Secondary Nameserver.....	105
SecurityFocus.....	669
SecurityFocus.com.....	678
Segmentation Fault.....	699, 834
SELECT, Ausgabe von beeinflussen.....	817
Selective Acknowledgements.....	481
Semi-professionelle Angreifer.....	34
SEQ-Test.....	478
Sequenznummer.....	22, 277, 477
Sequenznummer, Wahl der.....	478
Sequenznummern auslesen.....	581
Sequenznummern synchronisieren.....	276
services-Datei.....	399
services-Datei, lokale.....	397
Session Fixation.....	893
Session kopieren.....	891
Session Riding.....	801
Session-ID.....	891
Session-ID erzeugen.....	892
Sessionnamen.....	449
setcookie.....	783
setproctitle.....	852
shell_exec.....	761
Shellcode.....	839
Shellcode, Zeichensatz.....	845
Shellcodes, Linux.....	839
Shellcodes, systemunabhängige.....	843
Shellcodes, Windows.....	841
Sicherheit, Definition.....	36
Sicherheitslücke.....	667
Sicherheitslücke ausnutzen.....	53, 58, 692
Sicherheitslücken beweisen.....	58
Sicherheitsrichtlinien prüfen.....	66
Sicherheitsrichtlinien.....	38
Sicherheits techn. Schwachst. in Organisation e.....	
Unternehmens ermitteln.....	56
Sicherheitsüberprüfung a. konzeption. Ebene.....	57
Sicherheitsüberprüfung, Dokumentation.....	36
Sicherheitsüberprüfung, hostbasiert.....	60
Sicherheitsüberprüfung, kontrollierte, Phasen.....	84
Sicherheitsüberprüfung, netzwerkbasierte.....	61
Sicherheitsüberprüfung, primäre.....	84
Sicherheitsüberprüfung, Standards.....	37
Sicherheitsüberprüfungen organisieren.....	27
Simple Services.....	364, 369, 431
SING.....	461
Single Point of Failure.....	644
Site-to-End-VPN.....	655
Site-to-Site-VPN.....	655
Sitzungs-Timeout.....	427
Skript-Kiddies.....	32
Slashdot-Effekt.....	830
Slow-Scans.....	385
SMB/CIFS.....	419
SMTP, Begrüßungsverhalten.....	505
SMTP, NOP-Kommando überprüfen.....	522
SMTP, Onlinehilfe auswerten.....	512
SMTP, optionale Kommandos.....	518
SMTP, Standards.....	500
SMTP-Befehle, gefährliche.....	514
SMTP-Fingerprinting.....	500
SMTP-Mailheader.....	117, 118
SMTP-Proxy, Port.....	604
smtpscan.....	501
smurf.c.....	563
Smurf-Attacken.....	565
Sniffer.....	23, 878
Sniffing.....	128, 144, 270, 581
SNMP.....	865
SOA Resource Record.....	105
Social Engineering.....	116, 671
Socket-Konzept.....	596
Software-Inventarliste.....	64
Solaris ermitteln.....	455
IST/SOLL-Analyse.....	39
Sonderzeichen nicht als Tags interpretieren.....	796
Source Routing, Hops.....	181
Speicherabhängiger Code.....	855
Speicherbereiche prüfen.....	712
Speicherinhalte d. Stacks auslesen.....	852
Speichermangel.....	676
Speicherstellen, beliebige überschreiben.....	853
Speicherzustände manipulieren.....	698
Spoofing.....	237
Spoofing-Angriff.....	548
Sporadisches N00P.....	432
sprintf.....	712
SQL Injection.....	810
SQL, Performance-Analyse.....	830
SQL-Injection durch Eingabeungültigkeit.....	817
SQL-Parameter-Injection.....	813
SQL-Server hinter Webseite, Port.....	95
SQL-Statement manipulieren.....	813
Stack manipulieren.....	852
Stack, Pointer manipulieren.....	834, 845
Standardkonten.....	876
Standardpaßwörter.....	876
stat.....	860
Stateless Paketfilter-Firewalls.....	172
Statische ARP-Einträge.....	266
Statische Zeichenketten.....	754
Statistik des Datenverkehrs ausgeben.....	128
Statistische u. indir. Analyse v. TCP-Ports.....	316

