

**Tobias Klein**

# **Linux-Sicherheit**

**Security mit Open-Source-Software -  
Grundlagen und Praxis**

| " | | dpunkt.verlag

14 - ZJZ  
05

# Inhaltsübersicht

1	Einleitung	.1
2	Über dieses Buch	.9
3	Installation	.17
4	Authentifikation	.37
5	Sicherheitsrelevante Systemadministration	.71
6	Härtung des Linux-Systems	.107
7	Kernel	.163
8	Sudo	.175
9	Buffer Overflows	.185
10	Systemanomalien	.211
11	Computer-Würmer	.217
12	Viren	.225
13	Trojanische Pferde	.237
14	Spoofing	.251
15	Netzwerk-Scan-Techniken	.277
16	Sniffer	.329
17	Linux und Verschlüsselung	.345
18	Denial-of-Service-Attacks	.449
19	Distributed-Denial-of-Service-Attacks	.469
20	Audit-Mechanismus, Logfiles und Accounting	.505
21	Firewalls	.551
22	Intrusion Detection	.621
23	Hostbasierte Intrusion Detection	.651
24	Netzwerkbasierte Intrusion Detection	.713
25	Sicherheitsstandards	.745
26	Notfallplan - Mögliche Reaktionen auf eine Systemkompromittierung	.771

## Inhaltsübersicht

### Anhang

A	Kernelparameter. . . . .	787
B	Angriff- und Verteidigungsmatrix. . . . .	797
C	Organisationen. . . . .	799
D	Sicherheitsrelevante Request for Comments (RFC). . . . .	801
E	Sicherheitsneuigkeiten. . . . .	807
F	Die wichtigsten sicherheitsrelevanten Mailinglisten und Newsgroups. . . . .	809
G	Glossar. . . . .	811
H	Literatur. . . . .	819
	Index. . . . .	823

# Inhalt

<b>1</b>	<b>Einleitung</b>	<b>1</b>
1.1	Systemsicherheit	1
1.2	Linux	3
1.3	Linux und Sicherheit	4
<b>2</b>	<b>Über dieses Buch</b>	<b>9</b>
2.1	Umfang und Grenzen	9
2.2	Voraussetzungen der Leser	10
2.3	Verwendete Distribution und Rechnerarchitektur	10
2.4	Darstellungskonventionen	11
2.5	Der vi-Editor	13
<b>3</b>	<b>Installation</b>	<b>17</b>
3.1	Auswahl der Distributionsversion	17
3.2	Noch vor der Installation	19
3.3	Installationsvarianten	19
3.4	Erstellung der Bootdisketten	20
3.5	Minimale Grundinstallation	21
3.6	Auswahl der Pakete	31
3.7	Installation über Netzwerk	33
3.8	Mögliche Komplikationen	34
<b>4</b>	<b>Authentifikation</b>	<b>37</b>
4.1	Was versteht man unter Authentifikation?	38
4.2	Der Anmeldevorgang	39
4.3	Sichere Passwörter	41
4.4	Sicherheitsrisiko Zugangsberechtigung	45
4.5	One-Time-Passwords	49
4.6	PAM	50
4.6.1	Konfiguration von PAM	52
4.6.2	PAM im Einsatz: Login und PAM	55
4.6.3	PAM im Einsatz: Zugriffszeiten beschränken	64
4.6.4	PAM im Einsatz: su einschränken	66
4.6.5	PAM im Einsatz: zusätzliche PAM-Module	67
4.6.6	Fazit	70
<b>5</b>	<b>Sicherheitsrelevante Systemadministration</b>	<b>71</b>
5.1	Multi-User-System	71
5.2	root	71
5.3	Benutzerverwaltung	73

