

# Inhaltsverzeichnis

<b>I</b>	<b>Authentifikation am System</b>	<b>6</b>
<b>1</b>	<b>PAM — austauschbare Authentifizierungsverfahren</b>	<b>7</b>
1.1	Überblick . . . . .	7
1.2	Konfiguration des PAM-Systems . . . . .	9
1.2.1	Konfiguration der PAM-fähigen Anwendungen . . . . .	9
1.2.2	Austausch des Authentifizierungsverfahrens . . . . .	14
1.3	Wissensfragen . . . . .	18
1.4	Übungen . . . . .	21
1.5	Lösungen . . . . .	22
<b>2</b>	<b>LDAP Directory Server</b>	<b>25</b>
2.1	Einführung . . . . .	25
2.1.1	Directory-Clients und -Server . . . . .	26
2.1.2	Allgemeine Begriffe . . . . .	27
2.1.3	<i>LDAP</i> und <i>X.500</i> . . . . .	27
2.2	Überblick LDAP-Modelle . . . . .	28
2.3	Das Informationsmodell - Objekte und Attribute . . . . .	29
2.4	Das Namensmodell . . . . .	37
2.4.1	Der Namensraum des Directory Information Tree (DIT) . . . .	37
2.4.2	Verteiltes Directory — Partitionierung des Verzeichnisbaumes	39
2.4.3	LDAP URLs . . . . .	45
2.5	Das Funktionsmodell . . . . .	46
2.5.1	Suchfilter . . . . .	47
2.5.2	Directory-Operationen . . . . .	48
2.6	Das Sicherheitsmodell . . . . .	49
2.6.1	TLS-Konfiguration . . . . .	50
2.6.2	SASL-Konfiguration . . . . .	50
2.6.3	Access Control Lists . . . . .	50
2.7	Das LDAP-Data-Interchange-Format ( <i>LDIF</i> ) . . . . .	52

## INHALTSVERZEICHNIS

---

2.8	Installation und Konfiguration des OpenLDAP-Servers . . . . .	53
2.8.1	Konfigurieren des LDAP-Servers . . . . .	54
2.9	LDAP-Clients und Hilfsprogramme . . . . .	59
2.10	LDAP-Replikation mit <b>slapd</b> und <b>slurpd</b> . . . . .	64
2.10.1	Replikation konfigurieren . . . . .	65
2.10.2	Umgang mit Replikationsfehlern . . . . .	67
2.11	Wissensfragen . . . . .	69
2.12	Übungen . . . . .	73
2.13	Lösungen . . . . .	74
2.14	Querverweise . . . . .	76
 <b>II Firewall und Security</b>		<b>77</b>
 <b>3 Host-Security</b>		<b>78</b>
3.1	Buffer Overflow . . . . .	79
3.2	Die <i>tmp-race</i> -Problematik . . . . .	80
3.3	Gegenmaßnahmen . . . . .	80
3.3.1	<i>SUID</i> -Programme entschärfen . . . . .	81
3.3.2	Sonderfall Dateirechte bei der SuSE-Distribution . . . . .	82
3.4	Dämonen . . . . .	83
3.4.1	Der <b>[x]inetd</b> . . . . .	83
3.4.2	Startskripte . . . . .	85
3.5	Physikalischer Zugriff . . . . .	86
3.5.1	Sicherheitsloch Bootmanager . . . . .	86
 <b>4 SSH: Sicherer Zugriff auf entfernte Rechner</b>		<b>91</b>
4.1	Das SSH-Protokoll . . . . .	92
4.2	Den SSH-Client verwenden . . . . .	95
4.2.1	<b>ssh</b> . . . . .	95
4.2.2	<b>scp</b> . . . . .	97
4.2.3	<b>sftp</b> . . . . .	98
4.3	Den SSH-Server <b>sshd</b> administrieren . . . . .	100