Status Messages.....	536
Statuscodes, erweiterte.....	524
Statuslose Firewall.....	294
Statusmeldungen, MS IIS.....	536
Statusorientierung.....	275
stcmin.....	328
Stealth-Rules.....	632
Stealth-Scan.....	333
Stealth-Techniken.....	380
Steuerdaten injizieren.....	762
Stille Anwendungen.....	494
Stille Banner.....	408
Stille Dienste.....	406
Stimm-/Spracherkennung.....	885
stomin.....	327
Stored Procedures, Angriffe auf.....	827
Stored Procedures, Microsoft SQL Server.....	828
strcat.....	712
strcpy.....	711, 712, 832
Stressing-Tools.....	667
Strict Source Routing.....	181
String-Input.....	426
strip_tags.....	796
Strobe.....	318, 325, 383
strpos.....	750
Stürme.....	560
Subnetzmaske.....	140, 250, 630
Suchmaschinen.....	87
Suchmaschinen abfragen.....	112
suid.....	736
SuperScan.....	377
SwitcH, interne ARP-Tabelle.....	271
Switchover.....	645
Systembefehl, Programm kontroll. beenden.....	841
Symantec NetRecon.....	684
Symbole, reservierte.....	770
SYN.....	276
SYN-Cookie.....	563
SYN-Flag.....	277, 345
synflood.....	562
SYN-Flooding.....	327, 337, 560
SYN-Paket.....	170
SYN-Scan.....	334
SYN-Scan, TCP-Segmente sparen.....	335
syslog.....	266, 852
syslog-Server.....	122, 659
System einfrieren.....	548
System fragt anderes nach Uhrzeit.....	245
Systemabsturz.....	547
Systemaufrufe, Linux.....	841
Systemauslastung.....	548
Systembibliotheken, Windows.....	841
Systemkommandos auf Webserver.....	759
Systemkommandos injizieren.....	759
Systemneustart.....	548
T	
tail.....	122
tcdump, Darstellung des Paketinhalts.....	24
tcdump, Filterbeschreibung.....	24
tcdump, Infos d. Schicht 2 anz.....	24
tcdump, Namensauflösung unterdrücken.....	24
tcdump, Pakete in Datei schreiben.....	24
tcdump, Pakete von Datei lesen.....	24
tcdump, Zeitstempel abschalten.....	24
TCP RST, Rückantwort.....	592
TCP Window Size.....	484
TCP.....	275
TCP, 4-Segmente-Prinzip.....	280
TCP, halboffene Verbindung.....	277
TCP, Verbindungsabbau.....	327
TCP/IP.....	21
TCP/IP-Stack um Paketfilter-Funktionalität erweitern.....	587
TCP-/UDP-Mapping.....	274
TCP-Dienste, Ports.....	285
tcpdump.....	21, 118, 270, 878
tcpdump, Oktetts übergeben.....	24
tcpdump, Optionen.....	24
tcpdump-Mittschnitt.....	21
TCP-Fingerprinting.....	468
TCP-Flag, keines setzen.....	348
TCP-Flags prüfen.....	293
TCP-Flags.....	22, 171, 275, 276
TCP-Flags, viele gesetzt.....	344
TCP-Flooding.....	327
TCP-Hijacking.....	580
TCP-Mapping anhand ACK-Flag.....	292
TCP-Mapping in Adreßbereichen.....	298
TCP-Mapping m. SYN-Flag, keine Rückgabe.....	292
TCP-Mapping.....	275
TCP-Port 53.....	105
TCP-RST-Kill.....	580
TCP-Segment mit FIN-Flag an Zielport senden.....	341
TCP-Segment mit gefälschter Absenderadresse.....	563
TCP-Segment mit RST-Flag.....	286, 342
TCP-Segment, Aufbau.....	276
TCP-Segment, Funktion.....	275
TCP-Sitzung schließen.....	280
tcptraceroute.....	162
tcptraceroute, TCP-Pakete.....	162
tcptraceroute, TCP-Segmente.....	169
tcptraceroute, Transportprotokoll.....	164
TCP-Tunneling.....	597
TCP-Verbindung, Datenaufkommen verringern.....	289
TCP-Verbindung, Duplikate.....	482
TCP-Verbindung, Log-Eintrag vermeiden.....	286
TCP-Verbindung, unvollständige.....	380
TCP-Verbindungsabbau mit FIN-Methode.....	278
TCP-Verbindungsabbau b. versch. Portstati.....	317
TCP-Verbindungsabbau.....	276
TCP-Verbindungsabbau, erster.....	277
tcpview.....	118
TCP-Wrapper.....	338
Teardrop.....	576
Technische Sicherheitsüberprüfung.....	57
tee.....	74
Telnet.....	100
Telnet, Zielport manuell festlegen.....	281
telnet.exe.....	281
Telnet-Abfrage.....	100
Telnet-Client, Banner-Grabbing.....	405
Thin Clients, automatische Konfiguration.....	251
Tiger Team.....	58
Timeline-Diagramme.....	23
Timeout-Verhalten v. Anwendungen.....	431
timestamp.....	22
Timestamp-Berechnung.....	482
Timestamp-Pakete nicht weiterleiten.....	249
Timestamp-Zugriff.....	245
TOCTOU.....	859
Token, Authentisierung ohne.....	883
Token-basierte Systeme.....	882
Token-System.....	122
TOS.....	433, 460
TOS Unused Bit.....	463
TOS-Bit.....	178
TOS-Werte übernehmen.....	462
TOS-Werte von Netzwerkanwendungen.....	180
tracpath, UDP-Pakete.....	162

