

# Inhalt

Credits .....	XI
Vorwort .....	XVII
<b>Kapitel 1. Unix-Host-Sicherheit .....</b>	<b>1</b>
1. Sichern Sie Mount-Punkte ab	2
2. Suchen Sie nach SUID- und SGID-Programmen	4
3. Suchen Sie nach Verzeichnissen mit globalen und Gruppen-Schreibrechten	5
4. Erstellen Sie flexible Berechtigungshierarchien mit POSIX-ACLs	6
5. Schützen Sie Ihre Protokolle vor Verfälschung	10
6. Delegieren Sie administrative Rollen	12
7. Automatisieren Sie die Überprüfung kryptografischer Signaturen	14
8. Überprüfen Sie lauschende Dienste	17
9. Verhindern Sie, dass sich Dienste an ein Interface binden	20
10. Schränken Sie Dienste mit einer Sandbox-Umgebung ein	22
11. Verwenden Sie proftpd mit einer MySQL-Authentifizierungsquelle	27
12. Verhindern Sie Stack-Smashing-Angriffe	30
13. Verriegeln Sie Ihren Kernel mit grsecurity	32
14. Schränken Sie Anwendungen mit grsecurity ein	38
15. Schränken Sie Systemaufrufe mit systrace ein	40
16. Automatisierte Systrace-Regelerstellung	45
17. Kontrollieren Sie den Login-Zugriff mit PAM	47
18. Beschränken Sie Benutzer auf SCP und SFTP	52

19. Verwenden Sie Einmalpasswörter für die Authentifizierung	56
20. Eingeschränkte Shell-Umgebungen	59
21. Erzwingen Sie Ressourcenbeschränkungen für Benutzer und Gruppen	61
22. Automatisieren Sie System-Aktualisierungen	63
<b>Kapitel 2. Windows-Host-Sicherheit</b> . . . . .	<b>66</b>
23. Überprüfen Sie Server auf eingespielte Patches	67
24. Verwenden Sie Gruppenrichtlinien, um automatische Updates zu konfigurieren	72
25. Erstellen Sie eine Liste mit geöffneten Dateien und den Prozessen, die sie besitzen	76
26. Listen Sie laufende Dienste und offene Ports auf	77
27. Aktivieren Sie die Überwachung	79
28. Zählen Sie die automatisch ausgeführten Programme	80
29. Sichern Sie Ihre Ereignisprotokolle ab	82
30. Ändern Sie Ihre maximalen Protokolldateigrößen	83
31. Sichern und löschen Sie die Ereignisprotokolle	85
32. Deaktivieren Sie Standardfreigaben	88
33. Verschlüsseln Sie Ihren Temp-Ordner	89
34. EFS sichern	91
35. Leeren Sie die Auslagerungsdatei beim Herunterfahren	99
36. Prüfen Sie auf Passwörter, die niemals ungültig werden	100
<b>Kapitel 3. Privatsphäre und Anonymität</b> . . . . .	<b>103</b>
37. Gehen Sie Traffic-Analysen aus dem Weg	103
38. Tunneln Sie SSH durch Tor	107
39. Verschlüsseln Sie Ihre Dateien lückenlos	109
40. Schützen Sie sich vor Phishing	113
41. Benutzen Sie das Web mit weniger Passwörtern	118
42. Verschlüsseln Sie Ihre E-Mails mit Thunderbird	120
43. Verschlüsseln Sie Ihre E-Mails in Mac OS X	126
<b>Kapitel 4. Firewalls</b> . . . . .	<b>130</b>
44. Firewall mit Netfilter	131
45. Firewall mit OpenBSD-PacketFilter	135
46. Schützen Sie Ihren Computer mit der Windows-Firewall	143
47. Schließen Sie offene Ports und blockieren Sie Protokolle	152
48. Ersetzen Sie die Windows-Firewall	154
49. Erzeugen Sie ein Gateway mit Benutzerauthentifizierung	162

