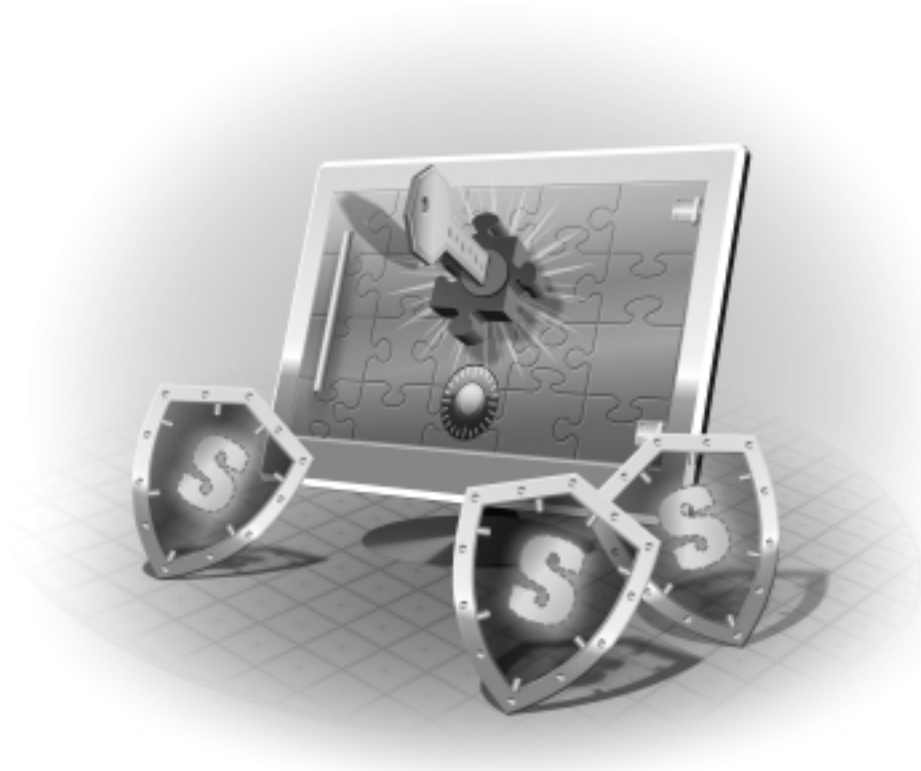




Computer & Literatur Verlag GmbH

PENETRATIONS-TESTS

von Thomas Werth



Bibliographische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliographie; detaillierte bibliographische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Alle Rechte vorbehalten. Ohne ausdrückliche, schriftliche Genehmigung des Herausgebers ist es nicht gestattet, das Buch oder Teile daraus in irgendeiner Form durch Fotokopie, Mikrofilm oder ein anderes Verfahren zu vervielfältigen oder zu verbreiten. Dasselbe gilt für das Recht der öffentlichen Wiedergabe.

Der Verlag macht darauf aufmerksam, daß die genannten Firmen- und Markenzeichen sowie Produktbezeichnungen in der Regel marken-, patent-, oder warenzeichenrechtlichem Schutz unterliegen.

Die Herausgeber übernehmen keine Gewähr für die Funktionsfähigkeit beschriebener Verfahren, Programme oder Schaltungen.

1. Auflage 2012

© 2012 by C&L Computer und Literaturverlag
Zavelsteiner Straße 20, 71034 Böblingen
E-Mail: info@cul.de
WWW: <http://www.CuL.de>

Coverdesign: Hawa & Nöh, Neu-Eichenberg
Satz: C&L Verlag
Fotografien in Kapitel 3: Nadine Werth
Druck: PUT i RB DROGOWIEC
Printed in Poland

Dieses Buch wurde auf chlorfrei gebleichtem Papier gedruckt

ISBN 978-3-936546-70-5

Gewidmet meiner lieben Familie:

Meiner wunderbaren Frau Nadine,
meiner phantastischen Tochter Maya
und unserem Neuzugang Tom

INHALT

Geleitwort 17

Vorwort 19

Kapitel 1: Die Testorganisation 21

1.1 Der Auftrag 22

 1.1.1 Testtypen 22

 1.1.2 Methodik 26

 1.1.3 Audit 31

1.2 Die Dokumentation 35

1.3 Der Vertrag 39

 1.3.1 Vereinbarungen 39

 1.3.2 Vertragsanhang 44

1.4 Der Arbeitsplatz 45

Kapitel 2: Die Arbeitsumgebung 47

2.1 Testprogramme 48

 2.1.1 Passwort-Programme 55

 Wortlisten 57

 Passworte bruteforce erraten 61

 Passworte offline knacken 61

 Sniffer und Passwortknacker 67

 Sniffer und Man in the Middle 68

 2.1.2 WLAN-Tools 74

 aircrack-ng 74

 2.1.3 Informationsverwaltung 83

2.2 Exploit-Frameworks.....	87
2.2.1 Metasploit Framework.....	89
Programme.....	93
Module.....	105
Plugins	111
2.2.2 Social Engineering Toolkit	112
Installation.....	113
Konfiguration.....	114
Angriffe.....	115
Backdoors	119
2.2.3 Web Application Attack and Audit Framework.....	121
Profile.....	126
Angriffe.....	130
Shell-Sitzung	132
2.3 Tools für IPv6.....	133
2.3.1 THC IPv6 Attack Toolkit	134
dos-new-ip6.....	134
detect-new-ip6	135
alive6...	135
redir6.....	136
Fake_router6	137
parasite6.....	138
2.4 Backtrack	139
2.4.1 Installation	141
2.4.2 Grafische Oberfläche.....	152
2.4.3 Verschlüsselung.....	155
2.4.4 Konfiguration	160
2.4.5 Aktualisierung	169

Kapitel 3: Informationsgewinnung..... 171

3.1 Veröffentlichte Informationen sammeln.....	171
3.1.1 Basisinformationen.....	172
3.1.2 Detailinformationen.....	177
3.1.3 Domaininformationen	180
3.1.4 Infizierte Systeme suchen	184
3.1.5 Suchmaschinen.....	187
3.1.6 Testhindernisse suchen.....	197

3.1.7 Internetpräsenz untersuchen.....	201
3.2 Unveröffentlichte Informationen sammeln	208
3.2.1 Gesprächsführung	210
3.2.2 Rollen	214
3.2.3 Gesprächspartner einschätzen.....	216
3.2.4 Beeinflussung.....	224
3.2.5 Wahrnehmungsänderung.....	226

Kapitel 4: Dienste abtasten..... 229

4.1 Netzwerkverbindungen	229
4.1.1 Transport-Protokolle	231
4.1.2 TCP-Flags	235
4.1.3 Portscanner.....	236
Nmap.....	236
Unicornscan	241
Scanner-Hilfsmodule.....	243
4.1.4 IP-Adresse verbergen.....	244
4.2 Offene Ports untersuchen.....	246
4.2.1 FTP, Port 21.....	247
Versionserkennung.....	247
Anonymer Zugang.....	247
Bruteforce-Angriff.....	248
Zugangsdaten mitlesen.....	249
Konfigurationsdateien	249
4.2.2 SSH, Port 22.....	249
Versionserkennung.....	250
Bruteforce-Angriff.....	250
Zugangsdaten mitlesen.....	251
Konfigurationsdateien	253
4.2.3 Telnet, Port 23	253
Bruteforce-Angriff.....	254
Zugangsdaten mitlesen.....	254
Konfigurationsdateien	254
4.2.4 SMTP, Port 25	254
Versionserkennung.....	255
Benutzernamen raten	255
Bruteforce-Angriff auf Zugangsdaten	256

Gefälschte E-Mails versenden	257
Konfigurationsdateien	258
4.2.5 DNS, Port 53.....	259
Versionserkennung.....	259
IP-Adressen abfragen	260
Domain-Informationen abfragen	261
Konfigurationsdateien	265
4.2.6 TFTP, Port 69	266
4.2.7 Finger, Port 79.....	266
Befehlsausführung.....	266
Abfragen über mehrere Systeme hinweg	267
4.2.8 HTTP, Ports 80, 8080, 443.....	267
Versionserkennung.....	268
Funktionsprüfung.....	269
Schutzmaßnahmen suchen	271
Verzeichnisse suchen.....	272
Content-Management-Systeme prüfen.....	273
Informationsgewinnung.....	275
Zugangsgeschützte Bereiche angreifen	276
Datenverkehr untersuchen.....	279
Java-Applets analysieren	283
Web-Backdoor einschleusen.....	285
Schwachstellen auf statischen Webseiten suchen.....	290
Schwachstellen in Webanwendungen suchen	291
Schwachstellen ausnutzen	293
Web-Datenbanken angreifen.....	297
Konfigurationsdateien	309
4.2.9 RPC (Remote Procedure Call), Port 111.....	310
4.2.10 NTP, Port 123.....	310
4.2.11 NetBIOS/NetBEUI/CIFS (Samba), Ports 135 bis 139, 445.....	312
Versionserkennung.....	312
Informationsgewinnung.....	313
Bruteforce-Angriff	314
Windows-Verbindungsdaten mitlesen	315
Samba-Verkehr umleiten	319
Code-Ausführung	321
Konfigurationsdateien	323
4.2.12 SNMP, Port 161.....	323
Bruteforce-Angriff	323
Zugangsdaten mitlesen.....	325

Informationen auslesen	325
Systemwerte ändern.....	326
Konfigurationsdateien	327
4.2.13 LDAP, Port 389	327
4.2.14 VPN, Port 500	329
IPSec-VPN	330
SSL-VPN.....	336
4.2.15 MS-SQL Server, Port 1433 und 1434	337
Versionserkennung.....	337
Bruteforce-Angriff.....	338
4.2.16 Citrix-ICA-Server, Port 1494, 80, 443	340
Citrix-Mainframes suchen	341
Informationsgewinnung.....	341
Bruteforce-Angriff.....	342
Klassisches Hacken	342
4.2.17 Oracle, Port 1521.....	351
Bruteforce-Angriff.....	352
Zugangsdaten mitlesen.....	353
Backtrack-Tools	354
4.2.18 NFS, Port 2049.....	354
Freigaben anzeigen	354
NFS-Freigabe einbinden.....	355
NFS-Dateirechte umgehen.....	355
Zugriff auf NFS-Shares	356
Konfigurationsdateien	357
4.2.19 MySQL, Port 3306.....	358
Versionserkennung.....	358
Bruteforce-Angriff.....	359
Zugangsdaten mitlesen.....	359
SQL-Abfragen	360
Abfragen automatisieren	365
Konfigurationsdateien	367
4.2.20 RDP, Port 3389.....	368
4.2.21 Sybase, Port 5000.....	369
4.2.22 SIP, Port 5060	369
Fingerprinting.....	371
Telefongeräte suchen.....	375
Gespräche mitschneiden	375
Bruteforce-Angriff.....	376
Authentisierungsdaten mitlesen	377

Telefonsystem abstürzen lassen	378
Konfigurationsdateien	379
4.2.23 PostgreSQL, Port 5432.....	379
Versionserkennung.....	380
Bruteforce-Angriff.....	380
Datenbankserver abfragen	380
Dateien auslesen.....	381
4.2.24 VNC, Port 5900.....	382
VNC-Server mit Authentifizierung.....	382
VNC-Server ohne Authentifizierung.....	383
Konfigurationsdateien	383
4.2.25 X11, Port 6000	383
Offene X11-Systeme suchen.....	384
Bildschirm abfangen	385
Tastatureingaben abfangen	385
Konfigurationsdateien	386
4.2.26 JetDirect, Port 9100.....	386
4.2.27 Unbekannter Port und Dienst.....	387
Bannerabfrage	387
Prüfung auf HTTP	388
Kommunikation über SSL.....	388
Identifizierte Dienste	390

Kapitel 5: Systeme angreifen und kontrollieren..... 393

5.1 Schwachstellen ausnutzen	393
5.1.1 Exploit suchen	394
Exploit-DB.....	395
OSVDB	397
CVE.....	400
Packet Storm	402
Metasploit Framework	404
5.2 Direkter Systemzugriff.....	405
5.2.1 Klartextpasswörter suchen.....	406
5.2.2 Windows-System booten	406
5.2.3 Linux-System booten	409
5.2.4 Universelle Boot-CD.....	410
5.3 Systemkontrolle.....	412

5.3.1 Systemzugang	412
Backdoor einschleusen	414
Gegenstelle einrichten	422
Persistente Backdoor	423
Backdoor schützen.....	423
5.3.2 Informationsgewinnung	429
Systeminformationen.....	430
Windows-Registry	432
Virtualisierung prüfen.....	437
5.3.3 Netzwerkprüfung	438
Netzwerke auslesen.....	438
DNS-Auflösung manipulieren.....	438
Datenverkehr mitlesen	439
Zielsystem als Gateway.....	441
5.3.4 Datenabfluß	443
Daten vom Zielsystem laden	443
Tastatureingaben abfangen	444
5.3.5 Rechteausweitung.....	444
Benutzerrechte übernehmen.....	444
Passworthashes auslesen.....	446
Passworthashes knacken.....	447
5.3.6 Zugangsausweitung.....	448
Windows-Fernverbindungen.....	448
Telnet-Server.....	450
5.3.7 Spurenbeseitigung.....	450
Zeitstempel manipulieren	450
Systemlogs leeren.....	452

Kapitel 6: Angriffe auf gehärtete Umgebungen..... 455

6.1 Drahtlose Verbindungen.....	455
6.1.1 WLAN-Zugangsdaten.....	457
Unverschlüsseltes WLAN	457
WEP-Verschlüsselung.....	459
WPA/WPA2-Verschlüsselung.....	460
WPA Enterprise.....	461
WPS-Verschlüsselung	464
Denial of Service	466