Traceroute 125, 589
 traceroute, !A 159
 traceroute, !C 159
 traceroute, alternative Portnummern 166
 traceroute, ICMP 161
 traceroute, Trägerprotokolle 160
 traceroute-Zugriff mit spez. Zielport 167
 traceroute-Zugriffe, Ports 165
 tracert.exe 127
 Trägerprotokolle, alternative für traceroute 160
 Transportprotok., verbindg- und statuslos 364
 Trigger von amap 415
 Trojanische Pferde 395
 TTL läuft ab 125
 TTL-Auswertung 144
 TTL-Wert 125, 589
 TTL-Wert im IP-Header der Rückantwort 177
 TTL-Wert von 1 152
 TTL-Wert, initialer 145
 TTL-Wert, niedrige 155
 TTL-Wert, Reaktion auf niedrigen 155
 TTL-Werte anpassen 195
 TTL-Werte dekrementieren 155
 Tunneling 612
 TURN-, SOML- und SAML-Statuscodes 518
 Type of Service 433
 Type-of-Service-Feld 179, 433
 Typische Schwachstellen suchen 677

U

Überfluten mit Anfragen 560
 Überlappende Fragmentierung 576
 Überlauf von Speicheradressen 839
 Überlauf 701
 Überprüfungen zyklische wiederholen 85
 Überprüfungsmodule 49
 Überprüfungsmodus festlegen 53
 UDP 364
 UDP, Fehlermeldungen 304
 UDP, Portstati 366
 UDP-Datagramm 160
 UDP-Datagramm, Aufbau 303
 UDP-Datagrammheader 365
 UDP-Mapping 303
 UDP-Port 366
 UDP-Port bietet keinen Dienst an 204
 UDP-Port, geschlossen 366
 UDP-Portscan 317, 364, 365
 UDP-Portscan auf die ersten 1024 Ports
 einer CP-Firewall 592
 UDP-Portscan, keine Antwort 368
 UDP-Reiz, einzelner für Rückantwort 369
 UDP-Rückantwort 369
 UDP-Rückantwort provozieren 566
 UDP-Scan auf daytime-Dienst 369
 UDP-Sturm 566
 UDP-Traceroute 125
 UID 734
 Umgebungsvariablen manipulieren 697
 Unerwartete Anfrage 340
 Unerwartete Daten injizieren 696
 Unicast-Ping 455
 UNION-Statements 826
 Unschuldige Quellports 389
 Unsichere Programmiersprachen 711
 Unterlauf 701
 Unvorhergesehene Zustände in
 Zielumgebung erzeugen 697
 Upstream 551
 Upstream, Auslastungsangriff 554
 URG-Flag 345

