

# Inhaltsverzeichnis

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Ziele des Buches .....	1
1.2	Wer sollte dieses Buch lesen? .....	1
1.3	Haftungsausschluss .....	2
1.4	Weitere Informationen .....	2
<b>2</b>	<b>Bughunting</b>	<b>3</b>
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
<b>3</b>	<b>Die 90er lassen grüßen</b>	<b>11</b>
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

<b>4</b>	<b>Flucht aus der Zone</b>	<b>29</b>
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
<b>5</b>	<b>NULL Pointer FTW</b>	<b>59</b>
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
<b>6</b>	<b>Browse and you're Owned</b>	<b>81</b>
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
<b>7</b>	<b>Einer für alle</b>	<b>99</b>
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
<b>8</b>	<b>Ein Bug älter als 4.4BSD</b>	<b>127</b>
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
<b>9</b>	<b>Das Klingelton-Massaker</b>	<b>149</b>
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
<b>10</b>	<b>Was du vielleicht noch wissen willst über ...</b>	<b>169</b>
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
	<b>Schlusswort</b> .....	<b>223</b>
	<b>Index</b> .....	<b>225</b>