

LINUX-Sicherheits-Kochbuch

*Daniel J. Barrett, Richard E. Silverman &
Robert G. Byrnes*

*Deutsche Übersetzung von
Peter Klicman*

O'REILLY®

Beijing • Cambridge • Farnham • Köln • Paris • Sebastopol • Taipei • Tokyo

Inhalt

Vorwort	XI
System-Schnappschüsse mit Tripwire	1
1.1 Tripwire einrichten	4
1.2 Ausgabe der Policy und der Konfiguration	6
1.3 Policy und Konfiguration ändern	7
1.4 Grundlegende Integritätsprüfung	8
1.5 Leseorientierte Integritätsprüfung	9
1.6 Entfernte Integritätsprüfungen	10
1.7 Ultra-paranoide Integritätsprüfung	12
1.8 Teure, ultra-paranoide Integritätsprüfung	14
1.9 Automatisierte Integritätsprüfungen	15
1.10 Ausgabe des letzten Tripwire-Berichts	16
1.11 Aktualisierung der Datenbank	17
1.12 Dateien zur Datenbank hinzufügen	17
1.13 Dateien aus der Datenbank ausschließen	19
1.14 Windows VFAT-Dateisysteme prüfen	19
1.15 Prüfen RPM-installerter Dateien	20
1.16 Integritätsprüfung mit rsync	21
1.17 Manuelle Integritätsprüfung	22
Firewalls mit iptables und ipchains	25
2.1 Quelladress-Verifikation aktivieren	26
2.2 Sperren von ausspionierten Adressen	29
2.3 Den gesamten Netzwerkverkehr sperren	29
2.4 Eingehenden Netzwerkverkehr sperren	31
2.5 Ausgehenden Netzwerkverkehr blockieren	33
2.6 Eingehende Service-Anfragen blockieren	34
2.7 Zugriffe von einem entfernten Host sperren	34

2.8	Zugriff auf einen entfernten Port blockieren	35
2.9	Ausgehenden Zugriff auf alle Webserver eines Netzwerks blockieren . . .	36
2.10	Entfernten Zugriff blockieren, aber lokalen Zugriff erlauben	38
2.11	Zugriffskontrolle über die MAC-Adresse	39
2.12	Nur SSH-Zugriff erlauben	40
2.13	Ausgehende Telnet-Verbindungen unterbinden	41
2.14	Einen bestimmten Server schützen	42
2.15	Pings unterdrücken	42
2.16	Ausgabe der Firewall-Regeln	43
2.17	Firewall-Regeln löschen	44
2.18	Firewall-Regeln einfügen	45
2.19	Eine Firewall-Konfiguration sichern	46
2.20	Eine Firewall-Konfiguration laden	47
2.21	Eine Firewall-Konfiguration testen	49
2.22	Aufbau komplexer Regel-Bäume	50
2.23	Das Logging vereinfachen	51
	Zugriffskontrolle im Netz	53
3.1	Ausgabe Ihrer Netzwerkschnittstellen	56
3.2	Die Netzwerkschnittstelle aktivieren und deaktivieren	57
3.3	Aktivieren/Deaktivieren eines Dienstes (xinetd)	58
3.4	Aktivieren/Deaktivieren eines Dienstes (inetd)	59
3.5	Neue Dienste einbinden (xinetd)	60
3.6	Neue Dienste einbinden (inetd)	61
3.7	Den Zugriff auf bestimmte entfernte Benutzer beschränken	62
3.8	Den Zugriff auf bestimmte entfernte Hosts beschränken (xinetd)	63
3.9	Den Zugriff auf bestimmte entfernte Hosts beschränken (xinetd mit libwrap)	65
3.10	Den Zugriff auf bestimmte entfernte Hosts beschränken (xinetd mit tcpd)	66
3.11	Den Zugriff auf bestimmte entfernte Hosts beschränken (inetd)	67
3.12	Tageszeit-bezogene Zugriffsbeschränkungen	68
3.13	Zugriffe auf einen SSH-Server auf bestimmte Hosts beschränken	69
3.14	Zugriffe auf einen SSH-Server auf bestimmte Accounts beschränken	70
3.15	Dienste auf bestimmte Verzeichnisse des Dateisystems beschränken	71
3.16	Denial-of-Service-Angriffe verhindern	73
3.17	Umleitung an einen anderen Socket	75
3.18	Protokollieren von Zugriffen auf Ihre Dienste	76
3.19	Root-Logins über Terminals unterbinden	77