Mobile WLAN-Clients	467
6.1.2 WLAN-Datenverkehr mitlesen	470
Zugangspunkt fälschen	470
Datenverkehr umleiten	473
6.1.3 DECT-Telefonate	475
6.2 Firewalls	480
6.2.1 Architektur	480
6.2.2 Schwächen ausnutzen	483
RATTE-Server	484
RATTE-Client	486
RATTE verteilen	488
RATTE ausführen	490
6.3 Netzwerkgeräte	494
6.3.1 Router	494
6.3.2 Netzwerkkontroll-Systeme	495
6.4 Kiosk- und Terminalsysteme	498
6.5 Online-Banking	499
6.5.1 Sitzungsdaten abfangen	501
6.5.2 Signaturstick angreifen	505
Browser	506
Update	506
Verbindung	507
6.5.3 Eigener Signaturstick	508
6.6 Client-Systeme	509
6.6.1 Eigener Exploit-Stick	509
6.6.2 USB-Angriffsgerät	515
6.6.3 Präparierte Webseite	520
SET konfigurieren	521
Payload auswählen	522
6.7 Anwendungen und Systeme	526
6.7.1 Office-Dokumente	526
Dokument bauen	527
Dokument verteilen	533
6.7.2 Browser	533
Ungezielte Browser-Exploits	533
Gezielte Browser-Exploits	535
Präparierte Webseiten	537
Phishing	542
Kombinierter Angriff	546
6.7.3 Truecrypt-Festplattenverschlüsselung	548

6.7.4 E-Mails	553
6.7.5 IBM i5.....	556
6.7.6 Domänen-Controller	559
6.8 SAP ERP.....	567
6.8.1 SAP-Server.....	569
SAP-Server identifizieren.....	569
Passwort-Angriffe	572
Rootshell	583
Schwachstellenprüfung.....	587
ABAP-Programme manipulieren.....	604
Backdoor einschleusen	606
6.8.2 SAP-Clients.....	608

Anhang A: Berechnung der operativen Sicherheit 611

A.1 Einleitungsphase.....	611
A.2 Interaktionsphase	616
A.3 Dokumentation	645

Anhang B: Quelltexte.....Seite 653

B.1 RATTE.....	653
B.2 Java-Applet (The Thomas Werth Java Attack).....	658

Anhang C: Metasploit-Module 661

C.1 Auxiliary.....	661
C.2 Encoders.....	669
C.3 Exploits.....	670
C.4 Nops.....	687
C.5 Payloads.....	687
C.6 Post	692

Stichwortverzeichnis..... 695

LITERATUR

JÖRG BRAUN: Das VirtualBox-Buch. Hosts und Gäste. C&L Verlag 2012. 450 Seiten, ISBN 978-3936546-71-2

JÜRGEN DANKOWEIT (Hrsg.): FreeBSD. Installieren, Konfigurieren, Vernetzen. C&L Verlag 2009. 751 Seiten, ISBN 978-3936546-41-5.

RED. FREEX (Hrsg.): Linux im Netz. Dienste auf Server, Desktop, Notebook. C&L Verlag 2006. 864 Seiten, ISBN 978-3936546-34-7

DR. ROLF FREITAG: Die Kunst des Verdeckens. Daten verschleiern, verschlüsseln, zerstören. C&L Verlag 2011. 366 Seiten, ISBN 978-3936546-65-1

DR. MATTHIAS LEU: Check Point NGX. Das Standardwerk für FireWall-1/VPN-1. C&L Verlag 2007, 1292 Seiten, ISBN 978-3936546-37-8

ROSA RIEBL: Mozilla. Firefox, Thunderbird, SeaMonkey. C&L Verlag 2010. 446 Seiten, ISBN 978-3936546-52-1

MARC RUEF: Die Kunst des Penetration Testing. Handbuch für professionelle Hacker. C&L Verlag 2007. 911 Seiten, ISBN 978-3936546-49-1

FABIAN THORNS (Hrsg.): Das Virtualisierungs-Buch. Konzepte, Techniken und Lösungen. 2. aktual. Aufl., C&L Verlag 2008, 799 Seiten, ISBN 978-3936546-56-9
(im Verlag vergriffen)

THOMAS WERTH: Die Kunst der digitalen Verteidigung. Sicherheitsstrategien, Software-Diagnosen, Forensische Analysen. C&L Verlag 2009. 607 Seiten, ISBN 978-3936546-59-0

GELEITWORT

Die Informationssicherheit und ihre Überprüfung war schon immer eminent wichtig, die Form der Informationen spielte dabei eigentlich noch nie eine Rolle. Egal, ob sie vor ein paar Jahrzehnten nur auf Papier geschrieben waren oder heute überwiegend auf einem digitalen Datenträger gespeichert sind – schützenswerte Daten wurden schon immer unzugänglich aufbewahrt und die Wirksamkeit des Schutzes wurde schon immer regelmäßig und umfassend kontrolliert.

Wirklich verändert hat sich in den letzten Jahren die Bedrohungslage, der sich Unternehmen ausgesetzt sehen. Während einst noch Daten von Servern illegal kopiert wurden, um daraus einen wirtschaftlichen Vorteil zu erhalten, so wird damit heute massiver und vor allem öffentlicher umgegangen. Kundenlisten tauchen im Internet auf, Server werden kompromittiert und ganzen Internetseiten werden für Stunden lahmgelegt. Die Folgen solcher Angriffe können enorm sein, sie reichen vom gerade noch verschmerzbaeren Imageschaden bis hin zum Verlust der Existenzgrundlage.

Eine wirkungsvolle Strategie für die Datensicherheit von Unternehmen muß deshalb aus mehreren Komponenten bestehen, Compliance, Risikomanagement, Informationssicherheit, Krisenmanagement, Know-how-Schutz, Zutrittskontrolle, Awareness und Datenschutz sind unabdingbar. Sind diese Punkte alle gemäß den internen Richtlinien vollständig oder zumindest in Teilbereichen umgesetzt, kommt der Teil der Sicherheitsstrategie, der von vielen Unternehmen vergessen oder verdrängt wird: die professionelle Überprüfung der vorhandenen Sicherheit von Daten, Informationen und Netzwerken. Gegen Fehler ist selbst der gewissenhafteste und erfahrenste Administrator nicht gefeit; ihm kann bei der Konfiguration einer Firewall und ihrer Integration in das Netzwerk ein kleiner Fehler unterlaufen, der sich auf die Sicherheit des gesamten Unternehmens auswirkt. Damit er nicht auf Dauer unbemerkt bleibt und unabsehbare Folgen nach sich ziehen kann, müssen die Systeme regelmäßig überprüft werden.

In den Medien werden Angreifer oft als frühreife Jugendliche gezeigt, die Skimasken tragen, neben der Tastatur die Chipstüte liegen haben und die gewonnenen Daten illegal weiterveräußern oder veröffentlichen. Ja, natürlich gibt es die, aber es gibt auch die professionellen Angreifer, die Auftragsarbeiten durchführen. Oder die Geheimdienste, die im Interesse der

eigenen Wirtschaft Unternehmen anderer Länder ausspionieren. Technisch versierte Angreifer können von außen und von innen kommen und sind oft sehr gut geschützt gegen Verfolgung, weil sie es verstehen, ihre Spuren zu verwischen. Von diversen, im Internet dokumentierten Angriffen und den Warnungen der Landesämter für Verfassungsschutz wissen wir, daß insbesondere das Know-how deutscher Unternehmen gern zum Ziel von Angreifern wird. Viele dieser Angriffe werden leider zu spät entdeckt, nämlich erst dann, wenn der Schaden schon eingetreten ist. Allerdings darf nicht vergessen werden, daß die Folgen nicht nur für das betroffene Unternehmen gravierend sein können, sondern die Angriffe auf die deutschen Wirtschaftsunternehmen und der resultierende Abfluß von Know-how zur Schwächung der Gesamtwirtschaft beitragen.

Mir ist natürlich klar, daß es den Unternehmern häufig nicht leicht fällt, zwischen Produktivität und ihrem Schutz den richtigen Mittelweg zu finden. Aber diese beiden Punkte müssen ineinander greifen und gegenseitig voneinander profitieren! Weil die aktive Unterstützung der Informationssicherheit nun mal einer der Grundpfeiler der Wirtschaftsleistung ist, muß sie ihren festen Platz in der Unternehmenskultur haben.

Um sein eigenes Unternehmen auf der Informations- und Datenebene zu schützen und diesen Schutz zu überprüfen, muß man so vorgehen, arbeiten und denken wie ein professioneller Angreifer. Der Autor dieses Buches gibt Ihnen als Leser das Werkzeug an die Hand, um genau das tun zu können: Das Netzwerk und die Datensicherheit des Unternehmens so zu überprüfen, wie ein Angreifer versuchen würde, in ein Unternehmen einzudringen.

Professionelle Angriffe auf Unternehmen sind gut organisiert und wohlgedacht. Sie sind glücklicherweise nicht immer von Erfolg gekrönt, aber leider noch immer ausreichend oft. Die Unternehmer und die Administratoren müssen sich deshalb Gedanken darüber machen, wie sie die Sicherheit des Unternehmens und damit die Unternehmenswerte erhalten können. Sie kann maßgeblich davon abhängen, wie sicher die Infrastruktur für die Daten ist und wie leicht ein Angreifer sich Zugriff verschaffen kann, ohne dabei bemerkt zu werden. Die technischen Aspekte von Sicherheitsüberprüfungen sowie die konzeptionellen Ansätze für eine professionelle Vorgehensweise finden sich in diesem Werk wieder. Der Leser bekommt eine vollständige Übersicht darüber, wie Dienste und Programme angegriffen werden und hat die Möglichkeit, die Vorgehensweisen selbst im Unternehmen zum eigenen Schutz zu testen. Die unterschiedlichen Angriffsmethoden auf Unternehmensnetzwerke werden ebenso ausführlich vorgestellt wie die benötigten Hilfsmittel und Werkzeuge. Weil die Komplexität von Angriffen gestiegen ist, ist auch die Komplexität von professionellen Sicherheitsüberprüfungen gestiegen. Sie und die enormen Anforderungen kann der Leser nach der Lektüre dieses Werks meistern und seinem Unternehmen zu einem hohen Maß an Sicherheit verhelfen.

Marko Rogge, IT-Sicherheitsberater und IT-Forensiker

**Es gibt Momente im Leben, die auch in der Wiederholung nichts
von ihrem Zauber verlieren.**

— Tom —

Liebe Leser,

eine hundertprozentige Systemsicherheit kann es nur dann geben, wenn der Computer nicht mit einem Netzwerk verbunden ist und keine Laufwerke besitzt, über die Schadsoftware auf ihn gelangen kann. Dies wird aber in einem Unternehmen niemals der Fall sein, dort kommunizieren die Arbeitsplatz-PCs mit den Dateiservern, Finanz- und Buchhaltungsdaten müssen an die DATEV und die Staatskassen übertragen werden, die Kunden und Lieferanten können ihre Bestellungen und Bestände über einen HTTP-Zugriff aufgeben und einsehen und die Mitarbeiter möchten in ihrer Mittagspause im Internet surfen. Damit es nicht zu einem illegalen Datenabfluß kommen kann, besteht sogar eine gesetzliche Pflicht zur Sicherung der Computersysteme und Netzwerke. Nur: Wer weiß denn, wie sicher sie trotz aller Maßnahmen wie Authentifizierung, Firewalls, DMZ und Filter wirklich sind? Die tatsächliche Sicherheit kann nur dann festgestellt werden, wenn die Systeme einem Einbruch – Penetrations-Test – unterzogen werden, die Guten quasi schneller als die Bösen. Sind die Einbrüche erfolgreich und führen zu einem Datenabfluß, erfährt man automatisch, wo noch Sicherheitslücken vorliegen und wie sie geschlossen werden müssen. Penetrations-Tests sind also systematische Einbrüche in Computer und Netzwerke, um den Grad der vorhandenen Sicherheit zu überprüfen und zu bewerten. Der Leitgedanke der Systematik hat mich auch beim Schreiben dieses Buchs begleitet. Mein Ziel war ein generisches Nachschlagewerk, in dem alle Verfahren beschrieben sind, um ein bestimmtes Testziel zu erreichen. Weil es wenig sinnvoll ist, den Kompletteinbruch in eine Firma X zu beschreiben, habe ich die Tests in Angriffe auf einzelne Dienste, Programme und Netzwerke aufgedröselt. Dabei habe ich die Ziele jedes Angriffs einzeln aufgeschlüsselt und die verschiedenen Verfahren beschrieben, wie ein Penetrations-Tester Zugriff auf das jeweilige

System und seine Daten erlangt. Mit diesen Anleitungen ist man dann auch in der Lage, einen Angriff auszuführen, in dem mehrere Ziele kombiniert werden.

Ich richte mich bei den Tests nach der Methodik des Open Source Security Testing Methodology Manual (OSSTMM). Nach meinen Erfahrungen ist es das einzige Handbuch, das alle Bereiche von Penetrations-Tests abdeckt und würdige es im Buch entsprechend.

Als Arbeitsumgebung nutze ich die spezielle Linux-Distribution Backtrack und diverse Programme und Frameworks wie beispielsweise Metasploit. Wenn Sie ein anderes System bevorzugen, können Sie dies natürlich entsprechend erweitern, ich biete Ihnen alle Informationen dazu.

