

Alexander Geschonneck

Computer-Forensik

Computerstraftaten erkennen, ermitteln, aufklären

5., aktualisierte und erweiterte Auflage

Alexander Geschonneck
geschonneck@computer-forensik.org

Lektorat: René Schönfeldt
Copy-Editing: Ursula Zimpfer, Herrenberg
Herstellung: Nadine Thiele
Autorenfoto: Markus Vogel
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

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

ISBN 978-3-89864-774-8

5., aktualisierte und erweiterte Auflage 2011
Copyright © 2011 dpunkt.verlag GmbH
Ringstraße 19 B
69115 Heidelberg

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Inhaltsverzeichnis

Einleitung	1
Wer sollte dieses Buch lesen?	2
Was lernt man in diesem Buch?	4
Was lernt man in diesem Buch nicht?	4
Wie liest man dieses Buch?	5
Was ist neu in der 5. Auflage?	8
1 Bedrohungssituation	11
1.1 Bedrohung und Wahrscheinlichkeit	11
1.2 Risikoverteilung	12
1.3 Motivation der Täter	16
1.4 Innetäter vs. Außentäter	21
1.5 Bestätigung durch die Statistik?	24
1.6 Computerkriminalität	25
2 Ablauf von Angriffen	33
2.1 Typischer Angriffsverlauf	33
2.2 Beispiel eines Angriffs	36
3 Incident Response als Grundlage der Computer-Forensik	45
3.1 Der Incident-Response-Prozess	45
3.2 Organisatorische Vorbereitungen	46
3.3 Zusammensetzung des Response-Teams	47
3.4 Incident Detection: Systemanomalien entdecken	49
3.5 Incident Detection: Ein Vorfall wird gemeldet	54
3.6 Sicherheitsvorfall oder Betriebsstörung?	57

3.7	Wahl der Response-Strategie	60
3.8	Reporting und Manöverkritik	61
4	Einführung in die Computer-Forensik	65
4.1	Ziele einer Ermittlung	65
4.2	Anforderungen an den Ermittlungsprozess	66
4.3	Phasen der Ermittlung	67
4.4	Das S-A-P-Modell	68
4.5	Welche Erkenntnisse kann man gewinnen?	70
4.6	Wie geht man korrekt mit Beweismitteln um?	77
4.7	Flüchtige Daten sichern: Sofort speichern	88
4.8	Speichermedien sichern: Forensische Duplikation	91
4.9	Was sollte alles sichergestellt werden?	94
4.10	Erste Schritte an einem System für die Sicherstellung	96
4.11	Untersuchungsergebnisse zusammenführen	97
4.12	Häufige Fehler	99
4.13	Anti-Forensik	101
5	Einführung in die Post-mortem-Analyse	105
5.1	Was kann alles analysiert werden?	105
5.2	Analyse des File Slack	107
5.3	Timeline-Analysen	111
5.4	NTFS-Streams	117
5.5	NTFS TxF	118
5.6	NTFS-Volumen-Schattenkopien	120
5.7	Windows-Registry	124
5.8	Windows UserAssist Keys	128
5.9	Windows Prefetch-Dateien	129
5.10	Auslagerungsdateien	132
5.11	Versteckte Dateien	133
5.12	Dateien oder Fragmente wiederherstellen	137
5.13	Unbekannte Binärdateien analysieren	138
5.14	Systemprotokolle	151
5.15	Analyse von Netzwerkmitschnitten	153

6	Forensik- und Incident-Response-Toolkits im Überblick	155
6.1	Grundsätzliches zum Tooleinsatz	155
6.2	Sichere Untersuchungsumgebung	157
6.3	F.I.R.E.	159
6.4	Knoppix Security Tools Distribution	163
6.5	Helix	164
6.6	ForensiX-CD	169
6.7	C.A.I.N.E. und WinTaylor	171
6.8	DEFT und DEFT-Extra	174
6.9	EnCase	175
6.10	dd	180
6.11	Forensic Acquisition Utilities	184
6.12	AccessData Forensic Toolkit	185
6.13	The Coroner's Toolkit und TCTUtils	189
6.14	The Sleuth Kit	190
6.15	Autopsy Forensic Browser	195
6.16	Eigene Toolkits für Unix und Windows erstellen	199
7	Forensische Analyse im Detail	205
7.1	Forensische Analyse unter Unix	205
7.2	Forensische Analyse unter Windows	236
7.3	Forensische Analyse von mobilen Geräten	279
7.4	Forensische Analyse von Routern	295
8	Empfehlungen für den Schadensfall	299
8.1	Logbuch	299
9	Backtracing	307
9.1	IP-Adressen überprüfen	307
9.2	Spoof Detection	310
9.3	Routen validieren	313
9.4	Nslookup	317
9.5	Whois	318
9.6	E-Mail-Header	320

10	Einbeziehung der Behörden	323
10.1	Organisatorische Vorarbeit	323
10.2	Strafrechtliches Vorgehen	325
10.3	Zivilrechtliches Vorgehen	328
10.4	Darstellung in der Öffentlichkeit	330
10.5	Die Beweissituation bei der privaten Ermittlung	331
10.6	Fazit	335
	Anhang	337
A	Tool-Überblick	339
B	C.A.I.N.E.-Tools	347
C	DEFT-Tools	355
	Literaturempfehlungen	359
	Index	361