## Inhalt

5.3.1	Anlegen eines Benutzers . . . . .	73
5.3.2	Setzen eines Passwortes . . . . .	76
5.3.3	Löschen eines Benutzers . . . . .	76
5.3.4	Erstellung, Verwaltung und Löschen von Gruppen . . . . .	77
5.3.5	Weitere Funktionen der Shadow Suite . . . . .	77
5.4	Dateisystem und Dateisicherheit . . . . .	81
5.4.1	Besitzverhältnisse und Zugriffsrechte . . . . .	82
5.4.2	Syntax der Zugriffsrechte . . . . .	82
5.4.3	t-Bit, SGID und SUID . . . . .	84
5.5	Werkzeuge für das Dateisystem . . . . .	88
5.5.1	chmod . . . . .	88
5.5.2	chown . . . . .	90
5.5.3	chgrp . . . . .	91
5.6	Erweiterte Funktionen des ext2-Dateisystems . . . . .	92
5.6.1	Konfigurationsprogramme . . . . .	94
5.6.2	Vorteile . . . . .	96
5.6.3	lcap . . . . .	97
5.6.4	Konkreter Einsatz . . . . .	97
5.6.5	Fazit . . . . .	102
5.7	Administrationswerkzeuge . . . . .	102
5.7.1	ps . . . . .	102
5.7.2	netstat . . . . .	103
5.7.3	lsof . . . . .	104
5.7.4	top . . . . .	105
5.8	Installationswerkzeuge . . . . .	105
5.8.1	RPM . . . . .	105
5.8.2	Tarballs . . . . .	106
<b>6</b>	<b>Härtung des Linux-Systems</b> . . . . .	<b>107</b>
6.1	Konfiguration . . . . .	107
6.2	Installation der Kompilerkomponenten . . . . .	111
6.3	Updates und Patches . . . . .	114
6.4	Hashfunktionen . . . . .	115
6.4.1	Sicherheitsrisiko Geburtstagsangriff . . . . .	117
6.4.2	MD5 . . . . .	117
6.4.3	SHS . . . . .	119
6.4.4	Beispiel einer Paketverifizierung anhand von MD5 . . . . .	120
6.5	SUID/SGID . . . . .	122
6.6	Partitionen und SUID/SGID . . . . .	125
6.7	Allgemeine Hinweise zur Restriktion von Filesystemen . . . . .	127
6.8	Konfiguration der angebotenen Dienste . . . . .	127
6.9	TCP_Wrapper . . . . .	133
6.10	xinetd . . . . .	136
6.10.1	inetd und TCP_Wrapper . . . . .	136
6.10.2	xinetd . . . . .	137
6.10.3	Fazit . . . . .	147
6.11	System-V-Init-Prozess . . . . .	147

6.12	Anpassen der Passwortdatei	153
6.13	Physikalische Sicherheit und Absicherung des Bootvorganges	155
6.14	shutdown	157
6.15	su	158
6.16	/etc/host.conf	158
6.17	/etc/services	159
6.18	Das Auffinden von worldwritable Dateien und Verzeichnissen	159
6.19	Verwaiste Dateien	160
6.20	.rhosts	160
6.21	Schutz der Systemlogfiles	160
6.22	Bastille Linux	161
6.23	Fazit	162
<b>7</b>	<b>Kernel</b>	<b>163</b>
7.1	Bezugsquellen	164
7.2	Kernelversionen	164
7.3	Sicherheitsprobleme	164
7.4	Kernelerstellung	165
7.4.1	Rettungsdiskette	165
7.4.2	Kerneloptimierung	166
7.4.3	Maximale Prozesse	166
7.4.4	Konfiguration	167
7.4.5	Kompilierung	170
7.4.6	Installation	170
7.4.7	Anpassung an einen monolithischen Kernel	172
7.5	Kernelparameter	174
<b>8</b>	<b>Sudo</b>	<b>175</b>
8.1	Bezugsquelle	176
8.2	Kompilierung und Installation	176
8.3	Konfiguration	177
8.4	Fazit	183
<b>9</b>	<b>Buffer Overflows</b>	<b>185</b>
9.1	Ausnutzung von Buffer-Overflow-Fehlern	185
9.2	Erläuterung des Buffer-Overflow-Beispiels	186
9.3	Gegenmaßnahmen I: Sichere Programmierung	189
9.3.1	ITS4	190
9.3.2	Slint	191
9.3.3	Weitere Quellen	192
9.4	Gegenmaßnahmen II: Openwall-Patch - Non-executable Stack	192
9.5	Gegenmaßnahmen III: Array-Grenzüberwachung	202
9.6	Gegenmaßnahmen IV: Immunix StackGuard-Compiler	203
9.7	Gegenmaßnahmen V: Libsafe	207
9.8	Fazit	209

