

Inhaltsverzeichnis

Vorwort	23
Einführung	25
I Was ist ein MAC und warum brauchen wir das?	27
1 Computersicherheit	29
1.1 Übersicht	29
1.2 Anfänge der Computersicherheit	30
2 Access Control Systeme	33
2.1 DAC-, MAC- und RBAC-Systeme	33
2.1.1 Discretionary Access Control (DAC)	33
2.1.2 Mandatory Access Control (MAC)	33
2.1.3 Multi Level Security	34
2.1.4 Multilateral Security	35
2.1.5 Role Based Access Control (RBAC)	37
2.2 Type Enforcement	37
2.3 Linux-Capabilitys	38
2.3.1 Was ist eine Capability?	38
2.3.2 Welche Capabilitys existieren?	39
2.3.3 Wie setzt man die Capabilitys ein?	42
2.3.4 Filesystem-Capabilitys	43
2.4 Alternative MAC-Systeme	45
2.5 Linux Intrusion Detection System (LIDS)	45
2.5.1 GetRewted Security (grsecurity)	46
2.5.2 RuleSet Based Access Control (RSBAC)	48
3 Benchmarks	51
3.1 Novell AppArmor	51
3.2 SELinux	52

II AppArmor	55
4 AppArmor-Geschichte	57
5 AppArmor-Anwendung	59
5.1 Installation unter SUSE Linux	59
5.2 Starten von AppArmor	60
5.2.1 Welche Prozesse werden überwacht?	61
5.3 Analyse der Protokolle	62
5.4 AppArmor-Benachrichtigungen und -Berichte	64
5.4.1 Executive Summary Report	66
5.4.2 Applications Audit	66
5.4.3 Security Incident Report	66
5.5 Erzeugen eines Profils mit Yast	66
5.6 Erzeugen eines Subprofils (Hat) mit Yast	72
6 AppArmor-Funktion	79
6.1 Was sollte immunisiert werden?	79
6.1.1 Netzwerkdienste	80
6.1.2 Netzwerkclients	80
6.1.3 Cron-Jobs	81
6.2 Wie schützt AppArmor?	81
6.3 AppArmor-Befehle	82
6.3.1 <code>apparmor_status</code>	82
6.3.2 <code>audit</code>	83
6.3.3 <code>autodep</code>	84
6.3.4 <code>complain</code>	84
6.3.5 <code>enforce</code>	85
6.3.6 <code>genprof</code>	85
6.3.7 <code>logprof</code>	87
6.3.8 <code>apparmor_parser</code>	90
6.3.9 <code>unconfined</code>	92

- 6.4 AppArmor-Konfigurationsdateien 93
 - 6.4.1 logprof.conf 93
 - 6.4.2 subdomain.conf 95
 - 6.4.3 reports.conf 96
 - 6.4.4 severity.db 96
 - 6.4.5 reports.crontab 96
- 6.5 AppArmor-Syntax 96
 - 6.5.1 Kommentare 96
 - 6.5.2 Include-Direktiven 97
 - 6.5.3 Profil 97
 - 6.5.4 Regel 97
 - 6.5.5 Variablen 99
 - 6.5.6 Capabilities 99
- 6.6 Abstractions 99
- 7 AppArmor-Installation 101**
 - 7.1 Ubuntu und Debian 101
 - 7.2 Installation aus den Sourcen 102
- 8 AppArmor für Fortgeschrittene 105**
 - 8.1 Erzeugen der Log-Markierung für logprof 105
 - 8.2 ChangeHat 106
 - 8.2.1 Apache 2.0 und mod_apparmor 106
 - 8.2.2 PAM und pam_apparmor 108
 - 8.3 Einzelne Benutzer mit unterschiedlichen Profilen 113
- 9 Typische AppArmor-Administrationsvorgänge 119**
 - 9.1 Weiteres Cacheverzeichnis für den Squid-Proxy 119
 - 9.2 Eine neue PHP-Anwendung für den Apache 120
 - 9.3 VirtualHosts mit Apache 121
 - 9.4 Überwachung von Snort mit AppArmor 125

