

Inhaltsverzeichnis

I. Vorwort10

KAPITEL 1: Kryptographie

1.1 OpenSSL.....14

 1.1.1 SSL/TLS14

 1.1.2 Zertifizierungsstelle (CA)16

 1.1.3 PKCS#12 Zertifikate19

 Fragen zu 1.121

1.2. GPG.....25

 1.2.1 Konfiguration.....25

 1.2.2 gpg-Befehle27

 1.2.3 Signaturüberprüfung.....30

 Fragen zu 1.231

1.3. Verschlüsselte Dateisysteme35

 1.3.1 dm-crypt.....36

 1.3.2 dm-crypt mit LUKS37

 1.3.3 Cryptmount39

 Fragen zu 1.339

KAPITEL2: Zugriffskontrolle

2.1 Hostbasierte Zugriffskontrolle44

 2.1.1 TCP-Wrapper44

 2.1.2 nsswitch.....47

 2.1.3 PAM48

 2.1.4 john52

Fragen zu 2.1	54
2.2 Erweiterte Attribute und Zugriffskontrolllisten	60
2.2.1 Erweiterte Attribute	60
2.2.2 Access Control Lists	63
Fragen zu 2.2	64
2.3 SELinux	69
2.3.1 Überblick	69
2.3.2 Type Enforcement	70
2.3.3 Policies und Module	72
2.3.4 Konfiguration	73
2.3.5 SELinux Befehle	75
2.3.6 SELinux PAM-Module	76
2.3.7 Zusammenfassung	77
Fragen zu 2.3	78
2.4 Andere obligatorische Zugriffssicherungssysteme	84
2.4.1 Smack	84
2.4.2 AppArmor	86
Fragen zu 2.4	88

KAPITEL 3: Sicherheit der Dienste

3.1 BIND/DNS	94
3.1.1 TSIG	95
3.1.2 DNSSEC	97
3.1.3 Bind und ACLs	102
3.1.4 Bind chroot	103
Fragen zu 3.1	105
3.2 E-maildienste	111
3.2.1 Postfix	111
3.2.1.1 main.cf	111

3.2.1.2 SASL	113
3.2.1.3 master.cf	117
3.2.2 Proxymap	118
3.2.3 Sendmail	119
Fragen zu 3.2	121
3.3 Apache/HTTP/HTTPS	126
3.3.1 Sicherheitsüberlegungen	126
3.3.2 httpd.conf	127
3.3.3 .htaccess	129
3.3.4 Apache2 und chroot	132
3.3.5 Apache2 mit SSL/TLS	135
Fragen zu 3.3	137
3.4. FTP	143
3.4.1 Vsftpd	144
3.4.1.1 Konfiguration	144
3.4.1.2 Upload Verzeichnis	145
3.4.1.3 Chroot	145
3.4.1.4 Virtuelle Benutzer	146
3.4.1.5 Benutzerlisten	147
3.4.2 PureFTPd	148
3.4.2.1 Konfiguration	148
3.4.2.2 Pure-FTPd und SSL/TLS	151
Fragen zu 3.4	151
3.5. OpenSSH	156
3.5.1 Einführung	156
3.5.2 Dateien, Einstellungen und Befehle	157
3.5.3 Forwarding mit SSH	162

- Fragen zu 3.5163
- 3.6 NFSv4.....168
 - 3.6.1 Einführung.....168
 - 3.6.2. Installation171
 - 3.6.3 Kerberos172
 - 3.6.4 NFSv4 mit Kerberos-Authentifizierung174
- Fragen zu 3.6.....177
- 3.7 Syslog.....182
 - Fragen zu 3.7187

KAPITEL 4: Operative Sicherheit / Host-Konfigurationsmanagement

- 4.1 RCS (Revisions-Kontrollsystem).....192
- 4.2 Puppet195
 - 4.2.1 Einführung.....196
 - 4.2.2 Manifeste199
 - 4.2.3 Puppet-ACLs202
- Fragen zu 4.1 und 4.2.....204

KAPITEL 5: Netzwerksicherheit

- 5.1 Erkennen von Eindringlingen210
 - 5.1.1 Snort.....210
 - 5.1.1.1 Einführung.....210
 - 5.1.1.2 NIDS Modus (Einbrucherkennung).....212
 - 5.1.1.3 Inline-Modus213
 - 5.1.1.4 Snort Regeln214
 - 5.1.1.5 Präprozessoren216

5.1.1.5 Includes	217
5.1.2 Tripwire	218
5.1.2.1 Komponenten von Tripwire	219
5.1.2.2 Regeln.....	219
5.1.2.2 Befehle	222
Fragen zu 5.1	225
5.2 Netzwerk-Sicherheitsüberprüfung.....	230
5.2.1 Nessus/NASL	230
5.2.1.1 Einführung.....	230
5.2.1.2 nmap	232
5.2.1.3 Konfiguration von Nessus	233
5.2.1.4 Nessus-Client und Plug-Ins.....	236
5.2.1.5 Honeypots	237
5.2.1.6 Buffer-Overflows.....	238
5.2.1.7 NASL (Nessus Attack Scripting Language)	239
5.2.2 Wireshark	239
5.2.2.1 Protokolle	240
5.2.2.2 TCP-Header	242
5.2.2.3 Capture-Filter	243
5.2.2.4 Anzeigefilter	245
Fragen zu 5.2	247
5.3 Netzwerkbeobachtung.....	252
5.3.1 Nagios.....	252
5.3.1.1 Einführung.....	252
5.3.1.2 Konfiguration.....	254

5.3.1.3 Objekte	254
5.3.1.4 Nagios Plug-Ins	255
5.3.1.5 Hosts und Benachrichtigungen	256
5.3.1.6 Nagios Dienste	257
5.3.1.7 Log-Einstellungen	258
5.3.1.8 Externe Befehle	258
5.3.1.9 Nagios Statistiken	259
5.3.2 ntop	261
Fragen zu 5.3	263
5.4 Netzfilter	269
5.4.1 NAT	269
5.4.2 transparente Firewall	273
5.4.3 Filter	274
Fragen zu 5.4	275
5.5 OpenVPN	280
5.5.1 Zertifikate	280
5.5.2 Serverkonfiguration	281
5.5.3 Clientkonfiguration	283
5.5.4 Das VPN-Netzwerk	284
Fragen zu 5.5	287
III Anhang	294
Vokabeltraining	294
Index	298