Zum Schluß möchte mich noch bedanken:

Zuerst meiner Frau Nadine für ihre Geduld und ihr Verständnis, insbesondere wenn ich mal wieder mehr mit dem Computer als mit ihr verheiratet war. Ich freue mich schon wieder auf die Zeit, wenn sie nicht mehr ohne mich den Kindern aus meinen herumliegenden Hacker-Büchern vorlesen muß. Womit ich auch meine zwei Kindern Maya und Tom dafür danke, daß sie mir jeden Tag ein Lächeln ins Gesicht zaubern. Ebenso danke ich meinen Eltern, Schwiegereltern und meiner großen Familie. Dabei möchte ich Jenny B. an dieser Stelle besonders hervorheben, die eine wunderbare Patentante ist. Ebenso verdient auch Sven K. eine besondere Erwähnung. Marko Rogge bin ich für die inzwischen mehrjährige Unterstützung mehr als dankbar und hoffe, daß dies in der Zukunft so bleiben wird. Auch meine lieben Freunde und Kollegen möchte ich nicht vergessen, ohne die das Leben doch um einiges ärmer wäre. Ebenso möchte ich Volker danken, weil er mich immer noch ohne zu zögern unterstützt, wenn ich mal Hilfe brauche. Vielen Dank auch an Steffi G., die sich als Fotomodell für die Bilder in Kapitel 3 zur Verfügung gestellt hat. Dank auch an meine Lektorin und Verlegerin Frau Riebl, die auf ihre gewohnt charmante Art das bestmögliche Werk aus einem Autor herauskitzelt.

Ihr

Thomas Werth

KAPITEL 1

DIE TESTORGANISATION

Ein Penetrations-Test ist ein auftragsgesteuerter Einbruch in die datenverarbeitenden Systeme eines Unternehmens, der zum Ziel hat, den Sicherheitszustand der Systeme festzustellen. Gelingt dem Tester der Einbruch und kann er Zugriff auf vertrauliche Informationen erlangen, beispielsweise in einer bestehenden Verbindung zwischen mehreren Computern Paßwörter mitschneiden, Daten aus Dateien oder Datenbanken auslesen oder ihren Informationsgehalt manipulieren, ist dies der Beweis, daß das System Sicherheitslücken hat. Der Auftraggeber muß sich dann darum kümmern, diese Sicherheitslücken zu schließen. Gelingt es dem Tester jedoch nicht, in die Systeme einzudringen, kann davon ausgegangen werden, daß die Systeme zu diesem Zeitpunkt als sicher erachtet werden können. »Zu diesem Zeitpunkt« deswegen, weil es durchaus der Fall sein kann, daß ein paar Tage nach dem erfolglosen Penetrations-Test eine generelle Sicherheitslücke in einem Programm oder in einer Verbindung entdeckt wird, auf deren Grundlage eine Angriffsmethode entwickelt wird, mit der ein Unbefugter in das System eindringen kann.

Die Methoden, wie in ein datenverarbeitendes System eingebrochen werden kann, sind nicht unbedingt nur technischer Natur. Natürlich gibt es etliche auf einen Einbruch spezialisierte Werkzeuge beziehungsweise können an sich harmlose Programme zweckentfremdet werden, um in eine Anlage einzudringen. Ein Einbruch kann aber nur dann gelingen, wenn der Penetrations-Tester vorher hinreichend Informationen über die Systeme besitzt. Dazu gehören die Namen von Computern und ihre Adressen, über die sie in einem Netzwerk erreichbar sind. Sowie die Art der auf den Computern angebotenen Programme und die Zugangsdaten, über die sich die Benutzer an den Systemen authentifizieren müssen. Diese Informationen müssen primär mit technischen Mitteln gesammelt werden, denn ein Programm kann nun mal schneller rechnen als sein Anwender und langweilt sich nicht beim schier endlosen Abarbeiten von Tabellen. Manchmal gelingt es aber einfach nicht, die wichtigen Informationen mit einem Computer zu ermitteln oder auf gut Glück ein System zu penetrieren. In solchen Fällen muß der Tester die Mitarbeiter, die an den Computern arbei-

ten, in seine Recherchen einbeziehen. Sie kennen ja mindestens die eigenen Zugangsdaten und das eine oder andere Detail zu den Systemen. Damit die Anwender einen Fremden – der der Penetrations-Tester ja ist – großzügig mit Informationen versorgen, muß er sich Mitteln bedienen, die eigentlich unterhalb einer moralischen Gürtellinie angesiedelt sind. Quasi als Nebeneffekt erforscht er dabei die Verschwiegenheit des Personals in einem Unternehmen. Schließlich macht der Penetrations-Tester nichts anderes als ein Unbefugter, der Geschäftsgeheimnisse erlangen möchte: Leute aushören und sie dazu bringen, in einer bestimmten Weise zu handeln.

1.1 DER AUFTRAG

Ein Penetrations-Test bedarf einer methodischen Vorgehensweise, schließlich geht es um die Feststellung des Sicherheitszustands eines ganzen Unternehmens. Würde hier unkoordiniert und unstrukturiert vorgegangen, wären die erzielten Ergebnisse zufällig, wären nicht nachvollziehbar und deswegen ungültig.

Nachfolgend werden die formalen Anforderungen an Penetrations-Tests vorgestellt.

1.1.1 Testtypen

Man könnte meinen, daß der einzige Sicherheitstest für ein Computersystem der Penetrations-Test ist. Dieser Begriff hat sich in den Medien durchgesetzt und scheint sich inzwischen als Oberbegriff für alle Sicherheitstests durchgesetzt zu haben. Es gibt aber mehrere Ausprägungen von Sicherheitsüberprüfungen.

Regelkonformität (Compliance Test)

Die Organisation eines Unternehmens bewegt sich nicht in einem rechtsfreien Raum. Vielmehr geben zahlreiche Gesetze und Vorschriften vor, wie Geschäftsvorfälle zu dokumentieren sind, was wie lange in einem Archiv gelagert werden muß und wie die datenverarbeitenden Systeme beschaffen sein müssen.

In erster Linie gibt das Handelsgesetz vor, daß die Computersysteme einbruchssicher sein müssen, so daß keine Betriebsgeheimnisse abfließen und in die Hände Unbefugter gelangen können, um Schaden von der Firma und der wirtschaftlichen Wettbewerbsfähigkeit des ganzen Staatsgebildes abzuwehren. Zur Konkretisierung dieser gesetzlichen Forderung wurden zahlreiche Standards und weitere Gesetze entwickelt, die bestimmte technische und organisatorische Maßnahmen vorschlagen. Allerdings steht es den Unternehmen frei, selbst interne Sicherheitsrichtlinien aufzustellen, die von den einzelnen Fachabteilungen eingehalten werden müssen. Natürlich müssen sich diese an den gesetzlichen Vorschriften orientieren.

Weil die Umsetzung von Normen und Standards mit viel Arbeit verbunden ist und zu Unbequemlichkeiten bei manchen Arbeitsabläufen führen kann, ist es mehr oder weniger gang und gäbe, daß sich im Laufe der Zeit Laxheiten bei ihrer Einhaltung einschleifen. Dies kann so weit führen, daß die Systeme unsicher werden und sogar gegen die geltenden Gesetze verstoßen wird.

Die Geschäftsleitung tut also gut daran, ab und zu nachzuforschen, ob im Tagesgeschäft die einstmals als bindend verabschiedeten Richtlinien auch wirklich (noch) angewandt werden. Eine Prüfung auf Einhaltung der Regeln heißt Compliance Test. Die Kriterien dieses Tests bilden die in einem bestimmten Prüfstandard festgelegten Anforderungen.

Wichtige interne und externe Standards sind:

- Individuelle Vorgaben des Auftraggebers. Hier muß normalerweise geprüft werden, ob interne Sicherheitsrichtlinien eingehalten werden (wie beispielsweise der Schutz von Betriebsgeheimnissen).
- IT-Sicherheitsstandards, so wie sie in den Normen ISO 27001 oder dem IT-Grundschutz festgeschrieben beziehungsweise vorgeschlagen sind. Die ISO-Norm 27001 beschreibt die Anforderungen an ein Informationssicherheits-Management-System. Das Handbuch zum IT-Grundschutz wurde vom deutschen Bundesamt für Sicherheit in der Informationstechnologie (BSI) zusammengestellt. Dieser Leitfaden, der keine bindende, sondern nur eine vorschlagende Funktion haben darf, hat das Ziel, die Sicherheit der IT-Strukturen anhand konkreter Maßnahmen zu erhöhen.
- Gesetzliche Vorgaben. Hier ist in erster Linie das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) zu nennen, das die Vorstände von Aktiengesellschaften und Gesellschaften mit beschränkter Haftung dazu verpflichtet, geeignete Maßnahmen zu treffen, um frühzeitig existenzgefährdende Entwicklungen zu erkennen. Dabei handelt es sich insbesondere um die Einführung von Überwachungssystemen, wozu auch das IT-Risikomanagement zählt. Ein anderes Gesetz ist EURO-SOX, eine EU-Richtlinie, die auf dem amerikanischen SOX-Gesetz aufbaut. Es verlangt die Einrichtung eines internen Kontrollsystems, das die Wirksamkeit von internen Kontrollen, Revisionen und des Risikomanagements überwacht.

In der Regel wird bei einem Compliance-Test das interne IT-Risikomanagement auf Funktionstüchtigkeit geprüft. Als Referenz dient dabei die jeweilige Norm oder das entsprechende Gesetz.

Bei allen Compliance-Prüfungen dokumentiert der Tester die Vorgehensweisen und die Arbeitsergebnisse. Zum Schluß vergleicht er die Vorgaben mit den tatsächlich im Unternehmen verwirklichten Maßnahmen und ermittelt daraus den Grad der Einhaltung der Vorgaben.

Möchte sich ein Unternehmen beispielsweise nach dem IT-Grundschutz zertifizieren lassen, muß ein zertifizierter BSI-Auditor kontrollieren, wie viele der Maßnahmen aus dem IT-Grundschutz umgesetzt wurden. Dazu vergleicht er die relevanten Maßnahmen aus den IT-Grundschutz-Katalogen mit der tatsächlichen Situation im Unternehmen. Am Ende der Prüfung wird das prozentuale Verhältnis der umgesetzten Maßnahmen zur Gesamtmenge der Maßnahmen gebildet. Beträgt das Ergebnis mindestens zweiundachtzig Prozent, gilt der Compliance-Test zum IT-Grundschutz als bestanden und es kann ein Zertifikat ausgestellt werden.

Schwachstellenprüfung (Vulnerability Assessment)

Sollen potentielle Schwachstellen in einem Netzwerk aufgespürt werden – bedingt beispielsweise durch unsichere Zugriffskonfigurationen, den Betrieb unsicherer Software und den Verzicht auf Verschlüsselung –, ist ein Vulnerability Assessment durchzuführen. Bei diesem Testtyp übernehmen automatische Schwachstellenscanner den Hauptteil der Arbeit. Der Tester selbst wendet keine Energie auf, um das Netzwerk eigenständig zu erforschen oder Zugangsdaten zu erlangen. Damit dennoch ein verwertbares Ergebnis erbracht werden kann, müssen die Werkzeuge mit bestimmten Daten gefüttert werden. Diese Daten müssen von der Geschäftsleitung beziehungsweise einer berechtigten Person erfragt werden:

- Komplette Zugangsdaten oder mindestens die Zugangsdaten eines Basisanwenders passend zur Tiefe des Tests, damit die Werkzeuge prüfen können, welche Möglichkeiten ein Angreifer aufgrund von Benutzerrechten hat.
- Zugriff auf Netzwerkdiagramme und -schemata, damit die Werkzeuge das gesamte Ziel erfassen können.
- Voller Zugriff auf Konfigurationsdateien und Skripte, damit die Werkzeuge auch die Konfigurationsdateien überprüfen können.

Bei einer Schwachstellenprüfung wird zuerst mit den üblichen Mitteln auf dem üblichen Weg im System ein neuer IT-Benutzer angelegt (beispielsweise mit den Bordmitteln des Betriebssystems und der nachfolgenden Eintragung in einen Samba-, LDAP- oder Active-Directory-Verzeichnisdienst). Dieser muß über die Benutzerrechte verfügen, die dem Prüfziel entsprechen. Dann wird der Test mit den Zugangsdaten dieses Benutzers ausgeführt. Hier wird mit einem Schwachstellenscanner (wie Nessus, OpenVAS oder Nexpose) gearbeitet, dem die Ziele und Zugangskennungen übergeben werden. Das Werkzeug prüft dann die Authentifizierung des Users und seine De-facto-Berechtigungen. Als Ergebnis der Prüfungen wird ausgegeben, wo es Sicherheitslücken vorgefunden wurden.

Nicht ungewöhnlich ist es, daß es dabei zu irritierenden Warnungen und Falschmeldungen kommt. Der Grund ist meist in der Version eines Dienstes zu suchen. Insbesondere die Prüfergebnisse von Webanwendungen müssen auf Plausibilität geprüft werden, da die meisten Scanner aus dem Tritt kommen und eine Schwachstelle des Webservers vermuten, wenn die Anwendung keine Standard-HTTP-Antworten wie die bekannte Fehlermeldung »404 Website not found« generiert, sondern beispielsweise eine eigene Fehlermeldungsseite ausgibt. Solche Falschmeldungen muß der Tester in der Schlußdokumentation manuell eliminieren.

Als Ergebnis wird dem Auftraggeber die Auflistung der Risiken und des resultierenden Schadenpotentials in Berichtsform übergeben. Um seine Erkenntnisse und Schlußfolgerungen zu untermauern, sollte der Tester als Anhang die Ausgabe des Schwachstellenscanners mitliefern, wobei die offensichtlichen Falschmeldungen vorher entfernt oder zumindest markiert werden müssen.