9.5	Überwachung von Shellscrip	127
9.6	Modifikation eines Profils ohne Neustart der überwachten Applikation	129
10	Kritische Betrachtung von AppArmor	131
10.1	Geschwindigkeit	131
10.2	Sicherheit	131
III	SELinux für Einsteiger	135
11	Hintergrund	137
11.1	Geschichte	137
11.2	Architektur	138
11.2.1	Access-Vector-Cache	139
12	SELinux-Grundlagen	141
12.1	Was ist SELinux?	141
12.2	Der Security-Context: SELinux-Benutzer, -Rollen und -Typen	141
12.3	Type Enforcement am Beispiel: Squid	143
12.4	Welche Ressource erhält welchen Context?	145
12.5	Das klassische Beispiel: passwd	146
12.5.1	Domänentransition	148
12.6	Rollen und Benutzer	149
12.7	Multi Level Security	151
12.8	Multi Category Security	153
13	SELinux-Anwendung	155
13.1	Distributionen	155
13.1.1	Fedora Core	155
13.1.2	Debian und Ubuntu	156
13.1.3	Gentoo	156
13.1.4	Slackware	156

- 13.2 Welche SELinux-Policy? 156
- 13.3 Erste Schritte und SELinux-Befehle 157
- 14 SELinux-Protokollmeldungen 163**
- 15 SELinux und boolesche Variablen 171**
 - 15.1 Administration der booleschen Variablen 175
- 16 SELinux-Anpassungen 179**
 - 16.1 Verwaltung der SELinux-Benutzer 179
 - 16.2 Verwaltung der Ports 180
 - 16.3 Verwaltung der Security-Contexts der Dateien 180
 - 16.4 Customizable Types 181
 - 16.5 Erweiterung der Policy 182
- 17 Policies 189**
 - 17.1 Die Targeted-Policy 189
 - 17.1.1 Deaktivierung von SELinux für einzelne Applikationen 190
 - 17.1.2 Die booleschen Variablen der Targeted-Policy 190
 - 17.1.3 Schutz zusätzlicher Applikationen mit SELinux 190
 - 17.2 Die Strict-Policy 191
 - 17.2.1 Was unterscheidet die Strict-Policy? 191
 - 17.2.2 Die booleschen Variablen der Strict-Policy 193
 - 17.2.3 Schutz zusätzlicher Applikationen mit SELinux 193
 - 17.2.4 Neue Rollen zur Delegation der Root-Fähigkeiten 193
 - 17.3 Die MLS-Policy 193
 - 17.3.1 Labeling der Objekte 194
 - 17.3.2 MLS in der Praxis 195
- 18 SELinux-Kommandos 197**
 - 18.1 apol 197
 - 18.2 avcstat 198
 - 18.3 audit2allow 198

18.4	auditwhy	200
18.5	chcat	200
18.6	chcon	201
18.7	checkmodule	201
18.8	checkpolicy	202
18.9	fixfiles	202
18.10	genhomedircon	203
18.11	getenforce	203
18.12	getsebool	203
18.13	load_policy	204
18.14	matchpathcon	204
18.15	newrole	204
18.16	restorecon	205
18.17	run_init	206
18.18	sealert	206
18.19	seaudit	207
18.20	seaudit-report	208
18.21	sediff	208
18.22	sediffx	208
18.23	seinfo	209
18.24	selinuxenabled	209
18.25	semanage	209
18.25.1	SELinux-User-Verwaltung	212
18.25.2	Hinzufügen neuer Dateien	213
18.25.3	Verwaltung der Netzwerk-Ports	213
18.26	semodule	214
18.27	semodule_expand	216
18.28	semodule_link	216
18.29	semodule_package	216
18.30	sesearch	217
18.31	sestatus	218

18.32	setenforce	219
18.33	setfiles	220
18.34	setsebool	220
18.35	setroubleshootd	221
18.36	system-config-securitylevel	222
18.37	togglesebool	222
19	Typische SELinux-Administrationsaufgaben	223
19.1	Abschalten von SELinux	223
19.2	Abschalten von SELinux für einen Dienst	224
19.3	Erneutes Labeln des Betriebssystems	225
19.4	Programme in unconfined_t funktionieren nicht	225
19.5	KDE-Programme	226
19.6	Start eines Dienstes mit ungewöhnlichem Port	227
19.7	Verwendung einer SWAP-Datei	228
19.8	Apache Webserver	228
19.8.1	Neues DocumentRoot-Verzeichnis	228
19.8.2	Gleichzeitiger Zugriff per FTP, Samba etc.	229
19.8.3	Zugriff auf eine MySQL-Datenbank	230
19.9	Sicherung (Backup)	230
20	Analyse mit apol	231
20.1	Policy-Components	232
20.2	Policy-Rules	232
20.3	File Contexts	233
20.4	Analysis	233
21	SELinux-Update	235
22	SELinux-Installation	239
22.1	Fedora Core	239
22.2	Debian Etch	240