## Inhalt

<b>10</b>	<b>Systemanomalien</b>	<b>211</b>
10.1	Systemanomalien der ersten Art . . . . .	212
10.2	Systemanomalien der zweiten Art . . . . .	213
10.3	Systemanomalien dritter Art . . . . .	214
<b>11</b>	<b>Computer-Würmer</b>	<b>217</b>
11.1	Geschichte der Computer-Würmer . . . . .	217
11.2	Der Morris-Wurm . . . . .	220
11.3	Fazit . . . . .	224
<b>12</b>	<b>Viren</b>	<b>225</b>
12.1	Was sind Computer-Viren? . . . . .	225
12.2	Viren unter Linux. . . . .	225
12.3	Skript-Virus. . . . .	226
12.4	Gegenmaßnahmen Teil 1. . . . .	228
12.5	Beispiel eines Linux-Virus: Der Bliss-Virus. . . . .	229
12.6	Gegenmaßnahmen Teil 2. . . . .	232
12.7	Fazit . . . . .	233
12.8	Weiterführende Links. . . . .	233
12.9	Linux als Virenfalle. . . . .	234
12.10	Anti-Viren-Software für Linux. . . . .	235
<b>13</b>	<b>Trojanische Pferde</b>	<b>237</b>
13.1	Infektion durch Trojanische Pferde. . . . .	237
13.2	Wirkungsweise. . . . .	239
13.3	Beispiele für Trojaner-Attacken. . . . .	239
13.4	Rootkits. . . . .	240
13.5	Schutz und Gegenmaßnahmen. . . . .	241
13.6	Loadable Kernel Modules. . . . .	244
	13.6.1 Funktionsweise. . . . .	245
	13.6.2 Systemcalls. . . . .	245
	13.6.3 Kernel- und Systemcall-Hintertüren. . . . .	246
	13.6.4 Schutzmaßnahmen. . . . .	248
<b>14</b>	<b>Spoofing</b>	<b>251</b>
14.1	IP-Spoofing . . . . .	251
	14.1.1 Einsatzgebiete. . . . .	253
	14.1.2 TCP-Sequenznummern-Angriff. . . . .	254
	14.1.3 Die Mitnick-Attacke. . . . .	255
	14.1.4 Fazit. . . . .	258
	14.1.5 Gegenmaßnahmen. . . . .	259
14.2	DNS-Spoofing. . . . .	265
	14.2.1 Wie funktioniert DNS-Spoofing?. . . . .	266
	14.2.2 Gegenmaßnahmen. . . . .	268
14.3	ARP-Spoofing. . . . .	268
	14.3.1 Gegenmaßnahmen. . . . .	270

14.4	RIP-Spoofing . . . . .	270
14.4.1	Gegenmaßnahmen . . . . .	271
14.5	WWW-Spoofing . . . . .	272
14.5.1	Konsequenzen . . . . .	272
14.5.2	Wie funktioniert eine Man-in-the-Middle-Attacke? . . . . .	272
14.5.3	Aufspüren des Angreifers . . . . .	274
14.5.4	Gegenmaßnahmen . . . . .	275
<b>15</b>	<b>Netzwerk-Scan-Techniken</b>	<b>277</b>
15.1	Scanning . . . . .	280
15.1.1	Online Check . . . . .	280
15.1.2	Port-Scanning . . . . .	284
15.1.3	Port-Scan-Detectoren I: Scanlogd . . . . .	287
15.1.4	Port-Scan-Detectoren II: PortSentry . . . . .	289
15.1.5	Grundsätzliche Probleme mit Port-Scan-Detectoren . . . . .	292
15.1.6	Erweiterte Port-Scan-Methoden . . . . .	294
15.2	Inverse Mapping . . . . .	297
15.3	Betriebssystemerkennung . . . . .	299
15.3.1	Klassische Methoden . . . . .	299
15.3.2	Verfügbare OS-Bestimmungsprogramme . . . . .	301
15.3.3	Spezielle Techniken der OS-Bestimmung . . . . .	302
15.3.4	Möglichkeiten gegen OS-Bestimmungssoftware . . . . .	306
15.4	Nmap . . . . .	308
15.5	Firewalking . . . . .	317
15.6	Security Scanner . . . . .	322
15.6.1	Hostbasierte Security Scanner . . . . .	323
15.6.2	Netzwerkbasierte Security Scanner . . . . .	325
15.7	Fazit . . . . .	328
<b>16</b>	<b>Sniffer</b>	<b>329</b>
16.1	Was ist überhaupt ein Sniffer? . . . . .	329
16.2	Anwendungsgebiete von Sniffern . . . . .	330
16.3	Funktionsweise von Sniffern . . . . .	330
16.4	Ethernet . . . . .	332
16.5	Die Media-Access-Control-Adresse . . . . .	333
16.6	Bezugsquellen . . . . .	334
16.7	Konkretes Beispiel . . . . .	335
16.8	Anzeichen einer Sniffer-Attacke . . . . .	336
16.9	AntiSniff . . . . .	338
16.10	Wie kann man sich vor einem Sniffer-Angriff schützen? . . . . .	340
16.11	Fazit . . . . .	344
<b>17</b>	<b>Linux und Verschlüsselung</b>	<b>345</b>
17.1	Grundlagen der Verschlüsselung . . . . .	345
17.2	Symmetrische Verschlüsselungsverfahren . . . . .	347
17.2.1	Historische Beispiele symmetrischer Verschlüsselungsverfahren . . . . .	347