Authentifizierungstechniken und Infrastrukturen.79
4.1 Entwicklung PAM-fähiger Anwendungen.	81
4.2 Starke Passwörter erzwingen mit PAM.	83
4.3 Zugriffskontrolllisten mit PAM erzeugen.	84
4.4 Validierung eines SSL-Zertifikats.	86
4.5 Dekodierung eines SSL-Zertifikats.	87
4.6 Installation eines neuen SSL-Zertifikats.	88
4.7 Generierung eines SSL-CSRs (Certificate Signing Requests).	89
4.8 Ein selbst signiertes SSL-Zertifikat erzeugen.	91
4.9 Eine Certifying Authority einrichten.	92
4.10 SSL-Zertifikate von DER in PEM umwandeln.	95
4.11 Einführung in Kerberos.	96
4.12 Benutzer zu einem Kerberos-Bereich hinzufügen.	101
4.13 Hosts zu einem Kerberos-Bereich hinzufügen.	102
4.14 Kerberos mit SSH nutzen.	103
4.15 Kerberos mit Telnet verwenden.	106
4.16 IMAP mit Kerberos absichern.	108
4.17 Kerberos mit PAM zur systemweiten Authentifizierung nutzen.	109
Autorisierung.113
5.1 Eine Root-Login-Shell ausführen.	115
5.2 X-Programme als root ausführen.	116
5.3 Befehle mittels sudo unter einem anderen Benutzer ausführen.	117
5.4 Die Passwort-Authentifizierung bei sudo umgehen.	118
5.5 Passwort-Authentifizierung in sudo erzwingen.	119
5.6 Host-basierte sudo-Autorisierung.	120
5.7 Rechte über sudo an Benutzergruppen vergeben.	121
5.8 Ausführung beliebiger Programme innerhalb eines Verzeichnisses über sudo.	122
5.9 Kommandoargumente mit sudo unterbinden.	122
5.10 Gemeinsame Nutzung von Dateien über Gruppen.	123
5.11 Eine gemeinsam genutzte Datei über sudo auf Leserechte beschränken .	124
5.12 Autorisierung von Passwort-Änderungen mittels sudo.	125
5.13 Daemons über sudo starten und anhalten.	126
5.14 Die root-Fähigkeiten mit sudo einschränken.	127
5.15 Prozesse über sudo beenden.	128
5.16 sudo-Aufrufe ausgeben.	129
5.17 sudo-Aufrufe entfernt protokollieren.	130
5.18 Root-Rechte über SSH teilen.	130
5.19 Root-Befehle über SSH ausführen.	132
5.20 Root-Rechte mit Kerberos-su teilen.	133

Ausgehende Netzwerkverbindungen schützen.137
6.1 Auf einem entfernten Rechner einloggen.138
6.2 Entfernte Programme ausführen139
6.3 Kopieren entfernter Dateien.140
6.4 Authentifizierung mittels Public Key (OpenSSH).142
6.5 Authentifizierung mittels Public Key (OpenSSH-Client, SSH2-Server, OpenSSH-Schlüssel).145
6.6 Authentifizierung mittels Public Key (OpenSSH-Client, SSH2-Server, SSH2-Schlüssel).146
6.7 Authentifizierung mittels Public Key (SSH2-Client, OpenSSH-Server) . .	.148
6.8 Authentifizierung über vertrauenswürdigen Host (Trusted Host).149
6.9 Authentifizierung ohne Passwort (interaktiv).152
6.10 Authentifizierung in cron-Jobs.154
6.11 Einen SSH-Agenten beim Ausloggen beenden.156
6.12 Host-orientierte Anpassung von SSH.157
6.13 Standardvorgaben des SSH-Clients ändern.158
6.14 Andere TCP-Sessions durch SSH tunneln.159
6.15 Passwörter nachhalten.160
Dateien schützen.163
7.1 Datei-Zugriffsrechte verwenden165
7.2 Schutz eines gemeinsam genutzten Verzeichnisses.165
7.3 Verzeichnis-Listing unterdrücken.166
7.4 Dateien mit einem Passwort verschlüsseln.167
7.5 Entschlüsselung von Dateien.169
7.6 Public Key-Verschlüsselung bei GnuPG einrichten.169
7.7 Ausgabe Ihres Keyrings.172
7.8 Einen Standard-Schlüssel festlegen.172
7.9 Gemeinsame Nutzung öffentlicher Schlüssel.174
7.10 Schlüssel in Ihren Keyring aufnehmen.175
7.11 Dateien für andere verschlüsseln.175
7.12 Signieren einer Textdatei.176
7.13 Signieren und Verschlüsseln von Dateien.177
7.14 Erzeugen einer separaten Signaturdatei.178
7.15 Prüfen einer Signatur.179
7.16 Ausgabe von Public Keys.179
7.17 Einen privaten Schlüssel sichern.180
7.18 Verzeichnisse verschlüsseln.182
7.19 Ihren Schlüssel in einen Keyserver aufnehmen.183
7.20 Neue Signaturen auf einen Keyserver hochladen.183
7.21 Schlüssel von einem Keyserver abrufen.184