Penetrations-Test

Ein Penetrations-Test ist eine Prüfung der aktuellen Sicherheit eines Programms (beispielsweise die Prüfung einer neuen Version der Online-Banking-Software auf mögliche Angriffsflächen) oder Netzwerks (beispielsweise die Überprüfung eines neu installierten drahtlosen Netzwerks mit Anschluß an das LAN, um sicherzustellen, daß kein unberechtigter Zugriff möglich ist).

In einem Penetrations-Test wird eine Schwachstellenprüfung um manuelle Prüfungen und Angriffe erweitert. Bei dieser Testform wird der Ausführende zum tragenden Element und nicht sein Werkzeug, er simuliert den Angriff eines Einbrechers oder böswilligen Anwenders. Das erste Ziel eines Penetrations-Tests ist die Suche von Schwachstellen in Programmen und Netzwerkverbindungen. Werden welche gefunden, wird versucht, sie mit bestimmten Programmen auszunutzen und auf diesem Weg in das System einzudringen. Gelingt dies, dienen die gekaperten Systeme als Grundlage dafür, weiter in das Netzwerk vorzudringen und Zugangsdaten mitzuschneiden und vertrauliche Daten zu lesen.

Whitebox-Test

Eine Variante des Penetrations-Tests ist der Whitebox-Test. Hier erhält der Tester einen kompletten Zugriff auf die zu testenden Systeme, indem ihm vorab Detailinformationen zum Netzwerk und den zu testenden Systemen übergeben werden. Ein solcher Test ist recht schnell abgeschlossen, weil grob gesagt die Phase der Informationsgewinnung entfällt. Ein Whitebox-Test kann noch weiter dahingehend differenziert werden, ob das Ziel über den Angriff in Kenntnis gesetzt wird (Tandem Test) oder nicht (Reversal Test). Bei letzterem wird auch die Reaktion der Mitarbeiter beziehungsweise der Systeme auf den Angriff geprüft.

Blackbox-Test

Das Gegenstück zum Whitebox- ist der Blackbox-Test. Bei einem solchen erhält der Tester keine ausführlichen Informationen über das Testziel. Ihm wird lediglich der Name des Unternehmens, der Name einer Domain oder eine beliebige IP-Adresse genannt. Er muß dann versuchen, alle relevanten Daten über das zu testende Objekt selbst zu ermitteln, um dabei Schwachstellen zu finden. Auch bei diesem Testtyp kann unterschieden werden, ob das Ziel über den Angriff informiert ist (Blind Test) oder nichts vom bevorstehenden Test weiß (Double Blind Test).

Der Ablauf eines Blackbox-Tests entspricht dem eines Whitebox-Tests. Weil der Tester sein Ziel noch nicht kennt, muß er zuerst öffentlich verfügbare Informationen zur Zielfirma einholen. Bevorzugter Anlaufpunkt dafür ist die Homepage des Auftraggebers. Aus ihr kann er unter Umständen wichtige Informationen für einen Einbruch gewinnen.

Graybox-Test

Zwischen den White- und Blackbox-Tests ist der Graybox-Test angesiedelt. Als Ausgangspunkt für den Test der Systemsicherheit erhält der Tester denselben Zugriff auf das interne

Netzwerk wie ein Mitarbeiter ohne alle Details des Netzwerks zu kennen. Er muß alle relevanten Daten über das zu testende Objekt selbst herausfinden. Hier besteht ebenfalls wieder die Option das Ziel über den Test, den Zielbereich und den Zeitrahmen zu informieren (Graybox Test) oder nicht (Double Graybox Test).

Der Ablauf eines Graybox-Tests entspricht dem eines Blackbox-Tests, jedoch mit dem Unterschied, daß der Tester soweit über das Ziel in Kenntnis gesetzt wurde wie auch ein interner Mitarbeiter mit normalen Benutzerrechten das Ziel kennt und über entsprechende Zugangsberechtigungen verfügt.

In seinem Abschlußbericht dokumentiert der Penetrations-Tester seine Vorgehensweisen und die Ergebnisse. Um seine Ergebnisse zu untermauern, muß er dem Auftraggeber eine Übersicht über die Tests zusammenstellen, in der die Zielsysteme, der Zeitrahmen sowie die Werkzeuge und Techniken genau aufgeführt werden. Neben den Testergebnissen muß er auch die daraus resultierenden Gefährdungen präsentieren.

1.1.2 Methodik

Werden in Computersystemen Sicherheitslücken gefunden, läßt sich anhand ihrer Menge und ihrer Auswirkung eine theoretische Aussage über das Sicherheitsniveau der getesteten Systeme zum Zeitpunkt der Prüfung treffen. Allerdings hängt das Auffinden von vorhandenen Sicherheitslücken stark vom Vorgehen und Können des Testers ab. Ein Tester, der kein Know-how zu Unix-Systemen hat, wird sich schwertun, solche Systeme erfolgreich zu prüfen. Seine Ergebnisse werden sicherlich von denen eines erfahrenen Unix-Testers abweichen. Es kann sogar passieren, daß eine bekannte Schwachstelle schlichtweg übersehen wird und er deswegen zu einem falschen Ergebnis kommt.

Erschwerend kommt hinzu, daß Testergebnisse nicht unwesentlich von der Vorgehensweise abhängen, in der die Systeme geprüft werden. Ein- und derselbe erfahrene Tester wird bei der mehrfachen Prüfung desselben Systems bei einer anderen Vorgehensweise zu unterschiedlichen Ergebnissen kommen.

Um solche inakzeptablen Unwägbarkeiten bei einem Penetrations-Test auszuschalten, müssen sich die Testreihen gemäß einer generelle Vorgehensweise durchgeführt werden, die garantiert, daß:

- Der Test gründlich durchgeführt wird.
- Der Test alle erforderlichen (Kommunikations-)Kanäle umfaßt.
- Der Test gesetzeskonform ist.
- Die Ergebnisse meßbar sind.
- Die Ergebnisse konsistent und wiederholbar sind.
- Der Test nur Schlußfolgerungen enthält, die aus dem Test selbst abgeleitet sind.

Das einzige Handbuch, das all diese Anforderungen abdeckt und das sich bei der Arbeit des Autors bewährt hat, ist das Open Source Security Testing Methodology Manual (OSSTMM). Sein Hauptziel ist die Erarbeitung einer wissenschaftlichen Methode zur genauen Bestimmung der tatsächlichen Sicherheit (in OSSTMM »operative Sicherheit«, kurz

OPSEC, genannt) mittels Untersuchung und Korrelation der Testergebnisse in einer konsistenten und zuverlässigen Weise. Das Handbuch wurde von der Isecom (<http://www.isecom.org/osstmm/>) entwickelt, diese bezeichnet sich selbst als offene, kooperative, Non-Profit-, Wissenschafts- und Sicherheits-Forschungsorganisation. Registriert ist sie in Spanien. Ihre Forschungsbemühungen sind nach eigenen Angaben ohne kommerziellen oder politischen Einfluß, ihr Ziel ist es, praktische Methoden und Messungen für Sicherheit und Integrität anzubieten, die vom Vorstandsmitglied bis zum Schüler verstanden werden. Zu diesem Zweck arbeitet Isecom mit Schulen, Universitäten, Unternehmen und Regierungsbehörden zusammen.

Das Handbuch bietet eine Methodik zur Durchführung von Sicherheitsanalysen (OSSTMM-Audits), um den Grad der die Sicherheit auf operativer Ebene genau messen zu können. Dabei werden subjektive Vermutungen oder Annahmen ausgeschaltet. Es gibt eine methodische Vorgehensweise vor, denn nur ein fester Testablauf kann automatisch wiederholbare und konsistente Ergebnisse liefern.

In Anhang A dieses Buchs ist der Ablauf eines OSSTMM-Audits an einem Beispiel vorgestellt, die einzelnen OSSTMM-Testphasen werden jeweils an einem externen und internen System gezeigt.

Im OSSTMM-Audit werden zuerst die ansprechbaren Systeme gesucht. Werden welche gefunden – in der Sprache des OSSTMM heißt ein gefundenes System *Visibility* –, werden sie in ein Formblatt eingetragen. Ebenso werden die im Test gefundenen Sicherheitslücken – als solche gelten nicht nur technische Verwundbarkeiten, sondern Informationspreisgaben durch Mitarbeiter –, in dem Blatt vermerkt. Zudem sind die bereits installierten Sicherheitsmaßnahmen in das Formelblatt aufzunehmen. Als Ergebnis liefert das Formular den Risk Assessment Value (RAV) des Testobjekts. Das ist eine Prozentzahl, die das vorgefundene Sicherheitsniveau in Relation zum nur in der Theorie erreichbaren Maximalwert von 100 Prozent ausdrückt. Die Höhe des Meßwerts ist die Grundlage für die Bewertung eines Systems als *sicher* beziehungsweise *unsicher*. Alle Schwächen bedeuten Abschläge von diesem Wert. Erst ein System ab einem RAV von 90 Prozent kann per definitionem als sicher eingestuft werden.

Der berechnete Meßwert läßt sich auch grafisch darstellen, Bild 1.1 zeigt ein Beispiel. In einer grafischen Aufbereitung kann das Sicherheitsniveau – vielleicht sogar im Lauf der Zeit – eingängig abgebildet werden. Um den Wert zu verdeutlichen, schadet es auch nicht, ihn in Relation zu beispielsweise früheren Testergebnissen oder Industriestandards zu setzen.

Weil die Gefährdungen (wie Sicherheitslücken und Informationsabflüsse) und die Sicherheitsmechanismen (wie Authentifizierung und Verschlüsselung) im Modell erfaßt werden, kann nicht nur die Sicherheit des Systems bewertet, sondern es kann auch mit anderen Systemen verglichen werden. Unterzieht man die Details der festgestellten Gefährdungen und Sicherheitsmechanismen einer genauen Analyse, kann festgestellt werden, wo Kontrollfunktionen nicht wie vorgesehen funktionieren oder wo Schwachstellen vorhanden sind.

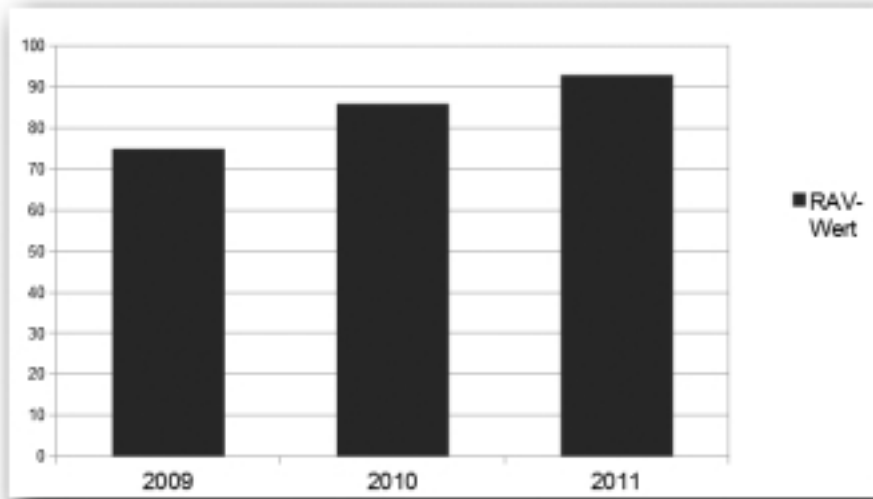


Bild 1.1: Die grafische Darstellung eines Risk Assessment Value (RAV)

Um eine möglichst hohe operative Sicherheit eines Systems zu erreichen, müssen die potentiellen Gefährdungen entweder vom operativen System getrennt werden – beispielsweise durch Trennung der Netzverbindung – oder kontrolliert werden, beispielsweise durch einen Zugangsschutz.

Sicherheitsfaktoren

Eine Sicherheit von vollen einhundert Prozent können nur solche Systeme erreichen, die vollständig von einem Netzwerk getrennt sind. Das können also ausschließlich Standalone-Computer sein, und die noch ohne Laufwerke, so daß über keinen Datenträger Schadcode in das System eindringen kann. Das wird in einem Unternehmen nie der Fall sein, jeder Arbeitsplatz-PC wird in irgend einer Form mit seiner Umwelt kommunizieren müssen.

Überall dort, wo ein System nicht komplett von einem Netzwerk getrennt ist, bestehen Interaktionsmöglichkeiten mit anderen Systemen. Jede mögliche Interaktion reduziert die Systemsicherheit automatisch unter hundert Prozent. Die Interaktionsmöglichkeiten werden im OSSTMM-Audit in drei Bereichen untersucht:

- Die Sichtbarkeit (Visibility). Als Visibility zählen die Systeme, die auf einen Ping oder einen ansprechbaren Dienst antworten. Diese müssen gezählt werden, die Anzahl muß notiert werden.
- Das Vorhandensein von Kommunikationspunkten (Access). Dies sind die ansprechbaren Dienste auf einem System. Auch ihre Anzahl wird notiert.
- Die Vertrauensbeziehungen zwischen Systemen (Trust). Darf beispielsweise der Webserver mit einem E-Shop automatisiert auf den Datenbankserver zugreifen, zählt dies als ein Trust. Die Anzahl der Trusts wird notiert.

Zum Schluß werden die einzelnen Posten zusammengezählt. Das Ergebnis ist die Summe der Interaktionsmöglichkeiten. Sie bezeichnet die Durchlässigkeit eines Systems (Porosity).

Kontrolle

Um die Auswirkung von Bedrohungen durch Interaktionsmöglichkeiten in Schach zu halten, sind in jedem Unternehmen bestimmte Kontrollmechanismen installiert, die in interaktive und defensive Mechanismen unterschieden werden.