## Inhalt

17.2.2	Beispiele für moderne symmetrische Verschlüsselungsalgorithmen . . . . .	355
17.3	Asymmetrische Verschlüsselungsverfahren . . . . .	359
17.3.1	Beispiele für asymmetrische Verschlüsselungsalgorithmen . . . . .	361
17.3.2	Fazit . . . . .	362
17.4	Angriffe gegen kryptographische Verfahren . . . . .	362
17.5	Weiterführende Literatur . . . . .	367
17.6	Verschlüsselungsimplementationen . . . . .	367
17.7	Secure Shell (SSH) . . . . .	368
17.7.1	SSH im Überblick . . . . .	369
17.7.2	Installation von SSH . . . . .	376
17.7.3	Konfiguration . . . . .	377
17.7.4	Benutzerdefinierte Client-Anpassung . . . . .	386
17.7.5	Funktionen und Gebrauch . . . . .	391
17.7.6	Fazit . . . . .	401
17.8	OpenSSH . . . . .	402
17.8.1	Vorbereitung der Installation . . . . .	404
17.8.2	Installation . . . . .	406
17.8.3	Konfiguration . . . . .	406
17.8.4	Benutzerdefinierte Client-Anpassung . . . . .	410
17.8.5	Funktion und Gebrauch . . . . .	411
17.8.6	Kompatibilität . . . . .	411
17.8.7	Fazit: SSH und OpenSSH . . . . .	414
17.9	OpenSSL . . . . .	415
17.10	IPSec - Internet Protocol Security . . . . .	418
17.10.1	IPSec-Implementierung . . . . .	421
17.10.2	Key Management . . . . .	424
17.10.3	Netzwerksicherheit durch IPSec . . . . .	425
17.10.4	Anwendungsgebiete von IPSec . . . . .	429
17.10.5	Freie IPSec-Implementierung für Linux . . . . .	434
17.11	Kryptographie auf Anwendungsebene: GnuPG . . . . .	437
17.12	Lokale Verschlüsselung . . . . .	439
17.12.1	Das Loopback Device . . . . .	439
17.12.2	Der International Kernel Patch . . . . .	440
17.12.3	Weitere lokale Verschlüsselungsmechanismen für Linux-Dateisysteme . . . . .	447
<b>18</b>	<b>Denial-of-Service-Attacken</b>	<b>449</b>
18.1	Hostbasierte DoS-Angriffe gegen das Linux-System . . . . .	449
18.1.1	Plattenplatz aufbrauchen . . . . .	450
18.1.2	CPU/RAM verbrauchen . . . . .	454
18.1.3	Prozessor-Fehler . . . . .	456
18.2	Netzwerkbasierte DoS-Angriffe gegen das Linux-System ..	456
18.2.1	E-Mail-Bombing . . . . .	457
18.2.2	Broadcast-Angriff . . . . .	457
18.2.3	Anfällige Kernelstrukturen . . . . .	462

