

## Inhaltsverzeichnis

<b>I Grundlagen zur Systemsicherheit</b>	<b>4</b>
<b>1 Verschlüsselte Kommunikation im Internet</b>	<b>5</b>
1.1 Methoden zur Verschlüsselung von Daten . . . . .	5
1.2 Schlüssel und Zertifikate . . . . .	9
1.3 Beispiele für Verschlüsselung . . . . .	11
1.3.1 Pretty Good Privacy, (PGP) . . . . .	11
1.3.2 Secure Socket Layer, (SSL) . . . . .	15
1.3.3 <b>stunnel</b> . . . . .	15
1.3.4 SSH . . . . .	17
1.4 Wissensfragen . . . . .	20
<b>2 SSH: Sicherer Zugriff auf entfernte Rechner</b>	<b>21</b>
2.1 Das SSH-Protokoll . . . . .	22
2.2 Den SSH-Client verwenden . . . . .	25
2.2.1 <b>ssh</b> . . . . .	25
2.2.2 <b>scp</b> . . . . .	27
2.2.3 <b>sftp</b> . . . . .	28
2.3 Den SSH-Server <b>sshd</b> administrieren . . . . .	30
2.3.1 Wichtige Dateien . . . . .	30
2.3.2 Die Konfiguration von <b>sshd</b> . . . . .	32
2.3.3 Die Konfiguration von <b>ssh</b> . . . . .	36
2.4 Weitergehende Anwendungen für SSH . . . . .	37
2.4.1 Varianten zur Authentifizierung . . . . .	37
2.4.2 Tunneln von TCP/IP-Protokollen . . . . .	41
2.4.3 Tunneln des X-Server Protokolls . . . . .	42
2.5 Fehlersuche . . . . .	42
2.6 SSH-Clients für Windows und MacOS . . . . .	43
2.7 Das Wichtigste in Kürze . . . . .	44
2.8 Wissensfragen . . . . .	46

## INHALTSVERZEICHNIS

---

2.9	Lösungen . . . . .	48
2.10	Übungen . . . . .	49
2.11	Lösungen . . . . .	50
<b>3</b>	<b>Host-Security</b>	<b>53</b>
3.1	Buffer Overflow . . . . .	54
3.2	Die <i>tmp-race</i> -Problematik . . . . .	55
3.3	Gegenmaßnahmen . . . . .	55
3.3.1	<i>SUID</i> -Programme entschärfen . . . . .	56
3.3.2	Sonderfall Dateirechte bei der SuSE-Distribution . . . . .	57
3.4	Dämonen . . . . .	58
3.4.1	Der [ <b>x</b> ] <i>inetd</i> . . . . .	58
3.4.2	Startskripte . . . . .	60
3.5	Physikalischer Zugriff . . . . .	61
3.5.1	Sicherheitsloch Bootmanager . . . . .	61
<b>4</b>	<b>Zuweisen von Festplattenquota</b>	<b>67</b>
4.1	Wissensfragen . . . . .	70
4.2	Übungen . . . . .	73
4.3	Lösungen . . . . .	74
<b>5</b>	<b>Firewall und Masquerading</b>	<b>75</b>
5.1	Übersicht über verschiedene Firewall-Architekturen . . . . .	75
5.1.1	Screening Router oder Paketfilter . . . . .	75
5.1.2	Dual-Homed-Gateway oder Proxy-Server . . . . .	76
5.1.3	Kombinierte Architektur mit demilitarisierter Zone . . . . .	76
5.2	Paketfilter mit <b>ipchains</b> . . . . .	78
5.3	<i>ipchains</i> -Handwerkszeug für Einsteiger . . . . .	81
5.3.1	Benutzerdefinierte Regellisten . . . . .	81
5.3.2	Regeln hinzufügen und entfernen . . . . .	82
5.3.3	Paketeigenschaften angeben . . . . .	83
5.3.4	Sprungziele festlegen . . . . .	84

## INHALTSVERZEICHNIS

---

5.3.5	mögliche Sprungziele . . . . .	84
5.3.6	Einige nützliche Werkzeuge für chains . . . . .	85
5.4	Anwendungsbeispiel . . . . .	86
5.5	Paketfilter mit <b>iptables</b> . . . . .	107
5.5.1	Unterschiede zwischen <b>ipchains</b> und <b>iptables</b> . . . . .	107
5.5.2	Stateful-Inspection-Firewall für Ungeduldige . . . . .	109
5.5.3	Stateful-Inspection-Firewall mit DMZ für Ungeduldige . . . . .	110
5.6	Suche nach offenen Ports mit <b>nmap</b> , Einsatz von <b>netstat</b> . . . . .	112
5.6.1	Einsatz von <b>nmap</b> . . . . .	112
5.6.2	Einsatz von <b>netstat</b> . . . . .	113
5.7	Übungen . . . . .	114
<b>II</b>	<b>Anhang</b>	<b>115</b>
<b>A</b>	<b>Die LPI-Prüfung 102</b>	<b>116</b>
A.1	Details für die Prüfung 102 (Allgemeines Linux, Teil II) . . . . .	117
A.2	Beispiels-Prüfungsaufgaben für das Examen 102 . . . . .	132
<b>B</b>	<b>Literaturhinweise</b>	<b>137</b>
<b>C</b>	<b>Stichwortverzeichnis</b>	<b>141</b>