

Inhaltsverzeichnis

I	Authentifikation am System	6
1	PAM — austauschbare Authentifizierungsverfahren	7
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
2	LDAP Directory Server	25
2.1	Einführung	25
2.1.1	Directory-Clients und -Server	26
2.1.2	Allgemeine Begriffe	27
2.1.3	LDAP und X.500	27
2.2	Überblick LDAP-Modelle	29
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	40
2.4.3	LDAP URLs	45
2.5	Das Funktionsmodell	46
2.5.1	Suchfilter	48
2.5.2	Directory-Operationen	49
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>)	53

2.8	Installation und Konfiguration des OpenLDAP-Servers	54
2.8.1	Konfigurieren des LDAP-Servers	54
2.9	LDAP-Clients und Hilfsprogramme	59
2.10	LDAP-Replikation mit slapd und slurpd	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
II	Firewall und Security	77
3	Host-Security	78
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 [x]inetd	83
3.4.2	Startskripte	85
3.5	Physikalischer Zugriff	86
3.5.1	Sicherheitsloch Bootmanager	86
4	SSH: Sicherer Zugriff auf entfernte Rechner	91
4.1	Das SSH-Protokoll	92
4.2	Den SSH-Client verwenden	95
4.2.1	ssh	95
4.2.2	scp	97
4.2.3	sftp	98
4.3	Den SSH-Server sshd administrieren	100

4.3.1	Wichtige Dateien	100
4.3.2	Die Konfiguration von sshd	102
4.3.3	Die Konfiguration von ssh	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
5	Netzwerkmonitore und Fehlerdiagnose	123
5.1	Diagnose-Werkzeuge	123
5.1.1	mii-tool	123
5.1.2	ethtool	123
5.1.3	arp	124
5.1.4	Das ping -Kommando	126
5.1.5	tracert	129
5.1.6	mtr	132
5.1.7	netstat	133
5.1.8	lsof	136
5.2	Netzwerkmonitore	137
5.2.1	Wireshark	138
5.2.2	tcpdump	139
5.2.3	iptraf	140
5.2.4	ntop	141
5.3	Security-Tools	142
5.3.1	Port-Scanning mit nmap	142

5.3.2	Schwachstellen-Analyse mit OpenVAS	144
5.4	Übungen	147
5.5	Lösungen	148
5.6	Querverweise	149
6	TCP/IP-Dienste konfigurieren	151
6.1	Ports, Sockets und die Datei /etc/services	151
6.2	Server mit eigenem Startskript	153
6.3	Der Internet-Dämon (x) inetd und der TCP-Wrapper	156
6.3.1	xinetd — der Internet-Super-Server	156
6.3.2	inetd – Der Internet Super-Server	158
6.3.3	Der TCP-Wrapper	160
6.4	Wissensfragen	162
6.5	Übungen	165
6.6	Lösungen	166
7	Iptables (Netfilter)	169
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
8	Intrusion Detection Systeme	193
8.1	IDS: Alarmanlagen im Netz	193
8.2	Spurensuche im Dateisystem: tripwire	193
8.2.1	Installation	194
8.3	Einfaches IDS mit ipchains/iptables	199
8.4	IDS mit snort	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 snortsnarf.pl	205
8.5	Übungen	207
8.6	Querverweise	208
III	Anhang	209
C	Die LPI-Prüfung 202	229
C.1	Details für die Prüfung 202	230
B	Literaturhinweise	225
C	Die LPI-Prüfung 202	229
C.1	Details für die Prüfung 202	230
D	Stichwortverzeichnis	243