18.2.4	Large-Packet-Attacks & . . . . .	465
18.2.5	Der "Slashdot-Effekt" V. . . . .	466
18.3	DoS-Attacken gegen Hardware. . . . .	466
***		
<b>19</b>	<b>Distributed-Denial-of-Service-Attacken</b>	<b>469</b>
19.1	Analyse bereits bekannter DDoS-Angriffstools. . . . .	471
19.1.1	trinoo. . . . .	471
19.1.2	TFN - Tribe Flood Network. . . . .	481
19.1.3	Stacheldraht. . . . .	485
19.1.4	Weitere DDoS-Angriffstools. . . . .	492
19.2	Anti-DDoS-Maßnahmen. . . . .	493
19.2.1	Netzwerkfilter und ISPs. . . . .	493
19.2.2	Weitere hostbasierte Anti-DDoS-Maßnahmen_____	500
19.2.3	Weitere netzwerkbasierte Anti-DDoS-Maßnahmen .	501
19.2.4	Fazit. . . . .	504
<b>20</b>	<b>Audit-Mechanismus, Logfiles und Accounting</b>	<b>505</b>
20.1	System und Kernel. . . . .	506
20.1.1	syslogd. . . . .	506
20.1.2	klogd. . . . .	515
20.1.3	Systemlogfile-Einträge auswerten. . . . .	515
20.1.4	logrotate. . . . .	517
20.1.5	Angriffe gegen Logfiles. . . . .	528
20.1.6	Schutz der Logfiles. . . . .	528
20.2	System Accounting. . . . .	537
20.2.1	Connection Accounting. . . . .	538
20.2.2	Process Accounting. . . . .	542
20.3	Fazit. . . . .	549
<b>21</b>	<b>Firewalls</b>	<b>551</b>
21.1	Theoretische Grundlagen. . . . .	551
21.1.1	Allgemeine Firewall-Mechanismen. . . . .	551
21.1.2	Schutzniveau. . . . .	552
21.1.3	Firewall-Topologien. . . . .	553
21.1.4	Firewall-Architekturen. . . . .	555
21.1.5	Zugriffskontrolle. . . . .	562
21.2	Praktischer Einsatz. . . . .	566
21.2.1	Kommerzielle Firewall-Produkte. . . . .	566
21.2.2	Verwirklichung einer Firewall unter Linux. . . . .	567
21.2.3	Linux-Firewall mit ipchains. . . . .	569
21.2.4	IP-Masquerading. . . . .	581
21.2.5	Beispiel für eine Paketfilterimplementation. . . . .	587
21.2.6	Übersicht über die Gateway- Paketfilterimplementation. . . . .	594
21.2.7	Paketfilterskript. . . . .	596
21.2.8	Installation des Paketfilterskriptes. . . . .	608
21.2.9	Proxy-Software. . . . .	615

## Inhalt

21.2.10	Freie Firewall-Toolkits	616
21.3	Fazit	617
21.4	Firewall Design Tools	618
21.5	Weiterführende Literatur	618
<b>22</b>	<b>Intrusion Detection</b>	<b>621</b>
22.1	Was ist Intrusion Detection?	622
22.2	Intrusion - Unerlaubtes Eindringen	625
22.3	IDS-Komponenten	625
22.3.1	Datensammlung	626
22.3.2	Datenanalyse	626
22.3.3	Anomaly-Detection-Intrusion-Detection-Systeme (AD-IDS)	627
22.3.4	Misuse-Detection-Intrusion-Detection-Systeme (MD-IDS)	629
22.3.5	Ergebnisdarstellung	630
22.4	Angriffstechniken und Anzeichen	631
22.5	Elemente der Systemsicherheit	633
22.6	Aspekte eines guten Intrusion-Detection-Systems	634
22.7	Fehleranfälligkeit	635
22.8	Sicherheitspolitik	636
22.9	Erkennen der Angriffsmuster	637
22.9.1	Misuse-Detection-Intrusion-Detection-Systeme	637
22.9.2	Arten von Misuse-Detection-Intrusion-Detection-Systeme	640
22.10	Burglar Alarms	642
22.11	Nutzwert eines Intrusion-Detection-Systems	644
22.12	Intrusion Response (IR) - Automatische Gegenmaßnahmen	645
22.12.1	Schäden verhindern mittels Gegenangriff	646
22.12.2	(Weitere) Schäden verhindern mittels Abschottung	647
22.12.3	Identifizierung des Angreifers	648
22.13	Arten der Misuse Detection Intrusion Detection	649
<b>23</b>	<b>Hostbasierte Intrusion Detection</b>	<b>651</b>
23.1	System Integrity Verifier (SIV)	651
23.1.1	sXid	651
23.1.2	Tripwire	655
23.2	Logfile-Analyse	669
23.2.1	logcheck	669
23.2.2	swatch	672
23.3	LIDS	675
23.3.1	Funktionsumfang	675
23.3.2	Funktionsweise	676
23.3.3	Installation	681
23.3.4	Konfiguration	687
23.3.5	Beispiel für eine konkrete Implementation	690

