

Inhaltsverzeichnis

1	Host-Security	5
1.1	Buffer Overflow	6
1.2	Die <i>tmp-race</i> -Problematik	7
1.3	Gegenmaßnahmen	7
1.3.1	<i>SUID</i> -Programme entschärfen	8
1.3.2	Sonderfall Dateirechte bei der SuSE-Distribution	9
1.4	Dämonen	10
1.4.1	Der [x]inetd	10
1.4.2	Startskripte	12
1.5	Physikalischer Zugriff	13
1.5.1	Sicherheitsloch Bootmanager	13
2	Verschlüsselte Kommunikation im Internet	19
2.1	Methoden zur Verschlüsselung von Daten	19
2.2	Schlüssel und Zertifikate	23
2.3	Beispiele für Verschlüsselung	25
2.3.1	Pretty Good Privacy, (PGP)	25
2.3.2	Secure Socket Layer, (SSL)	29
2.3.3	OpenSSL	29
2.3.4	stunnel	34
2.3.5	SSH	36
2.4	Wissensfragen	39
3	SSH: Sicherer Zugriff auf entfernte Rechner	41
3.1	Das SSH-Protokoll	42
3.2	Den SSH-Client verwenden	45
3.2.1	ssh	45
3.2.2	scp	47
3.2.3	sftp	48
3.3	Den SSH-Server sshd administrieren	50

INHALTSVERZEICHNIS

3.3.1	Wichtige Dateien	50
3.3.2	Die Konfiguration von sshd	52
3.3.3	Die Konfiguration von ssh	56
3.4	Weitergehende Anwendungen für SSH	57
3.4.1	Varianten zur Authentifizierung	57
3.4.2	Tunneln von TCP/IP-Protokollen	61
3.4.3	Tunneln des X-Server Protokolls	62
3.5	Fehlersuche	62
3.6	SSH-Clients für Windows und MacOS	63
3.7	Das Wichtigste in Kürze	64
3.8	Wissensfragen	66
3.9	Lösungen	68
3.10	Übungen	69
3.11	Lösungen	70
4	Virtual Private Networks (VPN)	73
4.1	Was ist ein VPN?	73
4.2	Grundlagen: tun/tap	77
4.3	Ein einfaches Szenario mit shared secret	78
4.4	Ein Produktions-Szenario mit Public-Key-Infrastruktur	81
4.5	Wissensfragen	91
4.6	Übungen	93
5	Firewall und Masquerading	95
5.1	Vorüberlegungen	95
5.2	Übersicht über verschiedene Firewall-Architekturen	97
5.2.1	Screening Router oder Paketfilter	97
5.2.2	Dual-Homed-Gateway oder Proxy-Server	98
5.2.3	Kombinierte Architektur mit demilitarisierter Zone	99
6	Iptables (Netfilter)	103
6.1	Grundlagen	103

6.2	Regeln erstellen und bearbeiten	106
6.3	Erweiterungen	110
6.3.1	Negieren von Merkmalen	110
6.3.2	Flags im TCP-Header	110
6.3.3	ICMP-Pakete	111
6.3.4	Eigene Regellisten	113
6.3.5	Filtern nach der MAC-Adresse	114
6.3.6	Limits setzen	114
6.4	Stateful Inspection	115
6.5	Network Address Translation	115
6.6	Masquerading als spezielle Form des NAT	117
6.7	Skripte, Konfigurationstools	119
6.7.1	Ein Beispielskript	119
6.7.2	Weitere Befehle	120
6.8	Wissensfragen	122
6.9	Lösungen	125
7	Der Proxy Squid	127
7.1	squid , ein Konfigurationsmonster?	127
7.2	Zugriffskonzept/ACLs	128
7.2.1	ACLs	128
7.2.2	Die <code>http_access</code> -Direktive	130
7.3	Minimalkonfiguration	130
7.4	Client-Konfiguration	131
7.5	Webseiten sperren	132
7.6	Zugriffszeiten definieren	132
7.7	Feintuning/Anpassung an die lokalen Gegebenheiten	133
7.8	Familienbande: squid mit Parents und Siblings	134
7.9	Transparent Proxy	135
7.10	Querverweise	137
7.11	Übungen	139
7.12	Lösungen	140

INHALTSVERZEICHNIS

8 Firewall mit DMZ und Proxy	141
8.1 Wofür eine DMZ?	141
8.2 Routing	142
8.3 iptables -Regeln für Server in der DMZ	143
8.4 iptables -Regeln für den Proxy squid	143
9 Firewall mit DMZ und Masquerading	147
9.1 Grundaufbau	147
9.2 Masquerading-Regeln für die DMZ	147
9.3 Öffentlicher Server mit Portumleitung	148
10 Fallstudie: Firewallscenario mit DMZ	151
10.1 Szenario	151
10.1.1 Firma Winzigweich	151
10.1.2 Die Firma Hugehard	153
10.2 Übungen	157
10.3 Lösungen	158
11 Stichwortverzeichnis	165