

Tobias Klein ist als IT-Sicherheitsberater tätig. Er hat zahlreiche Schwachstellen in verschiedenen Softwarelösungen aufgedeckt und ist bereits Autor zweier Fachbücher: »Linux-Sicherheit · Security mit Open-Source-Software · Grundlagen und Praxis« (dpunkt.verlag, 2001) sowie »Buffer Overflows und Format-String-Schwachstellen · Funktionsweisen, Exploits und Gegenmaßnahmen« (dpunkt.verlag, 2003).

Tobias Klein

Aus dem Tagebuch eines Bughunters

**Wie man Softwareschwachstellen
aufspürt und behebt**



dpunkt.verlag

Tobias Klein
tk@trapkit.de

Lektorat: René Schönfeldt
Copy-Editing: Ursula Zimpfer, Herrenberg
Herstellung: Birgit Bäuerlein
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: Media-Print Informationstechnologie, 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 978-3-89864-659-8

1. Auflage 2010
Copyright © 2010 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

1	Einleitung	1
1.1	Ziele des Buches	1
1.2	Wer sollte dieses Buch lesen?	1
1.3	Haftungsausschluss	2
1.4	Weitere Informationen	2
2	Bughunting	3
2.1	Nur zum Spaß?	4
2.2	Techniken und Vorgehensweisen	4
2.3	Speicherfehler	6
2.4	Handwerkszeug	7
	2.4.1 Debugger	7
	2.4.2 Disassembler	8
2.5	EIP = 41414141	8
2.6	Was nun folgt	9
	<i>Literatur</i>	9
3	Die 90er lassen grüßen	11
3.1	Die Schwachstelle	12
3.2	Ausnutzung der Schwachstelle	15
3.3	Behebung der Schwachstelle	22
3.4	Gewonnene Erkenntnisse	25
3.5	Nachtrag	26
	<i>Literatur</i>	27

4	Flucht aus der Zone	29
4.1	Die Schwachstelle	29
4.2	Ausnutzung der Schwachstelle	40
4.3	Behebung der Schwachstelle	55
4.4	Gewonnene Erkenntnisse	56
4.5	Nachtrag	57
	<i>Literatur</i>	57
5	NULL Pointer FTW	59
5.1	Die Schwachstelle	59
5.2	Ausnutzung der Schwachstelle	64
5.3	Behebung der Schwachstelle	75
5.4	Gewonnene Erkenntnisse	79
5.5	Nachtrag	79
	<i>Literatur</i>	80
6	Browse and you're Owned	81
6.1	Die Schwachstelle	81
6.2	Ausnutzung der Schwachstelle	93
6.3	Behebung der Schwachstelle	95
6.4	Gewonnene Erkenntnisse	96
6.5	Nachtrag	96
	<i>Literatur</i>	97
7	Einer für alle	99
7.1	Die Schwachstelle	99
7.2	Ausnutzung der Schwachstelle	117
7.3	Behebung der Schwachstelle	125
7.4	Gewonnene Erkenntnisse	125
7.5	Nachtrag	125
	<i>Literatur</i>	126
8	Ein Bug älter als 4.BSD	127
8.1	Die Schwachstelle	127
8.2	Ausnutzung der Schwachstelle	134

8.3	Behebung der Schwachstelle	146
8.4	Gewonnene Erkenntnisse	146
8.5	Nachtrag	147
	<i>Literatur</i>	148
9	Das Klingelton-Massaker	149
9.1	Die Schwachstelle	149
9.2	Auswertung der Abstürze und Ausnutzung der Schwachstelle	158
9.3	Behebung der Schwachstelle	166
9.4	Gewonnene Erkenntnisse	166
9.5	Nachtrag	167
	<i>Literatur</i>	167
10	Was du vielleicht noch wissen willst über ...	169
10.1	Stack Buffer Overflows	169
	<i>Literatur</i>	174
10.2	NULL Pointer Dereferences	175
10.3	Typkonvertierungen in C	176
	<i>Literatur</i>	179
10.4	Hilfreiche Kommandos des Solaris-Debuggers (mdb)	180
10.4.1	Starten und stoppen von mdb	180
10.4.2	Allgemeine Kommandos	180
10.4.3	Breakpoints	180
10.4.4	Programmsteuerung	180
10.4.5	Untersuchung von Daten	181
10.4.6	Informative Kommandos	181
10.4.7	Weitere Kommandos	181
	<i>Literatur</i>	181
10.5	Hilfreiche Kommandos des Windows-Debuggers (WinDBG)	182
10.5.1	Starten und stoppen einer Debugger-Sitzung	182
10.5.2	Allgemeine Kommandos	182
10.5.3	Breakpoints	182
10.5.4	Programmsteuerung	182
10.5.5	Untersuchung von Daten	183
10.5.6	Informative Kommandos	183
10.5.7	Weitere Kommandos	183
	<i>Literatur</i>	183

10.6	Hilfreiche Kommandos des GNU-Debuggers (gdb)	184
10.6.1	Starten und stoppen von gdb	184
10.6.2	Allgemeine Kommandos	184
10.6.3	Breakpoints	184
10.6.4	Programmsteuerung	184
10.6.5	Untersuchung von Daten	185
10.6.6	Informative Kommandos	185
10.6.7	Weitere Kommandos	185
	<i>Literatur</i>	185
10.7	Exploit-Gegenmaßnahmen	186
10.7.1	Address Space Layout Randomization (ASLR)	186
10.7.2	Security Cookies (/GS), Stack Smashing Protection (SSP) oder Stack Canaries	187
10.7.3	NX und DEP	187
10.7.4	Wie kann ich erkennen, ob ein Programm oder ein Prozess solche Schutzmechanismen einsetzt?	187
	<i>Literatur</i>	197
10.8	Das Sun-Solaris-Zonenkonzept	199
10.8.1	Terminologie	199
10.8.2	Erstellen einer nicht globalen Solaris-Zone	200
	<i>Literatur</i>	202
10.9	Die »GOT Overwrite«-Exploit-Technik	203
	<i>Literatur</i>	208
10.10	RELRO	209
	<i>Literatur</i>	213
10.11	Windows-Kernel-Debugging	214
	<i>Literatur</i>	217
10.12	Mac-OS-X-Kernel-Debugging	218
	<i>Literatur</i>	222
	Schlusswort	223
	Index	225