50. Sichern Sie Ihr Netzwerk ab	165
51. Testen Sie Ihre Firewall	167
52. MAC-Filter mit Netfilter	170
53. Blockieren Sie Tor	172
<b>Kapitel 5. Verschlüsseln und Sichern von Diensten</b> . . . . .	<b>175</b>
54. IMAP und POP mit SSL verschlüsseln	176
55. Benutzen Sie SMTP/TLS in Kombination mit Sendmail	178
56. Benutzen Sie TLSSMTP mit Qmail	181
57. Installieren Sie Apache mit SSL und suEXEC	183
58. Sichern Sie BIND	188
59. Richten Sie einen einfachen, aber sicheren DNS-Server ein	191
60. Sichern Sie MySQL ab	195
61. Sichere Dateifreigaben in Unix	198
<b>Kapitel 6. Netzwerksicherheit</b> . . . . .	<b>203</b>
62. Entdecken Sie ARP-Spoofing	204
63. Erstellen Sie eine statische ARP-Tabelle	206
64. Schützen Sie sich vor SSH-Brute-Force-Angriffen	209
65. Täuschen Sie Software zur entfernten Betriebssystemerkennung	211
66. Machen Sie eine Bestandsaufnahme Ihres Netzwerks	215
67. Scannen Sie Ihr Netzwerk auf Schwachstellen	218
68. Halten Sie Ihre Server-Uhren synchron	229
69. Erzeugen Sie Ihre eigene Zertifizierungsstelle	231
70. Verteilen Sie Ihre CA an Clients	235
71. Sichern und Wiederherstellen einer Zertifizierungsstelle mit Zertifikatdiensten	237
72. Entdecken Sie Ethernet-Sniffer aus der Ferne	246
73. Helfen Sie dabei, Angreifer zu verfolgen	252
74. Scannen Sie auf Ihren Unix-Servern nach Viren	254
75. Verfolgen Sie Schwachstellen	259
<b>Kapitel 7. Sicherheit von Drahtlossystemen</b> . . . . .	<b>262</b>
76. Verwandeln Sie Ihre herkömmlichen Drahtlos-Router in eine ausgeklügelte Sicherheitsplattform	263
77. Verwenden Sie eine ausgeklügelte Authentifizierung für Ihr drahtloses Netzwerk	267
78. Ein Captive Portal einrichten	271

<b>Kapitel 8. Protokollierung</b> .....	<b>277</b>
79. Betreiben Sie einen zentralen syslog-Server	278
80. Steuern Sie syslog	280
81. Integrieren Sie Windows in Ihre Syslog-Infrastruktur	282
82. Fassen Sie Ihre Protokolle automatisch zusammen	290
83. Überwachen Sie Ihre Protokolle automatisch	292
84. Vereinigen Sie Protokolle von entfernten Sites	295
85. Protokollieren Sie die Benutzeraktivität mit Prozess-Accounting	301
86. Überwachen Sie die Sicherheitslage Ihrer Server zentral	303
<b>Kapitel 9. Monitoring und Trending</b> .....	<b>311</b>
87. Überwachen Sie die Verfügbarkeit	312
88. Stellen Sie Trends grafisch dar	321
89. Echtzeitstatistiken aus dem Netzwerk	323
90. Sammeln Sie mit Firewall-Regeln Statistiken	326
91. Durchschnüffeln Sie das Ethernet von einem entfernten Ort aus	328
<b>Kapitel 10. Sichere Tunnel</b> .....	<b>332</b>
92. Richten Sie IPsec unter Linux ein	333
93. Richten Sie IPsec unter FreeBSD ein	337
94. Richten Sie IPsec in OpenBSD ein	341
95. Verschlüsseln Sie den Datenverkehr automatisch mit Openswan	346
96. Weiterleiten und Verschlüsseln des Datenverkehrs mit SSH	348
97. Automatisieren Sie Logins mit SSH-Client-Schlüsseln	350
98. Squid Proxy über SSH	353
99. Setzen Sie SSH als SOCKS-Proxy ein	355
100. Verschlüsseln und tunneln Sie Datenverkehr mit SSL	358
101. Tunneln Sie Verbindungen innerhalb von HTTP	361
102. Tunneln Sie mit VTun und SSH	363
103. Automatische Generierung von VTun-Konfigurationen	369
104. Erstellen Sie ein plattformübergreifendes VPN	374
105. Tunneln Sie PPP	381

<b>Kapitel 11. Netzwerk-Intrusion-Detection</b> .....	<b>384</b>
106. Entdecken Sie Einbrüche mit Snort	385
107. Gehen Sie Alarmmeldungen nach	390
108. Echtzeitüberwachung des IDS	394
109. Verwalten Sie ein Sensor-Netzwerk	401
110. Schreiben Sie Ihre eigenen Snort-Regeln	409
111. Verhindern Sie mit Snort_inline Einbrüche oder dämpfen Sie diese damit ein	416
112. Automatischer Firewall-Einsatz gegen Angreifer mit SnortSam	420
113. Stellen Sie ungewöhnliches Verhalten fest	424
114. Aktualisieren Sie automatisch die Regeln von Snort	425
115. Schaffen Sie ein Netzwerk mit verteilten und getarnten Sensoren	428
116. Verwenden Sie Snort in Hochleistungsumgebungen mit Barnyard	430
117. Erkennen und verhindern Sie Einbrüche über Web-Anwendungen	433
118. Scannen Sie den Netzwerkverkehr auf Viren	438
119. Täuschen Sie ein Netzwerk mit verwundbaren Hosts vor	443
120. Zeichnen Sie Honeypot-Aktivitäten auf	450
<b>Kapitel 12. Wiederherstellung und Reaktion auf Vorfälle</b> .....	<b>457</b>
121. Erstellen Sie ein Image gemounteter Dateisysteme	457
122. Überprüfen Sie die Dateiintegrität und finden Sie kompromittierte Dateien	460
123. Finden Sie kompromittierte Pakete	465
124. Scannen Sie nach Rootkits	468
125. Ermitteln Sie den Eigentümer eines Netzwerks	471
<b>Index</b> .....	<b>475</b>