4.3.1	Wichtige Dateien . . . . .	100
4.3.2	Die Konfiguration von <b>sshd</b> . . . . .	102
4.3.3	Die Konfiguration von <b>ssh</b> . . . . .	106
4.4	Weitergehende Anwendungen für SSH . . . . .	107
4.4.1	Varianten zur Authentifizierung . . . . .	107
4.4.2	Tunneln von TCP/IP-Protokollen . . . . .	111
4.4.3	Tunneln des X-Server Protokolls . . . . .	112
4.5	Fehlersuche . . . . .	112
4.6	SSH-Clients für Windows und MacOS . . . . .	113
4.7	Das Wichtigste in Kürze . . . . .	114
4.8	Wissensfragen . . . . .	116
4.9	Lösungen . . . . .	118
4.10	Übungen . . . . .	119
4.11	Lösungen . . . . .	120
<b>5</b>	<b>Netzwerkmonitore und Fehlerdiagnose</b>	<b>123</b>
5.1	Diagnose-Werkzeuge . . . . .	123
5.1.1	<b>mii-tool</b> . . . . .	123
5.1.2	<b>ethtool</b> . . . . .	123
5.1.3	<b>arp</b> . . . . .	124
5.1.4	Das <b>ping</b> -Kommando . . . . .	126
5.1.5	<b>traceroute</b> . . . . .	129
5.1.6	<b>mtr</b> . . . . .	132
5.1.7	<b>netstat</b> . . . . .	133
5.1.8	<b>lsof</b> . . . . .	136
5.2	Netzwerkmonitore . . . . .	137
5.2.1	<b>wireshark</b> . . . . .	138
5.2.2	<b>tcpdump</b> . . . . .	139
5.2.3	<b>iptraf</b> . . . . .	140
5.2.4	<b>ntop</b> . . . . .	141
5.3	Security-Tools . . . . .	142
5.3.1	Port-Scanning mit <b>nmap</b> . . . . .	142

## INHALTSVERZEICHNIS

---

5.3.2	Schwachstellen-Analyse mit OpenVAS . . . . .	144
5.4	Übungen . . . . .	147
5.5	Lösungen . . . . .	148
5.6	Querverweise . . . . .	149
<b>6</b>	<b>TCP/IP-Dienste konfigurieren</b>	<b>151</b>
6.1	Ports, Sockets und die Datei /etc/services . . . . .	151
6.2	Server mit eigenem Startskript . . . . .	153
6.3	Der Internet-Dämon ( <b>x</b> ) <b>inetd</b> und der TCP-Wrapper . . . . .	156
6.3.1	<b>xinetd</b> — der Internet-Super-Server . . . . .	156
6.3.2	<b>inetd</b> – Der Internet Super-Server . . . . .	158
6.3.3	Der TCP-Wrapper . . . . .	160
6.4	Wissensfragen . . . . .	162
6.5	Übungen . . . . .	165
6.6	Lösungen . . . . .	166
<b>7</b>	<b>Iptables (Netfilter)</b>	<b>169</b>
7.1	Grundlagen . . . . .	169
7.2	Regeln erstellen und bearbeiten . . . . .	172
7.3	Erweiterungen . . . . .	176
7.3.1	Negieren von Merkmalen . . . . .	176
7.3.2	Flags im TCP-Header . . . . .	176
7.3.3	ICMP-Pakete . . . . .	177
7.3.4	Eigene Regellisten . . . . .	179
7.3.5	Filtern nach der MAC-Adresse . . . . .	180
7.3.6	Limits setzen . . . . .	180
7.4	Stateful Inspection . . . . .	181
7.5	Network Address Translation . . . . .	181
7.6	Masquerading als spezielle Form des NAT . . . . .	183
7.7	Skripte, Konfigurationstools . . . . .	185
7.7.1	Ein Beispielskript . . . . .	185
7.7.2	Weitere Befehle . . . . .	186

7.8	Wissensfragen . . . . .	188
7.9	Lösungen . . . . .	191
<b>8</b>	<b>Intrusion Detection Systeme</b>	<b>193</b>
8.1	IDS: Alarmanlagen im Netz . . . . .	193
8.2	Spurensuche im Dateisystem: <b>tripwire</b> . . . . .	193
8.2.1	Installation . . . . .	194
8.3	Einfaches IDS mit <b>ipchains/iptables</b> . . . . .	199
8.4	IDS mit <b>snort</b> . . . . .	199
8.4.1	Installation . . . . .	200
8.4.2	Falscher Alarm . . . . .	201
8.4.3	Alte Bekannte: Angriffe aus der Trickkiste . . . . .	203
8.4.4	Fallensteller . . . . .	204
8.4.5	Analyse mittels <b>snortsnarf.pl</b> . . . . .	205
8.5	Übungen . . . . .	207
8.6	Querverweise . . . . .	208
<b>III</b>	<b>Anhang</b>	<b>209</b>
<b>C</b>	<b>Die LPI-Prüfung 202</b>	<b>233</b>
C.1	Details für die Prüfung 202 . . . . .	234
C.2	Beispiels-Prüfungsaufgaben für das Examen 202 . . . . .	248
<b>B</b>	<b>Literaturhinweise</b>	<b>229</b>
<b>C</b>	<b>Die LPI-Prüfung 202</b>	<b>233</b>
C.1	Details für die Prüfung 202 . . . . .	234
C.2	Beispiels-Prüfungsaufgaben für das Examen 202 . . . . .	248
<b>D</b>	<b>Stichwortverzeichnis</b>	<b>251</b>