7.22	Einen Schlüssel widerrufen	186
7.23	Verschlüsselte Dateien mit Emacs verwalten	188
7.24	Verschlüsselte Dateien mit vim verwalten	188
7.25	Backups verschlüsseln	190
7.26	PGP-Schlüssel mit GnuPG verwenden	191
E-Mail schützen		193
8.1	Verschlüsselte Mail mit Emacs	194
8.2	Verschlüsselte Mail mit vim	196
8.3	Verschlüsselte Mail mit Pine	196
8.4	Verschlüsselte Mail mit Mozilla	198
8.5	Verschlüsselte Mail mit Evolution	199
8.6	Verschlüsselte Mail mit mutt	199
8.7	Verschlüsselte Mail mit elm	200
8.8	Verschlüsselte Mail mit MH	201
8.9	Einen POP/IMAP-Mailserver mit SSL betreiben	202
8.10	Eine SSL Mail-Verbindung testen	207
8.11	POP/IMAP mit SSL und Pine sichern	208
8.12	POP/IMAP mit SSL und mutt sichern	209
8.13	POP/IMAP mit SSL und Evolution schützen	210
8.14	POP/IMAP mit stunnel und SSL sichern	211
8.15	POP/IMAP mit SSH sichern	213
8.16	POP/IMAP mit SSH und Pine sichern	214
8.17	Mail mit einem »unsichtbaren« Server empfangen	217
8.18	Einen SMTP-Server von beliebigen Clients nutzen	218
Testen und überwachen		223
9.1	Testen von Login-Passwörtern (John the Ripper)	224
9.2	Testen von Login-Passwörtern (CrackLib)	226
9.3	Accounts ohne Passwort ermitteln	227
9.4	Superuser-Accounts aufspüren	228
9.5	Accounts auf verdächtige Nutzung untersuchen	229
9.6	Accounts bei mehreren Systemen auf verdächtige Nutzung untersuchen	230
9.7	Test Ihres Suchpfads	233
9.8	Dateisysteme effizient durchsuchen	234
9.9	setuid- oder setgid-Programme finden	238
9.10	Gerätedateien schützen	240
9.11	Schreibbare Dateien aufspüren	241
9.12	Nach Rootkits suchen	242
9.13	Nach offenen Ports suchen	243

9.14	Lokale Netzwerk-Aktivitäten untersuchen	249
9.15	Tracing von Prozessen.	255
9.16	Netzwerk-Traffic beobachten.	257
9.17	Netzwerk-Traffic beobachten (GUI).	263
9.18	Netzwerk-Traffic nach Strings durchsuchen	265
9.19	Unsichere Netzwerk-Protokolle erkennen	268
9.20	Einstieg in Snort.	273
9.21	Packet-Sniffing mit Snort	275
9.22	Mit Snort Einbrüche erkennen	276
9.23	Snort-Alarm-Meldungen verstehen.	278
9.24	Logging mit Snort	280
9.25	Snort-Logs in separate Dateien aufteilen	282
9.26	Den Regelsatz von Snort aktualisieren und optimieren.	283
9.27	System-Meldungen in Log-Dateien umleiten (syslog).	284
9.28	Eine syslog-Konfiguration testen.	288
9.29	Logging auf entfernten Rechnern.	289
9.30	Log-Dateien rotieren.	291
9.31	Meldungen an den System-Logger senden.	291
9.32	Log-Einträge über Shell-Skripten schreiben.	293
9.33	Log-Einträge mit Perl schreiben.	295
9.34	Log-Einträge mit C schreiben.	296
9.35	Log-Dateien kombinieren.	297
9.36	Logs mit logwatch zusammenfassen.	299
9.37	Einen logwatch-Filter definieren.	301
9.38	Überwachung aller ausgeführten Befehle.	302
9.39	Ausgabe aller ausgeführten Befehle.	304
9.40	Parsing des Prozess-Accounting-Logs.	306
9.41	Sich von einem Hack »erholen«.	308
9.42	Einen »Incident Report« ausfüllen.	309
	Index.	313