23 Sicherer Betrieb eines Webservers mit FastCGI und SELinux	245
23.1 FastCGI mit mod_fcgid	247
23.1.1 Konfiguration des Apache und mod_fcgid	248
23.2 SuExec und mod_fcgid	252
23.3 SELinux und mod_fcgid	254
23.4 Geschwindigkeit von mod_fcgid und SELinux	257
IV SELinux-Policy-Entwicklung	259
24 Die erste eigene Policy	261
24.1 Start	262
24.2 Domänen und Typen	263
24.3 File-Contexts	265
24.4 Übersetzung	265
24.5 Laden der Policy und Labeln der Dateien	266
24.6 Test und Analyse der Fehlermeldungen	267
24.7 Policy mit Require-Block	270
24.8 Policy unter Zugriff auf die Schnittstellen	272
24.9 Setzen der Uhrzeit erlauben	278
24.10 Ist die Policy nun fertig?	279
24.11 Interface	280
24.12 Fazit	281
25 Boolesche Variablen	283
25.1 Überblick	283
25.2 Operatoren	284
25.3 Booleans und Interfaces	284
25.4 Praktische Anwendung bei unserer date-Policy	284
26 Policy für einen Netzwerkdienst	287
26.1 Installation von HAVP	287
26.2 Erzeugung der Policy	288
26.3 Verzicht auf run_init	295

27	Labeln von Objekten	297
27.1	Labeling von Dateien	297
27.1.1	Labeling mit xattrs	299
27.1.2	Task-basiertes Labeling	301
27.1.3	Transitionsbasiertes Labeling	302
27.1.4	Generelles Labeling	302
27.2	Labeling von Netzwerkobjekten	303
27.2.1	Netzwerkkarten	303
27.2.2	IP-Adressen	304
27.2.3	Ports	304
27.2.4	IP-Pakete	305
27.2.5	Security-Associations	305
27.3	Labeling weiterer Objekte	306
27.3.1	Socket	306
27.3.2	System V IPC	306
27.3.3	Capability	306
27.3.4	Prozess	306
27.3.5	System und Security	307
28	Entwicklung unter der Strict-Policy	309
28.1	Der Befehl date	309
28.2	Ein Modul für die Targeted- und Strict-Policy	312
28.3	Weitere Rollen zur Delegation	313
29	Die komplett eigene Policy	317
30	SELinux-Policy-Editoren und -IDES	321
30.1	Vim als SELinux-Editor	321
30.2	SELinux Policy IDE (SLIDE)	321
30.2.1	SLIDE-Installation	322
30.2.2	SLIDE-Funktionen	322
30.3	SELinux Policy Editor (SEedit)	328

30.3.1	Simplified Policy Description Language (SPDL)	328
30.3.2	SEedit-Installation	330
30.4	Cross Domain Solutions Framework (CDS Framework)	330
30.4.1	CDS-Konzept	331
V	Ältere SELinux-Implementierungen	333
31	Die Example-Policy	335
31.1	Struktur der Example-Policy	335
31.2	Anpassung und Entwicklung von eigenen Regeln	336
VI	SELinux-Zukunft	337
32	SELinux Policy Management Server	339
32.1	Installation	340
32.1.1	Anpassung der Policy	340
32.1.2	Anwendung des Policy Management Servers	341
32.1.3	Erlauben der Policy-Verwaltung	343
32.2	Fazit	344
33	SELinux-erweitertes XWindow	345
34	SELinux-Symposium	347
VII	Anhänge	349
A	Auditd-Daemon	351
A.1	Zertifizierungen nach Common Criteria	351
A.2	auditd	352
A.3	auditctl	355
A.4	aureport	357
A.5	ausearch	359
A.6	autrace	360

- B Profile für den Benchmark 361**
 - B.1 AppArmor-Profil für den Benchmark 361
 - B.2 SELinux-Richtlinie für den Benchmark 365

- C Ergebnisse des LMBench 369**
 - C.1 AppArmor 369
 - C.2 SELinux 370

- Literaturverzeichnis 373**

- Stichwortverzeichnis 375**