Interaktive Kontrollmechanismen haben direkten Einfluß auf die drei Eckpfeiler der operativen Sicherheit Visibility, Access und Trust und werden der **Klasse A** zugeordnet.

In diese Klasse gehören:

- Die **Authentifizierung**: Ein Benutzer wird anhand von Zugangsdaten identifiziert oder autorisiert.
- Die **Absicherung**: Das ist eine zusätzliche Schutzmaßnahme als Vereinbarung in Form einer Warnmeldung oder Lizenz zwischen dem Systembesitzer und dem interaktiven Teilnehmer oder eine Versicherung gegen Computerschäden.
- Die **Vorgaben**: Sie bestimmen verbindlich, wie interagiert werden soll, wobei der Kommunikationspartner keine Möglichkeit hat, die Art der Interaktion zu wählen, weil sie erzwungen wird, beispielsweise eine verschlüsselte Verbindung.
- Die **Kontinuität**: Auch im Falle eines Ausfalls oder Fehlers bleiben alle Dienste verfügbar.
- Die **Widerstandsfähigkeit**: Im Falle eines Ausfalls oder Fehlers funktionieren die anderen Sicherheitsvorkehrungen weiterhin und fallen nicht aus; beispielsweise wenn eine Blockall-Funktionalität in einer Firewall nicht davon betroffen ist, wenn es auf der Firewall zu Fehlern kommt.

Defensive Kontrollmechanismen werden in der **Klasse B** abgebildet. Sie beeinflussen nicht direkt die Interaktionen, sondern stellen Schutzmaßnahmen im Fall einer Gefährdung dar.

Zu ihnen zählen:

- Die **Unabstreitbarkeit**: Die Teilnehmer einer Interaktion werden eindeutig identifiziert und protokolliert, beispielsweise durch Logging oder Monitoring. Das Ziel ist, daß niemand die Teilnahme an der Interaktion leugnen kann.
- Die **Vertraulichkeit**: Sie garantiert die Vertraulichkeit der übermittelten Daten einer Interaktion, beispielsweise eine Verschlüsselung über SSH oder SSL.
- Die **Geheimhaltung**: Nur die beteiligten Personen wissen, wo der Informationsaustausch stattfindet; Beispiele sind Port-Knocking oder das Betreiben von Diensten abseits der Standardports.
- Die **Integrität**: Die Kommunikationspartner werden informiert, falls sich Daten während des Austauschs geändert haben; üblicherweise wird die Integrität durch Verschlüsselung oder Prüfsummen sichergestellt.
- Der **Alarm**: Er meldet eine (anhaltende) Interaktion.

Sicherheitslücken

Werden in einem System Sicherheitslücken gefunden, haben diese unterschiedliche Auswirkungen. Ihre möglichen Folgen auf die Sicherheit müssen im Rahmen des OSSTMM-Audits bewertet werden. Darin werden fünf Varianten von Sicherheitslücken unterschieden:

- **Kritische Lücken (Vulnerability)** können folgende Auswirkungen haben:
 - (a) Sie blockieren auch autorisierten Personen oder Prozessen den Zugang zu einem System,
 - (b) sie erlauben auch unautorisierten Personen oder Prozessen privilegierten Zugriff und/oder
 - (c) unautorisierte Personen oder Prozesse können die eigenen Aktivitäten verschleiern.
- **Schwachstellen (Weakness)** vermindern die Wirksamkeit eines Kontrollmechanismus der Klasse A oder heben ihn sogar auf.
- **Bedenken (Concern)** vermindern die Wirksamkeit eines Kontrollmechanismus der Klasse B oder heben ihn sogar auf.
- **Informationspreisgabe (Exposure)** macht Ziele direkt oder indirekt sichtbar. Dazu zählt beispielsweise die Anzeige von Versionsnummern von Diensten.
- **Anomalie (Anomaly)** ist ein unidentifiziertes oder unbekanntes Problem, das nicht kontrolliert und im normalen Betrieb berücksichtigt werden kann.

Category		OPSEC	Limitations
Operations		Visibility	Exposure
		Access	Vulnerability
		Trust	
Controls	Class A	Authentication	Weakness
		Indemnification	
		Resilience	
		Subjugation	
		Continuity	
	Class B	Non-Repudiation	Concern
		Confidentiality	
		Privacy	
		Integrity	
		Alarm	
			Anomalies

Bild 1.2: Die Einordnung einer Schwachstellen in eine Kategorie (Quelle: OSSTMM)

Die Sicherheitslücken werden fünf Kategorien zugeordnet:

- Ist die Sichtbarkeit (Visibility) betroffen, handelt es sich um eine Schwachstelle aus dem Bereich Informationspreisgabe (Exposure).
- Wirkt sich die Schwachstelle auf Kommunikationspunkte (Access) oder Vertrauensbeziehungen (Trust) aus, handelt es sich um eine kritische Lücke (Vulnerability).

- Sind die Kontrollmechanismen der Klasse A betroffen, wird von einer Schwachstelle (Weakness) gesprochen.
- Sind die Kontrollmechanismen der Klasse B beeinflusst, handelt es sich um ein Bedenken (Concern).
- Unklarheiten werden als Anomalie vermerkt.

Bild 1.2 stellt dar, nach welchen Gesichtspunkten eine im Test gefundene Schwachstelle einer der fünf genannten Kategorien zugeordnet wird. So würde beispielsweise ein Telnet-Zugang ohne Paßwortabfrage eine Schwachstelle im Bereich Kommunikation (Access) darstellen und ist als kritische Lücke (Vulnerability) zu werten.

1.1.3 Audit

Ein OSSTMM-Audit besteht aus mehreren Komponenten: der Planungsphase, der Ablaufphase und der Berechnung des Risikofaktors.

Planungsphase

In der Planungsphase ist zunächst zu definieren, welche Systeme einer Sicherheitsbestimmung zu unterziehen sind. Diese Systeme werden in einem OSSTMM-Audit *Assets* genannt. Die eigentlichen Ziele des Tests sind die Schutzmaßnahmen dieser Assets, denn letztlich entscheiden diese darüber, ob ein System sicher ist oder nicht.

Außer den Assets selbst müssen ihre Umgebung, ihre Schutzmechanismen und die umgebenden Prozesse betrachtet werden, weil diese mit den Assets interagieren. Sie bilden den Bereich, in dem die Zielsysteme miteinander kommunizieren.

Ebenso muß alles untersucht werden, was benötigt wird, um die Zielsysteme am Laufen zu halten. Dazu zählen neben der Infrastruktur auch Prozesse, Protokolle und Ressourcen. Sie bilden den Zielbereich (Scope) des Tests. In diesem arbeitet später der Tester.

Auch die Interaktionen innerhalb des Zielbereichs und zwischen dem Zielbereich mit der Außenwelt müssen analysiert werden. Diese Interaktionswege werden logisch in Richtungen unterteilt, beispielsweise von innen nach außen, von außen nach innen, Abteilung A zu Abteilung B und so weiter. Diese einzelnen Interaktionswege heißen Vektoren. Jeder Vektor muß eigens untersucht werden.

Dann müssen die Interaktionsmöglichkeiten jedes Vektors herausgefunden werden. Diese werden in fünf Kanäle und drei Klassen unterschieden:

In der Klasse der physikalischen Sicherheit sind die Kanäle Mensch und Gerät angesiedelt; in dieser Klasse geht es um die Täuschung von Anwendern und den Einbruch und Diebstahl von Systemen. Die Klasse der Spektrumsicherheit betrifft die drahtlosen Übertragung, es wird jede elektrische Kommunikation, Signalübertragung oder Ausstrahlungen in den elektromagnetischen Bereichen analysiert. Die Kommunikationssicherheit ist die dritte Klasse ab und umfaßt die Telekommunikation und Datenkommunikation, sprich: die Telefonie und Datenübertragung. Jeder in einem Vektor identifizierte Kanal muß einzeln getestet werden.

Abschließend muß das genaue Ziel des Tests festgelegt werden: Sollen nur die Interaktionsmöglichkeiten getestet werden oder auch die Reaktion der vorhandenen Sicherheitsmaßnahmen? Die Antwort auf diese Frage bestimmt den Testtyp. Dieser ist für jeden aus dem obigen Schema abgeleiteten Test individuell zu bestimmen.

Zu guter Letzt muß sichergestellt werden, daß der geplante Test mit den im OSSTM definierten Regeln (Rules of Engagement) konform ist. Diese geben ethische und organisatorische Hinweise zum OSSTM-Audit. Die Regeln sind sehr umfangreich, hier kann nur eine grobe Übersicht gegeben werden. So soll bei der Auftragsbeschaffung seriös um Kunden geworben werden. Angst machen oder öffentliche Hackervorfürungen sind untersagt. Aufträge dürfen nur mit schriftlicher Genehmigung des Ziels angenommen werden. Zudem dürfen offensichtlich unsichere Systeme gar nicht erst getestet werden. Bei der Vertragsgestaltung sind der Zielbereich und die Grenzen schriftlich zu fixieren, dem Auftraggeber muß ein Testplan vorgelegt werden. Auch zum Testvorgang selbst finden sich diverse Vorschriften wie die Einhaltung der Gesetze. Zum Schluß wird der Abschlußbericht unter die Lupe genommen, unter anderem wird vorgeschlagen, was er enthalten muß und wann die Privatsphäre von Personen zu berücksichtigen ist.

Ablauf

Ein OSSTM-Audit besteht aus mehreren Phasen.

Phase 1: Einleitungsphase

Die Einleitungsphase des Audits beginnt mit dem Definieren der Anforderungen, des Zielbereichs und der Testeinschränkungen. Zu berücksichtigen sind dabei die Firmenkultur und Vorgaben aus Normen, Gesetzen und Richtlinien. Damit die Messungen technisch nachvollziehbar sind, muß geprüft werden, welche Auswirkungen die Qualität der Netzverbindung und der räumliche Abstand zum Ziel auf die Testergebnisse hat beziehungsweise haben könnte. Als letztes wird getestet, ob technische Maßnahmen vorhanden sind, die auf den Versuch Interaktionen zu finden reagieren. Mit anderen Worten: Es werden die Einbruchserkennungs-Systeme identifiziert.

Phase 2: Interaktionsphase

In der Interaktionsphase werden die sichtbaren Ziele im Zielbereich ermittelt (Visibility Audit). Dann wird geprüft, welche Kommunikation mit den Zielen möglich ist (Access Verification). Zudem werden die Vertrauensbeziehungen zwischen den einzelnen Zielen ermittelt (Trust Verification) und die Kontrollmechanismen der Klasse B getestet (Control Verification).

Phase 3: Prüfungsphase

Die Ergebnisse der Prüfungsphase hängen stark von den Informationen ab, die der Tester vorab sammeln konnte beziehungsweise die ihm übergeben wurden. Zuerst wird geprüft,

STICHWORTVERZEICHNIS

4

4to6-Tunnel	169
7zip entpacken (Windows, Linux)	141

A

a.out	54
ABAP-Programme, Speicherort	605
ABAP-Stack	568
Absenderadresse e. Pakets modifiz.	233
Absenderadresse fälschen	257
ActiveX-Komponenten	608
Adreßinformationen fälschen	356
aircrack-ng, Module	80, 458
Alternativer Datenstrom, ADS	484
Android erweitern	147
androidVNC	150
Anfragen verstecken	236
Angriffe automatisieren	241
Angriffs-Webseite erzeugen	534
Anti-Abuse-Projekt	184
Antworten von welchem System?	198
Applet-Signatur	521
Application Level Gateways	481
Arduino	515
ARP-/IP-Spoofing	356
ARP-Pakete, Netzwerk fluten mit	72
ARP-Poisoning	316
ARP-Protokoll	133
ARP-Request-Replay-Angriff	459
ARP-Spoofing	69, 316, 356, 497
asn.shadowserver.org	183
Asset	31
Audit-Phasen	31
Authentifizierung	29
Authentifizierungscookie	279
Authentifizierungsserver	456
Autonomes System (Def.)	183
autopawn	241
Autorisierungstoken	501

B

Backdoor	412
— (Def.)	88
— aus RATTE bauen	486
— einschleusen	414
— in and. Prozeß schieben	426
— in Anwendung einbetten	425
— schützen	423
— suchen	190
— unabschaltbar machen	426
— verschlüsseln	102, 425
—, Angriffswege	517
—, lokale Firewall deaktivieren	428
—, persistente	415, 423
—, Rückverbindung	421

—, typische Portnummern	184
—, unsichtbare	425
—, Verbindung mit	94
—, Virenschutz abschalten	429
Backdoor-Gegenstelle	118, 422
Backslash maskieren	437
Backtrack	47, 139
— aktualisieren	170
— verschlüsseln	155
—, ARM-Release	146
—, Bildschirmauflösung	163
—, Dateisystem	145
—, deutsche Sprache/Tastatur	161f.
—, DHCP	164
—, Festplattenamen	146
—, Gnome-Version	141
—, grafische Oberfläche aufrufen	140
—, IPv6	168
—, KDE-Version	141
—, Live-CD	143
—, Nameserver hinzufügen	165
—, Netzwerkkonfiguration	164
—, root-Passwort	139
—, Router eintragen	165
—, VMWare-Image	141
—, Windows erhalten	145
—, WLAN-Konfiguration	166
—, Firewall ausschalten	496
—, Menü	153
—, Zugangsdaten	146
Banking-Sitzung abfangen	501
Bannerabfrage	387
Basket	85
BeEF-Module	542
Befehlseinschlebung, geeignete Parameter suchen	302
Befehlshell öffnen	121
Benutzerrechte übernehmen	444
Betriebssystem erraten	619
Betriebssystem-Kernel patchen	411
Bind Payload (Def.)	88
Bind-Shell	416
— erzeugen	542
Bind-Shell-Payload, ausführbares	416
Bizploit	587
—, Exploits	592
—, SAP-Connectoren	587
—, Shell-Anweisungen	598
—, Plugins	588
—, Test	25
Boot-CD	406, 410
Bootkey	560
Bootlaufwerk verschlüsseln	156
Bootloader	411
— ersetzen	548
— wiederherstellen	550
Bootmanager	146
Botnetz	184
Broadcast-Anfragen senden	239
Browser ersetzen	484