URL, Codierung 794
 URL-Blacklist 609
 urldecode 795
 URLs filtern 609
 Usenet-Newsgruppen 91
 USER 424
 usr/share/nmap/nmap-os-fingerprints 470

V

Vanilla Scan 318, 383
 Variablen, Platzhalten 848
 Variablenzustände untersuchen 715
 Verbindung abrupt abbauen 286
 Verbindung abschließen 276
 Verbindung höflich beenden 424
 Verbindungen auf Kabel mitlesen 128
 Verbindungen unerlaubt trennen 579
 Verbindungen, nicht erfolgreiche 590
 Verbindungsabbau bestätigen 341
 Verbindungsabbau, autom. serverseitiger 428
 Verbindungsabbr., abrupter mit RST-Seg. 334
 Verbindungsanforderungen filtern 293
 Verbindungsaufbau bestätigen 170
 Verbindungsaufbau mit TCP 316
 Verbindungsaufbau, abrupter 330
 Verbindungsaufbau, Initiator bricht ab 334
 Verbindungs-Endpunkte 136
 Verbindungsorient. Protok. d. Transportsch. 275
 Verbindungsstatus, Statuscode 536
 Verfügbarkeit 43
 Vergeltungsangriff 31
 Verhaltensbezogenes Fingerprinting 500
 Verlorene ICMP-Datagramme 217
 verr 852
 Verschiedene Pakete anzeigen 309
 Verschiedene Quellsysteme auswählen 387
 Vertraulichkeit 42
 Verwundbarkeitsdatenbanken 669, 678, 679
 Verzeichnis-Hierarchie 744
 Verzeichnisstrukturen auswerten 450
 Videomitschnitte 76
 Vielzahl an Zugriffen zwecks Überlagerung 390
 Virtualisierung 650, 652
 VirtualPC 652
 Virtuelle Adreßräume 855
 Virtuelle Betriebssysteme 652
 VLAN, Hardware-Ports 651
 VLAN, IP-Adressen 651
 VLAN, MAC-Adressen 651
 VLAN, Schichten 651
 VLAN-ID 650
 VLANs anhand von Portnummern 651
 VLANs 650
 VM, Ausbruch aus Gastsystem 653
 VM, erweiterte Rechte in and. Gastsystem 653
 VMware 652
 Vorgehen b. gefundener Schwachstelle 57
 VPN 655
 VRFY- und EXPN-Statuscodes 515
 VRFY 514
 Vulnerability Assessment 57
 Vulnerability Scanner 667
 Vulnerability Scanning durch Exploiting 692
 Vulnerability Scanning 682
 Vulnerability S., Schwachst. ausnutz. während .. 687
 vulscan.sh 685
 vwarn 852