23.3.6	Beispiel einer Systemanpassung für den Einsatz von LIDS. . . . .	696
23.3.7	Fazit. . . . .	704
23.4	HostSentry. . . . .	705
23.5	Deception-Systeme - Honeypots. . . . .	706
<b>24</b>	<b>Netzwerkbasierte Intrusion Detection</b>	<b>713</b>
24.1	Snort. . . . .	714
24.1.1	Funktionsweise. . . . .	715
24.1.2	Konfiguration und Installation. . . . .	717
24.1.3	Snort-Optionen. . . . .	718
24.1.4	Angriffsmuster und Datenbanken - Erstellung neuer Filterregeln. . . . .	721
24.2	Konkrete Snort-Implementation. . . . .	731
24.2.1	Vorbereitungen. . . . .	732
24.2.2	Konfiguration. . . . .	734
24.2.3	Starten von Snort. . . . .	736
24.2.4	Testen von Snort. . . . .	738
24.2.5	Snort als ADS. . . . .	740
24.2.6	Auswertung. . . . .	741
24.2.7	Weiterführende Snort-Links. . . . .	742
24.3	Fazit. . . . .	742
24.4	Weiterführende Links. . . . .	742
24.5	Weiterführende Literatur. . . . .	743
<b>25</b>	<b>Sicherheitsstandards</b>	<b>745</b>
25.1	Sicherheitsbewertung. . . . .	746
25.2	Kriterienkataloge. . . . .	747
25.2.1	TCSEC. . . . .	747
25.2.2	Der ITSEC-Kriterienkatalog. . . . .	749
25.2.3	Common Criteria. . . . .	750
25.2.4	Internationale Sicherheitsinstitute und Kriterienkataloge in der Übersicht. . . . .	750
25.3	Sicherheitsbewertung eines Standard-Linux-Systems. . . . .	751
25.3.1	Vertraulichkeit von Daten. . . . .	751
25.3.2	Vertraulichkeit der Datenübermittlung. . . . .	752
25.3.3	Authentifikationsmechanismen und Zugangskontrolle. . . . .	752
25.3.4	Integrität. . . . .	753
25.3.5	Nachvollziehbarkeit, Logging. . . . .	754
25.3.6	Fazit. . . . .	754
25.4	Implementation von erweiterten Sicherheitsmodellen unter Linux. . . . .	755
25.4.1	Access Control Lists. . . . .	755
25.4.2	POSIX Access Control Lists für Linux. . . . .	757
25.4.3	Fazit. . . . .	767

## Inhalt

25.5	Weitere Projekte	767
25.5.1	RSBAC	767
25.5.2	SGL	769
25.5.3	NSA	770
<b>26</b>	<b>Notfallplan - Mögliche Reaktionen auf eine Systemkompromittierung</b>	<b>771</b>
26.1	Maßnahmen - Teil 1	772
26.2	Vertrauenswürdige Rekonstruktion	773
26.3	Maßnahmen - Teil 2	775
26.4	Praktische Rekonstruktionsmethoden	777
26.5	Nach der Rekonstruktion	780
26.6	Warum soll man Angriffe melden?	781
26.7	Wen sollte man benachrichtigen?	782
26.8	Wie und was soll berichtet werden?	782
26.9	Fazit	783
26.10	Backup	783
<b>A</b>	<b>Kernelparameter</b>	<b>787</b>
A.1	Der icmp_echo_ignore_all-Parameter	787
A.2	Der tcp_syncookies-Parameter	788
A.3	Der icmp_echo_ignore_broadcasts-Parameter	789
A.4	Der accept_source_route-Parameter	790
A.5	Der rp_filter-Parameter	791
A.6	Der always_defrag-Parameter	793
A.7	Der log_martians-Parameter	794
A.8	Der accept_redirects-Parameter	795
<b>B</b>	<b>Angriff- und Verteidigungsmatrix</b>	<b>797</b>
<b>C</b>	<b>Organisationen</b>	<b>799</b>
<b>D</b>	<b>Sicherheitsrelevante Request for Comments (RFC)</b>	<b>801</b>
<b>E</b>	<b>Sicherheitsneuigkeiten</b>	<b>807</b>
E.1	Securityportal	807
E.2	LinuxSecurity	807
E.3	Securityfocus	807
<b>F</b>	<b>Die wichtigsten sicherheitsrelevanten Mailinglisten und Newsgroups</b>	<b>809</b>
<b>G</b>	<b>Glossar</b>	<b>811</b>
<b>H</b>	<b>Literatur</b>	<b>819</b>
	<b>Index</b>	<b>823</b>