Browser überlasten.....	542
Browser übernehmen	537, 539
Browser, Befehle nachladen.....	540
Browser, Proxy eintragen.....	280
Browser-Exploits.....	93, 533
Browsersitzung, Kennung	503
Bruteforce-Angriff.....	61, 91, 239
— (Def.)	56
BSSID.....	80
BusyBox	140, 147

C

Cache-Poisoning-Angriffe	263
Cain and Abel.....	67
CD-Autostart, bössartiger	509
CentralOps.....	187, 195
Certificate Authority einschleusen	92
CIFS.....	312
Citrix.....	340
—, Default-Ports.....	340
—, Tastaturkürzel	343
Citrix-Mainframes suchen	341
Citrix-Server, Shell öffnen	342
Client-PC Schadcode unterschieben.....	526
Code-Injection	298
Compliance Test	22
Container	156
Content-Management-Systeme	273
Cookie.....	483
Cookies auswerten	278, 502
Credential-Harvester-Angriff	542
Cross-Site Scripting.....	299, 537
Crunch, Parameter.....	59
Curl	286
CVE.....	400
Cygin	47

D

Datei hochladen auf Opfer	121, 414
Dateidialoge aufrufen	343
Dateien mit Benutzernamen suchen	190
Dateien vom Ziel herunterladen.....	443
Dateien verschlüsseln.....	156
Dateisystem, Zugriff auf	132, 246
Datei-Uploads.....	190
Datei-Zeitangaben.....	451
Datei-Zeitstempel ändern	414
Datenbank hinter Webseite suchen.....	300
Datenbankabfragen, verschachtelte	302
Datenbankadministrator suchen	305
Datenbank-Benutzer ermitteln.....	361
Datenbanken anzeigen.....	362
Datenbankserver, Zugriff auf Dateisystem	308
Datenbank-Tabelle anzeigen	362
Datenbank-Tabelle auslesen	306f.
Datenbank-Tabelle, Struktur anzeigen	363
Datenverkehr im lok. Netzwerk mitlesen	72, 92, 439
Datenverkehr über Zielsystem leiten	441
Datenverkehr umleiten.....	72, 473
DB2.....	557
—, Systemtabellen.....	558
Deauthentication-Angriff.....	459
Debian-Schlüssel.....	632
DECT-Telefonie.....	475
Defaulttroute ändern	522
Denial-of-Service-Angriff (DoS).....	42
DHCP, IP-Adresse zuweisen.....	280
DHCP-Server konfigurieren.....	471

DHCP-Server, sich ausgeben als.....	71
Dienst (Def.)	229
—, Signatur.....	236
—, unbekannter	387
—, Verbinden mit	387
—, verschlüsselten identifizieren	389
—, Versionserkennung	236
Dienste, angebotene suchen	229, 619
Dienste, Authentifizierung abfragen	627
dig.....	186, 553
DNS, Versionserkennung	259
DNS-Antworten.....	198
DNS-Auflösung manipulieren	178, 438
DNS-Bind.....	643
DNS-Caching.....	186
DNS-Einträge abfragen.....	196, 261
DNS-Informationen fälschen.....	184, 259
DNS-Informationen suchen.....	195
DNS-Informationen über Domain	262
DNS-Konfigurationsdateien	265
DNS-Server zuweisen	471
DNS-Server, PTR-Eintrag.....	616
DNS-Server, Versionsinformationen.....	260
Dokument mit Backdoor	527
Dokumente lokal analysieren.....	207
Dokumente online analysieren.....	205
Dokument-Eigenschaften.....	205
Domain	180
— abfragen.....	187
— suchen.....	172
—, IP-Adressen abfragen.....	263
Domain-Informationen suchen	197
Domainname ermitteln	616
Domänen-Account angreifen.....	408
Domänen-Controller	559
Dork-Kategorien	189, 191
DoS-Skripte	240
Drei-Wege-Handshake	236
dsusers, Parameter.....	565
Durchlässigkeit e. Systems.....	29

E

Easus Partition Master	144
EBCDIC	556
Eingabeaufforderung erlangen	343ff.
Einwahlknoten anzeigen	204
Elicitation.....	210
E-Mail-Absender	255
— fälschen.....	553
E-Mailadresse, best. gespeichert?.....	255
E-Mail-Angriff.....	117
E-Mail-Austausch.....	254
E-Mail-Empfänger.....	255
E-Mails einer bestimmten Domain.....	553
E-Mails, gefälschte versenden (Spoofing).....	257
E-Mailserver ermitteln	553
E-Mail-Verzeichnisse suchen.....	190
Erreichbarkeit d. Ziels prüfen	197
ESSID.....	74
— verwalten	79
Ettercap	249
— konfigurieren	69
—, allgemeine Optionen.....	73
—, Anzeigeformat/-optionen.....	72
—, Log-Optionen	72
—, Parameter	73
—, Sniffing-/Angriffsoptionen	72
Eventlog löschen	414
Exploit.....	240, 394

STICHWORTVERZEICHNIS

— (Def.)	88
— suchen	394
exploit, Parameter	422
Exploit-Datenbanken/Exploit-DB	395
Exploit-Frameworks	87
Exploit-Stick, eigener	509
Exploit-Stick, HTTP-Server	510

F

FastFlux-Netzwerk	184
—, TTL	186
Festplatte partitionieren	143
finger, Befehle unterschieben	266
Fingerabdruck	236
finger-Abfragen umleiten	267
Firefox/Thunderbird, Zugangsdaten auslesen aus	92
Firewall ausschalten	321
Firewall überlisten	198
Firewall, ausgehender Verkehr	524
Firewall, IP-Adressen d. Benutzer	482
Firewall, Sicherheitslücke	483
Firewall-Backdoor	486
Firewalls suchen	197
Flash-Player, Exploit f.	536
Formatstrings	299
Fritz!Box	168
FTP	247
—, anonymer Zugang	93, 239, 247
—, Datenverkehr umleiten	249
—, Passwörter erraten	248
—, Versionserkennung	247
FTP-Anmeldung	93
FTP-Datenport	247
FTP-Konfigurationsdateien	249
FTP-Verwaltungsport	247

G

Gateway	441
—, Angreifer als	69
Geographische Suche n. PCs	191
Geräte m. Internetanschluß suchen	190
Geschlossener Port	237
—, Reaktion	229
Geschützter Port, Reaktion	231
getcountermeasure, Parameter	427
gettelnet	450
GNU-Dreisatz	53
Google	187
—, ODER-Suche	188
—, UND-Suche	188
Google-Dorks	189
— für SAP	570
Google-Suche, Operatoren	188
Grant-Tabelle	361
Graybox-Test	25
Grub	163
— reparieren	146

H

Handler (Def.)	88
Handler aufrufen	422
Handler f. Payload	514
handler-Modul	287
Handshake	74, 460
Hashverfahren	56
Hashwert	55
Hop (Def.)	197

host	186, 261
hosts-Datei ändern	259, 438
Hosts, virtuelle suchen	178
hostsedit, Parameter	438
.htaccess durchsuchen	277
.htaccess modifizieren	277
HTTP	267
—, Anfrage zurückverfolgen	270
—, Datei anfordern	270
—, Datei hochladen	270
—, Datei löschen	270
—, Dateien anbieten über	510
—, Dateihheader anfordern	270
—, Nutzdaten verstecken	483
—, Parameter f. Datenübermittlung	483
—, prüfen auf	388
—, Ressourcen-Anhang	270
—, Server-Optionen	270
—, Verbindung trennen	299
HTTP-Anfrage, Details ansehen	473
HTTP-Antworten	24
HTTP-Authentifizierung	291
HTTP-Befehle	270
HTTP-Optionen abfragen	621
HTTP-Protokollversionen	267
httpprint	268
—, neue Signaturen	269
HTTPS, Daten über HTTP nachladen	291
HTTPS-Verbindung, MitM-Angriff auf	507
HTTPS-Verbindung, Zertifikat	507
Hydra	61, 248
—, Parameter	60

I

i5, ASCII-Datenstrom konvertieren	557
i5, Datenbankzugriff	557
i5-Systeme, MitM	69
IANA	230
ICA-Sitzung	340
ICMP-Fehlermeldung	241
ICMP-Paket, Header	234
ICMP-Redirect-Pakete	71
Idle-Scan	236, 244
ifconfig	133, 281, 556
IKE	330
ike-scan, Parameter	335
Infizierte Systeme suchen	190, 240
Interaktionsmöglichkeiten (Def.)	28
Internet Explorer, Schwäche	542
Internet Explorer, Shellzugriff im	349
Internet-Telefonie, Sprachübertragung	369
Internet-Zugangspvder ermitteln	613
IP-Adresse der eigenen Netz Karte	522
IP-Adresse einer Domain	260
IP-Adresse gegen Blacklists prüfen	184
IP-Adresse in Namen auflösen	186
IP-Adresse lokalisieren	204
IP-Adresse zuweisen	471
IP-Adresse, andere annehmen	244
IP-Adresse, aus welchem Land	183
IP-Adresse, bösartige	184
IP-Adresse, eigene fälschen	244, 356
IP-Adresse, statische eintragen	164
IP-Adressen e. Domain, verschiedene	184
IP-ID überwachen	244
IPSec-VPN	330
IP-Spoofing	233, 356
IP-Tables bearbeiten	472
iptables-Regeln	69

IPv6 scannen.....	237
IPv6, Adressräume.....	134
IPv6, Datenverkehr umleiten.....	137
IPv6, Man-in-the-Middle-Angriff.....	136
IPv6-Netz, testen auf.....	133
IPv6-Router.....	168
IPv6-Tools.....	133
IT-Grundschutz.....	23

J

Java-Applet ausführen.....	542
Java-Applet dekompileieren.....	283, 508
Java-Applet einbetten.....	523
Java-Applet, On-the-Fly-Signierung einschalten.....	522
Java-Applet, Payload des.....	522
Java-Applet, Verschlüsselungsfunktionen.....	284
Java-Applet-Angriff.....	112, 520
Java-Applets.....	283
Java-Datenbanktreiber f. DB2.....	557
JavaScript in Webseite einschleusen.....	299, 538
JavaScript-Sitzung, Kennung der.....	503
JetDirect.....	386
John the Ripper, Parameter.....	63, 575
John, Betriebsmodi.....	62
John, Konfigurationsdatei.....	62
John, Passwörter einlesen/übergabe.....	65f.
John-Regeln.....	62
Joomla untersuchen.....	274

K

Kernelmodule, fremde.....	54
Keylogger aktivieren.....	92, 444
Kiosksystem.....	498
Klartextpasswörter suchen.....	406
Kommunikation, verschlüsselte.....	249, 388
Kon-Boot.....	410
Konsolenzugriff a. entf. Systeme.....	253

L

Lastverteilung.....	184
LDAP.....	327
—, Verschlüsselung.....	328
LDAP-Konfigurationsdateien.....	328
Link manipulieren.....	537
Linux, Anwenderrechte ändern.....	411
Linux, Passwort entfernen.....	409
Linux, Passwort ermitteln.....	410
Linux, Systemupdate.....	47
Linux-Kernel, Paketweiterleitung.....	73
Linux-Passwörter knacken.....	66
Linux-TTL.....	620
Listener (Def.).....	88
LM-Verschlüsselung.....	316f., 567
Load-Balancer.....	184
— suchen.....	197
Logdateien suchen.....	190
Loginsseiten suchen.....	190
Lücken, kritische.....	30

M

MAC-Adresse.....	70
— fälschen.....	497
— überschreiben.....	316
—, andere annehmen.....	465
MAC-Filter.....	457
Mail eXchanger Record.....	553