W

warn	852
Web Developer	768
Webanwendung, geschützter Bereich	888
Webanwendung, öffentlicher Teil	888
Webanwendung, Statusorientierung	890
Webapplikation, einloggen in gesperrte	826
Webapplikation, genutzte Technologie	449
Webbasierte Administrationsschnittstellen	594
Webbugs	124
WebDAV	498
Webformulare einschränken	768
Webfrontend der Konfigurationsschnittstelle	594
Webproxy	608
Webseite, Scriptcode injizieren	774
Webserver ermitteln	530
Webserver unter Kontrolle d. Angreifers	785
Webserver unterstützt welche Befehle	540
Webserver, 200-Meldung	536
Webserver, 404-Meldung	534
Webserver, Allow-Order	540
Webserver, Content-Length	537
Webserver, Entity Tag	541
Webserver, Header-Ordering	538
Webserver, Header-Wording	537, 538
Webserver, Logdateien	120
Webserver, Namenskonventionen	106
Webserver, Statuscode 301	689
Webserver, Systemkommandos	759
Webserver, Ressourcen unter alter URL	889
Webserver, Zeilentrennzeichen	543
Webserver-Fehlermeldungen	495
WebServerFP	530
Webverzeichnis, Aufbau	91
Well-known Ports	397
Werte von Assets	43
Wettlaufsituation	858
wget	555
WHERE-Abfragen manipulieren	820
WHERE-Klausel, fehlerhafte	818
White Hat Hacker	54
Whitebox-Überprüfung	54f.
Whitelists ermitteln	787
Whitelists	610
Whitelists, Eingabeinschränkung	787
whois, Domänen-Abfrage	97
whois, Standardport	96
whois-Abfrage	96, 110, 139
whois-Abfrage für IP-Adressen	99
whois-Abfrage, manuelle	100
Willkommens-Banner	407, 419, 496
Willkommens-Banner provozieren	420
Willkommens-Banner, Struktur	420
%windir%\system32\drivers\etc\hosts	226
Window Size	22, 353, 483
Window Size 0	353
Window-Scan	353
Windows-Version ermitteln	444
Windows-Versionen, Portstati	444
Windows-XP Service Packs ermitteln	454
WINS	442
Wortlisten verknüpfen	875
Wortlisten	873

Wortlisten, personalisierte	875
Wrapper-Skript	816
www.iana.org/assignments/port-numbers	397
www.samspace.org	243
www.scip.ch	679
www.secunia.com	679
Wyd	875

X

XArp	267
Xmas-Scan	340, 344
XMLHttpRequest	804
xp_cmdshell	828
xwinjig	705

Z

Zähler, unterschiedl. für versch. Protokolle	474
Zeichenbasiertes Fuzzing	703
Zeichenkette in Datei suchen	400
Zeichenkombinationen überprüfen	868
Zeilenvorschubzeichen	543
Zeitstempel	22
Zertifizierung d. Informationssicherheitssyst	37
Ziel einer Sicherheitsüberprüfung	42
Zielbereiche aufteilen	387
Zielnetzwerk auswerten	103
Zielobjekt beeinflussen	697
Zielobjekt einer Sicherheitsüberprüfung, ablenken von	392
Zielport, Rückgabe provozieren	396
Zielports aufteilen	387
Zielportverhalten, anhd. d. Diensts erkenn	413
Ziel-Socket	22
Zielsystem ACK-Segment schicken	170
Zielsystem indirekt ermitteln	282
Zielsystem mit Verbindungsanfrg. überflut	560
Zielsysteme in IP-Adreßber. herausfinden	298
Zombiehost	355, 359
Zombiehost, Rückantwort	356
Zonendatei	105
Zonen-Segmentierung	649
Zonentransfer	105, 108
Zu lange Fragmentierung	575
Zufälligkeit	892
Zugriff kommentarlos werfen	591
Zugriff ohne Authentisierung	887
Zugriff verbieten	591
Zugriff wiederholen	878
Zugriffe partiell eingeschränkt, traceroute	152
Zugriffsbit	736
Zugriffspfad ermitteln	125
Zugriffspfaddiagramm erstellen	143
Zugriffsprotokoll	390
Zugriffsrechte in Unix/Linux-Umgebungen	733
Zugriffsrechte in Windows-Umgebungen	730
Zugriffsrechte	729, 735
Zweites Fragment e. Anfrage	174
Zwischenablage, Inhalt senden an and. Server	786
Zwischenstation der ICMP-Pakete im IP-Header	183
Zyklische Sicherheitsüberprüfungen	51