Mailserver.....	254
— akzeptiert gefälschte Absender.....	556
— für Domain ermitteln.....	197, 617
—, autorisierter.....	553
—, Name des.....	183
—, zuständigen finden.....	553
Mainframe.....	340
make-Tool.....	53
Makro in Dokument einbetten.....	529
Makro programmieren.....	527, 349
Maltego.....	172
—, Entities.....	173
—, Informationskategorien.....	172
Man-in-the-Middle-Angriff.....	55, 68, 249, 251, 254, 277
— verhindern.....	497
—, Einwegvariante.....	357
—, Optionen.....	72
Metadaten.....	205
Metagoofil.....	205
—, Parameter.....	275
Metasploit Community Edition.....	89, 404
Metasploit, Auxiliary-Module.....	91, 93
Metasploit, Backdoor schreiben.....	287
Metasploit, Datenverkehr routen.....	95
Metasploit, Encoder-Module.....	91
Metasploit, Exploit-Modul konfigurieren.....	90, 109
Metasploit, Kommandozeilenschnittstelle.....	104
Metasploit, Konsole beenden.....	95
Metasploit, Modul (Def.).....	90
Metasploit, Modul ausführen.....	110
Metasploit, Modul konfigurieren.....	108
Metasploit, Modul laden/entladen.....	108
Metasploit, Module anzeigen.....	95, 106
Metasploit, Module-Kategorien.....	91
Metasploit, Payload-Module.....	91
Metasploit, Plugin laden/entladen.....	95
Metasploit, Plugins.....	92, 111
Metasploit, Post-Module.....	92
Metasploit, Programme.....	92
Metasploit, Shell-Sitzung, Befehle.....	96
Metasploit, Sitzungen verwalten.....	95
Metasploit, Such-Optionen.....	404
Metasploit, Telnet-Verbindung.....	95
Metasploit, Verbindung m. Backdoor.....	94
Metasploitable-Image.....	611
Metasploit-Datenbank.....	90, 97, 295, 241
Metasploit-Konsole, Befehle.....	93, 95
Metasploit-Scanner suchen.....	243
Metasploit-Skripte.....	96
Meterpreter.....	91
Meterpreter (Def.).....	413
Meterpreter-Anweisungen.....	415
Meterpreter-Backdoor.....	414
Meterpreter-Backdoor automatisieren.....	426
Meterpreter-Backdoor, persistente.....	92
Meterpreter-Payload definieren.....	415
Meterpreter-Post-Module.....	414
Meterpreter-Sitzung beenden.....	414
Meterpreter-Sitzung in Hintergrund senden.....	414, 441
Meterpreter-Sitzung, and. Prozeß.....	414
Meterpreter-Sitzung, Datei a. Zielsystem laden.....	414
Meterpreter-Sitzung, Dateien verwalten.....	414
Meterpreter-Sitzung, Prozeß beenden.....	414
Meterpreter-Sitzung, Route über.....	92
Meterpreter-Sitzung, Routing-Tabelle anzeigen.....	414
Meterpreter-Sitzung, Shell öffnen.....	414
Meterpreter-Sitzung, Tastatureingaben mitschneiden.....	414
Meterpreter-Sitzung, Zielsystem beenden.....	414
metsvc, Parameter.....	423
Monitor-Modus.....	456

STICHWORTVERZEICHNIS

MS SQL Server, Payload ausführen.....	90
msfpayload.....	287, 416, 418
—, Parameter.....	102, 419
msfvenom, Parameter.....	103, 425
MS-SQL Server, Default-Passwörter.....	338
MS-SQL Server, Ports.....	337
MS-SQL-Module, Metasploit.....	339
MySQL.....	358, 636
—, Datei in Tabelle laden.....	364
—, Dateizugriff.....	363
—, Passwörter ermitteln.....	305
—, Standarduser.....	358
—, Tabelle m. Userdaten.....	637
—, Versionserkennung.....	358
—, Zugangsdaten.....	359
MySQL-Abfrage.....	298, 360
MySQL-Anmeldung.....	93
MySQL-Konfigurationsdateien.....	367
MySQL-Module v. Metasploit.....	358
MySQL-Server, Datei herunterladen.....	363

N

Namensanfragen-Verarbeitung.....	195
Namensauflösung.....	613
— verhindern.....	238
Nameserver abfragen.....	261
Nameserver suchen.....	197
Nameserver, Name des.....	183
Ncrack.....	382
NetBIOS over TCP/IP.....	312
NetBIOS-Namensanfragen fälschen.....	93
Network Address Translation.....	133
Netzverbindungen überwachen.....	111
Netzwerk Routen hinzufügen.....	111
Netzwerkadapter.....	164
Netzwerk-Brücke in and. Netzwerke.....	441
Netzwerke auslesen.....	438
Netzwerkkarte ermitteln.....	556
Netzwerkkarte, IP-Adresse d. eigenen.....	522
Netzwerkkarte, Monitor-Modus.....	456
Netzwerkkarte, Promiscuous-Mode.....	70
Netzwerkkonfiguration ausgeben.....	430
Netzwerkkontrollsystem ausschalten.....	497
Netzwerksniffer f. Windows.....	67
Netzwerktreiber, virtuelle.....	470
Netzwerkzugangskontrollsystem.....	496
Netzzugangsschicht.....	231
Next Generation Firewalls.....	481
NFS.....	354
—, Dateirechte umgehen.....	355
—, Freigabe einbinden.....	355
—, Freigaben anzeigen.....	354
NFS-Konfigurationsdateien.....	357
NFS-Shares, Zugriff auf.....	356
Nmap Scripting Engine.....	239
Nmap, bösartige Skripte.....	240
Nmap, DNS-Informationen.....	263
Nmap, Kooperation m. Metasploit.....	241
Nmap, Parameter.....	239
Nmap-Skripte, Kategorien.....	239
ntds.dit.....	560
— extrahieren.....	563
NTLM, Rainbow-Tabellen für.....	567
NTLM-Verschlüsselung.....	408, 567
NTLM-Verschlüsselung downgraden.....	316
NTP.....	310
NTP-Server, Traffic abfragen.....	311
Nullsession.....	313

O

Offene Ports suchen.....	236f.
Offener HTTP-Proxy.....	240
Offener Port, Reaktion.....	231
Öffentliche Schlüssel suchen.....	192
Office-Dokument, bösartiges.....	527
Office- Progr., Makro programmieren.....	349
Offline-Passwortknacker.....	61
Online-Banking.....	388
—, Cookie auslesen.....	500
—, USB-Stick.....	505
—, Verfahren.....	500
Online-Shopping, Daten suchen.....	190
Open Mail Relays suchen.....	556
OpenSSH.....	249
OpenSSL.....	389
Operative Sicherheit.....	26
Opfersystem steuern.....	91
Oracle.....	351
— Auditing Tools.....	354
—, interaktive Anweisungen.....	353
—, Kontodaten auslesen.....	353
—, SQL-Anweisung ausführen.....	353
—, Standardkonten.....	351
—, Tabelle f. Passworthashes.....	351
—, TNS-Dienst.....	353
—, Zugangsdaten erraten.....	353
OSSTMM-Handbuch.....	26
OSVDB.....	397
—, Suchoptionen.....	400

P

Packet Storm.....	402
Pakete verfolgen.....	618
Pakete, Lebensdauer.....	620
Paketfilter.....	480
Paketweiterleitung, Linuxkernel.....	73
Paketweiterleitungen.....	472
Partitionen, logische.....	144
Partitionen, Zahl d. primären.....	144
Passwort erlangen.....	55, 61
Passwort, Klartext.....	55
Passwort, schwaches.....	56
Passwort, verschlüsseltes.....	55
Passwortdateien.....	67
Passworte offline knacken.....	61
Passwörter mitschneiden.....	55, 67
Passwörter suchen.....	190
Passwörter wiederherstellen.....	61
Passwörter, eigene erzeugen.....	61
Passworthash (Def.).....	55
Passworthashes knacken.....	67
Passwortknack-Programme.....	56
Passwortlänge (Win.).....	446
Passwortlisten.....	65
Passwortschutz umgehen.....	405
Passwortliste, Metasploit-Listen.....	248
Payload.....	413
— (Def.).....	88
— für bestimmtes Protokoll.....	394
— in ausführbare Datei wandeln.....	418
— nachladen.....	517
—, Ausgabeformate.....	421
—, Rückkanal.....	394, 524
—, Verbindungswege.....	88
—, verschlüsseltes.....	91, 529
Payload-Arten.....	394
Payload-Größe.....	416

Payload-Kriterien..... 419
Pcap-Datei, Audioströme extrahieren..... 476
Pcap-Format 72, 80
PDF, bösartige..... 526
Penetrations-Test (Def.) 21
Personen/-gruppen suchen 172
Personensuchmaschinen..... 200
Phishing 117, 209, 542
PHP, Typüberprüfung 297
PHP-Shell auf Webserver hochladen 364
ping..... 197, 357
pingscan..... 615
Pipl..... 201
Port (Def.) 229
Port, unbekannter..... 387
Portbereiche 231
Portmapper 310
Portnummer 229
Ports f. Backdoors..... 184
Ports, Auflistung d. Dienste 230
Ports, offene ermitteln 623
Portscanner 236
Portscanning (Def.) 229
PostgreSQL 379, 641, 97
— m. SQL abfragen..... 380
—, Versionserkennung 380
—, Zugangsdaten erraten 380
PostgreSQL-Server, Dateisystem auslesen 381
Pre-Shared Key 330
Programme aus Quellen installieren 53
Protokoll-Prüfung 481
Protokollscan..... 623
Protokollversion downgraden..... 251
Proxy 244, 482
— in Browser eintragen 280
—, nutzbaren suchen 244
—, umleiten auf 473
Proxy-Autorisierung umgehen..... 483
psk-crack, Parameter 334
PSK/WPA-Verschlüsselung knacken 80
Putty kompromittieren..... 425

Q

Quellport..... 231
Quelltext übersetzen 52

R

RADIUS-Server..... 456
Rainbow-Tabelle (Def.) 56
Rainbow-Tabellen für NTLM 567
RATTE..... 112, 483
— verteilen 488
—, Standalone-Version 119
RATTE-Server..... 484
RAV-Formelblatt 33, 646
RDP..... 368
— aktivieren 92
—, Administrator-Account angreifen 368
Reaver 464
—, Parameter 465
Rechtestatus ändern..... 444
reg, Parameter 435
Regelkonformität 22
Registry auslesen..... 431, 433
Registry, Hauptschlüssel..... 433
Registry, Meterpreter 435
Registry-Pfad 435
Remote Desktop aktivieren 448

Remote Desktop Protocol..... 368
Remote-Shell 413, 416
remotewinenum, Parameter 431
Remote-Zugang a. Windows-Desktop..... 319
Reverse Engineering 508
Reverse Name Lookup..... 617
Reverse Payload (Def.) 88
Reverse Shell 416
reverse_tcp..... 91, 418
RFC-Schnittstelle 568
Risikofaktor berechnen 33
Risk Assessment Value/RAV 27
Rootshell, booten in 409
Route anlegen 442
route, Parameter 441
Router rooten 495
Router suchen 190
Router, MAC-Adresse 80
Routing-Advertisements..... 168
Routing-Informationen suchen 430
Routing-Regeln ändern..... 472
RPC 310
—, registrierte Funktionen 310
Runlevel..... 48

S

Safari, Schwäche 542
Safari, Zugriff a. lok. Dateisystem 542
Samba 312, 643
—, Freigaben abfragen 313
—, Metasploit-Module 313
—, passwortloses Gastkonto..... 313
—, Versionserkennung 312
—, Zugangsdaten erraten 314
Samba-Backdoor 321
Samba-Server, Passwortdatenbank 447
Samba-Verkehr umleiten..... 319
SAM-Datenbank ausgeben 414
SAP, Administratorkonto anlegen..... 585
SAP, angemeldeten User ausgeben 585
SAP, Anwenderauthentifizierungs-Prog..... 606
SAP, Befehle a. Betriebssystemebene ausf. 583
SAP, Change-Control-System umgehen..... 605
SAP, Dateien aus Internet laden 585
SAP, DIAG-Protokoll untersuchen 578
SAP, Fehlogins beschränken 574
SAP, Hashcode-Generator 576
SAP, Java-Stack 568
SAP, Logon-Modul 606
SAP, Passwörter auslesen 586
SAP, Remote-Desktop-Zugriff aktivieren..... 586
SAP, REPOSRC-Tabelle 605
SAP, RFC-Schnittstelle 568, 582
SAP, Rootshell erhalten 583
SAP, Shell-Befehle 583, 598
SAP, Speicherort d. Passwörter 575
SAP, Standard-Zugangsdaten..... 572, 573
SAP, Systemproxy 585
SAP, Systemtabellen..... 604
SAP, Vollzugriff auf 568
SAP, Windows-Firewall deaktivieren 585
SAP-Anwendungsserver 567
SAP-Benutzerrechte 568
SAP-Connector..... 587
SAP-Datenbank 575
SAP-Datenbank, Systemprogramme..... 605
SAP-Default-Mandanten..... 568
SAP-Dienst, Protokoll anpassen..... 587
SAP-Dorks 569

STICHWORTVERZEICHNIS

SAP-Exploits.....	591	Smartphone, Backtrack auf.....	146
SAP-GUI, ActiveX-Komponenten.....	608	Smartphone, Kernel.....	147
SAP-Hashes knacken.....	66	Smartphone, root-Rechte.....	147
SAP-Instanz.....	567	SMB, Authentifizierungsdaten.....	542
SAP-Kernel.....	568	SMB-Anmeldung.....	93
SAPMSYST.....	606	smbclient, Parameter.....	313
SAP-Passwörter wiederherstellen.....	583	SMB-Dienst, Exploit gegen.....	90
SAP-Passwörter, Format.....	575	SMB-Freigabe, Payload ausführen.....	90
SAP-Reports.....	568	SMB-Protokoll.....	68, 312
SAP-Serverkennungen.....	570	SMS fälschen.....	119
SAP-Systeme suchen.....	568	SMTP.....	254
SAP-System-ID.....	568	—, Benutzernamen raten.....	255
Scanner-Hilfsmodule.....	243	—, Brute-force-Angriff.....	256
Schadcode.....	88	—, Verbindungsabbau/-aufbau.....	255
— automatisch ausführen.....	118	—, Versionserkennung.....	255
— in RAM ausführen.....	517	SMTP-Befehle.....	255
Schattenkopien.....	560	SMTP-Dienst, Banner.....	197
— aktivieren.....	561	SMTP-Konfigurationsdateien.....	258
Schlüssel, geheimer/öffentlicher.....	250	Sniffer.....	68
Schlüsselaustausch.....	330	sniffer, Optionen.....	439
Schwachstelle.....	30	SNMP.....	93, 323
— ausnutzen.....	246, 393	—, Community-Strings.....	323
— quantifizieren.....	35	—, Zugangsdaten angreifen.....	324f.
— suchen.....	240	SNMP-Agent.....	323
Schwachstellenprüfung, benötigte Daten.....	24	SNMP-Einträge auslesen.....	325
Schwachstellenprüfung, erweiterte.....	25	SNMP-Managementstation.....	323
Schwachstellenprüfung, Falschmeldungen.....	24	Social Engineering.....	208, 520
Schwachstellen-Sammlungen.....	394	Social Engineering Framework.....	210
SCTP.....	238	Social Engineering Toolkit, SET.....	112, 210
Serverdienste.....	229	Software-Aktualisierung.....	54
Serversniff.....	197	Spoofing-Mail.....	522
Server-Standort ermitteln.....	204, 613	Sprachaufnahmen konvertieren.....	478
Session Stealing.....	501	SQL.....	297
SET aktualisieren.....	486	—, Hochkomma.....	298
SET Interactive Shell, Befehle.....	112, 121	—, kritische Zeichen.....	299
SET konfigurieren.....	114	SQL-Befehle einschleusen.....	132, 300
SET, Angriffskategorien.....	117	SQLMap.....	300, 365
SET, Payloads.....	112	—, Parameter.....	301
SET-Backdoors.....	119	SSH.....	249, 629
SET-Konfigurationsdatei.....	521	SSH Version 1.....	251
Shared Hosting (Def.).....	204	SSH, Brute-force-Angriff.....	250
Shared Hosting ermitteln.....	195	SSH, Passwort.....	61
shell_bind_tcp.....	91	SSH, Versionserkennung.....	250
shell_reverse_tcp.....	91	SSH, Zugangsdaten mitlesen.....	251
Shelldatei in and. Datei verstecken.....	288	SSH-Anmeldung.....	93
Shell-Sitzung.....	94	SSH-Filter.....	251
Shell-Upgrade.....	415	SSH-Konfigurationsdateien.....	253
Shell-Verbindung zum Opfer.....	88	SSH-Protokollversion downgraden.....	251
Shell-Verbindung, reverse.....	517	SSH-Protokollversion ermitteln.....	251
Shellzugang, Arten.....	416	SSID.....	457
Shellzugriff auf Linux-System.....	91	SSL.....	388
Shellzugriff auf Windows-System.....	91	SSL-Verbindungen aufbrechen.....	507
Shellzugriff erhalten.....	246	SSL-Verschlüsselung prüfen.....	197
Shellzugriff i. Windows.....	345	SSL-VPN.....	336
SHH, Zugangsdaten erraten.....	250	SSL-Zertifikatversionen suchen.....	192
Shodanq.....	187	Stacked Queries.....	302
—, Exploits.....	193	Standard-Zugangspasswörter.....	406
—, SSL-Filter.....	192	startx.....	140
Sicherheitslücken.....	30	Stateful Firewall.....	481
—, Kategorien v.....	30	Subdomains suchen.....	178, 194, 265
Sicherheitsrichtlinien.....	22	Suchmaschinen.....	187
Signaturstick, eigener.....	508	swvar, Parameter.....	375
Signaturstick, Komponenten.....	505	Swapspace.....	143
SIP.....	369, 377	Sybase, Tabelle m. Benutzerdaten.....	369
SIP-Module v. Metasploit.....	370	System aktiv?.....	239, 357
sipsak, Parameter.....	372	System umleiten.....	259
SIP-Server identifizieren.....	371	System, ansprechbares.....	27, 615
Skipfish.....	291	System, sicheres (Def.).....	27
—, Parameter.....	292	Systembenutzer ausgeben.....	430
smap, Parameter.....	371	Systemeigenschaften suchen.....	193

Systeminformationen sammeln	430
Systemkontrolle	412
System-Uptime ermitteln	197

T

Tabnapping	118
TCP	234
TCP/IP	231
TCP-Flags	233, 235
TCP-Handshake	236
TCP-Paket, Header	233
TCP-Pakete verfolgen	614
TCP-Scan	238, 241
TCP-Sequenznummer	232
TCP-Verbindung z. Angreifer herstellen	287
Teensy USB Board	119, 515
Teensy, Backdoor entwickeln	516
Telefongeräte suchen	375
Telefongespräche mitschneiden	375
Telefonsystem abstürzen lassen	378
telnet	247, 269
Telnet	253, 387, 558, 628
—, Bruteforce-Angriff	254
—, Zugangsdaten mitlesen	254
Telnet-Server aktivieren	450
Telnet-Verbindung	95
Terminalserver	340
Terminalsystem	498
Testmethodik	26
Testprogramme (Auflistung)	49, 50, 51, 52
Testtyp Double Blind	612
Testtypen	22
Testumfang	42
Testziele	41
TFTP	266
THC IPv6 Attack Toolkit	134
thc-ssl-dos	336
The Thomas Werth Java Attack	520
TheHarvester	177
timestamp, Parameter	451
Token übernehmen	445
Traceroute	196, 198, 374, 618
Transport-Protokolle	231
Transportschicht	233
TrueCrypt	155, 548
—, Schlüsseldatei	160
—, Verschlüsselungsmethoden	157
TrueCrypt-Bootloader patchen	549
TTL abfragen/TTL-Werte	186, 620
TUN/TAP-Modul	470
Tunnel durch Firewall	490
Tunnelndienst	168

U

U3-Tools, Komponenten	510
UAC deaktivieren	415
UDP	233, 241
UDP-Paket, Header	234
UDP-Scan	238, 241
Unicornscan, Parameter	243
UNION-Abfrage	302
Unix-Dateirechte	355
URLs auf Webserver suchen	295
USB-Adapter, böstätiger	119
USB-Angriffsvektor	112
USB-Autostartschutz umgehen	515
USB-Stick verschlüsseln	156
USB-Tastatur emulieren	515

V

Vektor (Def.)	31
Verbindungsaufbau	235, 269
Verbindungs-Endpunkt	229
Vermittlungsschicht	231
Vertragspartner, zustimmungspflichtiger	40
Vertrauensbeziehungen zw. Systemen	28
Verwundbare Systeme suchen	190
VirtualBox	142
Virtualisierung	437
Virtuelle Hosts	295
Virtuelle Maschine	48
—, Gast-Erweiterungen	143
—, Hardware	142
—, prüfen auf	92
Visibility	27
VM, IP-Adresse des Gast-Systems	281
VMWare-Player	142
VNC	382
VNC, Passwort erraten	382
VNC-Konfigurationsdateien	383
VNC-Passwort, Registryeintrag	383
VNC-Server auf Zielsystem aufrufen	415
VNC-Server mit/ohne Authentifizierung	382f.
Voice over IP	369
VPN	329
—, Aggressive-Mode	330, 333, 335
—, Authentifizierungs- und Integritätsfunktionen	330
—, Denial-of-Service	336
—, Internet Key Exchange	330
—, Main-Mode	330
—, Schlüsselaustausch	330, 333
VPN-Art prüfen	331
VPN-Einstellungen setzen	335
VPN-Server identifizieren	335
vssown, Parameter	561
Vulnerability	30
Vulnerability Assessment	24

W

W3AF	293
—, Befehle	126
—, Exploit-Befehle	131
—, Exploits	122, 132
—, Plugin (Def.)	121, 128
—, Plugin-Kategorien	128
—, Profil (Def.)	121, 127
—, Shellsitzungs-Befehle	133
Waffit	272
Wayback Machine	187, 203
Weakness	30
Web Application Attack and Audit Framework, W3AF	121
Web Application Firewall	271
Web-2.0-Inhalte	290
Web-Anwendungen prüfen	121, 291
Webauftritte verwalten mit Metasploit	295
Web-Backdoor	268
— einschleusen	285
— in Bilddatei speichern	288
— schreiben	287
Web-Backdoors, frei verfügbare	286
Webcams suchen	190
Web-Datenbank, Schwachstellen	297
Web-Datenverkehr umleiten	279
WebDAV	132, 267
—, Datei hochladen	288
Webdienst, Schwachstellenscanner	341
Webpräsenz testen	111

STICHWORTVERZEICHNIS

Web-Proxy.....	279
Webseite durchsuchen.....	93
Webseite klonen.....	523
Webseite kopieren.....	201
Webseite offline prüfen.....	202
Webseite präparieren.....	537
Webseite, Applet einschleusen.....	521
Webseite, bössartige.....	117
Webseite, Inhalte nachladen.....	537
Webseite, Überlauf provozieren.....	299
Webseite, Zugangsdaten abfangen.....	542
Webseiten in andere Webseite einbetten.....	537
Webseiten suchen.....	172
Webseiten, statische untersuchen.....	290
Webseiten-Generierungsumgebung.....	285
Webserver identifizieren.....	190
Webserver, Datei hochladen.....	286
Webserver, Dateifilter überlisten.....	288
Webserver, Dokumente auswerten.....	275
Webserver, Passwortdatei.....	298
Webserver, Passwörterhasches.....	277
Webserver, PHP-Shell hochladen.....	364
Webserver, Schutzmaßnahmen suchen.....	271
Webserver, Skriptsprachen.....	286
Webserver, Versionserkennung.....	268
Webserver, verwundbare Dateien suchen.....	190
Webserver, Verzeichnisse ermitteln.....	272, 626
Webserver, Zugangsdaten erraten.....	276f.
Webserver-Konfigurationsdateien.....	309
Webserver-Schwachstellen ausnutzen.....	293
Website, Authentifizierungsverfahren testen.....	127
Website-Archiv.....	187
Website-Prüfung, vollständige.....	127
WEP-Verschlüsselung knacken.....	79, 455
Whitebox-Test.....	25
whois, Parameter.....	180
whois-Daten.....	240
whois-Datenbanken.....	180
whois-Eintrag abfragen.....	196
whois-Server.....	182
Windows Retrieval.....	556
Windows Scripting Host, Skript ausführen.....	517
Windows XP, USB.....	47
Windows, Administrator-Passwort.....	406
Windows, Benutzerauthentifizierung.....	559
Windows, Benutzerkonten-Datenbank.....	432
Windows, Domänenkonten suchen.....	406, 408
Windows, Ereignisanzeige leeren.....	453
Windows, erweiterte Benutzerkontrolle angreifen.....	415
Windows, lokale Benutzerdaten suchen.....	406
Windows, Netzwerkniffer.....	67
Windows, Paßwörter m. Zeitstempeln.....	434
Windows, Passwörterhasches aufbereiten.....	567
Windows, Passwörterhasches extrahieren.....	560
Windows, Passwörterhasches knacken.....	447
Windows, Passwort-Verschlüsselung.....	408
Windows, Sicherheitsrichtlinien-Datei.....	432
Windows, Speicherort d. Passwörter.....	559f.
Windows, Verbindungsdaten mitlesen.....	315
Windows, verschlüsselte Passwörter anzeigen.....	408
Windows-Backdoor entwickeln.....	419
Windows-Domäne, Benutzerkonten.....	559
Windows-Fernverbindungen.....	448
Windows-Passwörter knacken.....	407
Windows-Passwörterhasches auslesen.....	92
Windows-Passwörterhasches direkt anwenden.....	446
Windows-Passwortverschlüsselung.....	567
Windows-Powershell.....	517
Windows-Registrierdatenbank.....	406
Windows-Registry.....	432

Windows-Shell auf Meterpreter-Sitzung erweitern.....	96
Windows-System fremdbooten.....	406
Windows-TTL.....	620
Wine.....	49
Wireshark.....	375
WLAN aufspannen.....	79
WLAN, Accesspoint emulieren.....	79, 82, 119, 458, 467, 470
WLAN, bössartiges.....	119
WLAN, Clients hinauswerfen.....	79, 457
WLAN, Denial of Service.....	466
WLAN, Pakete einspielen/einschleusen.....	79, 82, 457
WLAN, Pakete mitlesen.....	456
WLAN, PIN erraten.....	464
WLAN, virtuelles Tunnel-Interface.....	79
WLAN, Zielnetzwerk finden.....	459
WLAN-Accesspoint, virtueller.....	467
WLAN-Clients, mobile.....	467
WLAN-Karte ansprechen.....	77, 166
WLAN-Karte, Injektions-Modus.....	79, 458
WLAN-Karte, Monitormodus.....	74, 81
WLAN-Karten anzeigen.....	81
WLAN-Kartentreiber.....	74
WLAN-Kennung, WLAN-Name.....	74, 80, 457
WLAN-Netzwerkmitsschnitte entschlüsseln.....	79
WLANs auflisten.....	81
WLAN-Tools.....	74
WLAN-Verkehr mitschneiden.....	457
WLAN-Verschlüsselung.....	74, 455
WLAN-Zugangsdaten knacken.....	79
WMAP.....	294
Wortliste.....	56
—, eigene bauen.....	57
Wortlisten v. Metasploit.....	57
Wortlisten, spezialisierte.....	57
wpa_supplicant.....	166
WPA-Enterprise.....	456
WPA-Handshake.....	80
WPA-Verschlüsselung.....	456
WPS-Verschlüsselung.....	456
Wscript ausführen.....	517
WSCRIPT-Payload.....	517

X

X, Bildschirm abfangen.....	385
X, Bildschirm freigeben.....	384
X, Host.....	384
X, Tastatureingaben abfangen.....	385
X, Umgebungsvariable.....	383
X11.....	383
X11-Dienste suchen.....	93
X11-Systeme suchen.....	384
XEN App.....	340
xhost.....	384
X-Konfigurationsdateien.....	386

Z

Zeichenkette, interpretierte.....	299
Zeitserver.....	311
Zeitstempel ändern.....	414, 451
Zenmap.....	240
Zertifikat nach IT-Grundschutz.....	23
Zertifikaten v. best. Herstellern suchen.....	192
Zielbereich.....	31
Zielport.....	231, 233
Zielsystem Admin. hinzufügen.....	121
Zielsystem als Gateway.....	441
Zonentransfer.....	263, 618
Zugangsdaten, schwache.....	246