

Inhaltsverzeichnis

	Vorwort	9
I	Einleitung	11
I.1	Notwendigkeit von Penetrationstests	11
I.2	Organisatorische Einbettung	12
I.3	Prinzipielle Vorgehensweise	13
I.4	Grenzen von Penetrationstests	14
I.5	Klassifizierung von Penetrationstests	15
2	Vorbereitung eines Penetrationstests	21
2.1	Organisatorische Fragen	21
2.2	Rechtlicher Rahmen	29
2.3	Technische Werkzeuge	35
2.4	Planung des Ablaufs	41
2.5	Checklisten	42
3	Suche nach Sicherheitslücken	45
3.1	Allgemeine Informationsbeschaffung	45
3.2	Pingsweep, Portscanner und Bannertexte	51
3.3	Fingerprinting	64
3.4	Security-Scanner	68
3.5	Netzwerk-Sniffer	72
3.6	Dokumentation des Zwischenstands	75
3.7	Recherche nach Sicherheitslücken und Tools	75
3.8	Checklisten	80
4	Schwachstellen und Angriffsmöglichkeiten	83
4.1	Pufferüberlauf	83
4.2	Eingabe von Sonderzeichen	89
4.3	Race-Condition	92
4.4	Symbolische Links	94
4.5	Accounts	96

4.6	Verschlüsselung	100
4.7	Missgebildete Netzwerkpakete	104
4.8	Belastungstests	119
4.9	Man-in-the-Middle	121
5	Bericht und Präsentation	133
5.1	Aufbau des Berichts	133
5.2	Präsentation	139
6	Penetrationstest von Windows-Systemen	141
6.1	Potenzielle Schwachstellen	141
6.2	Informationsbeschaffung und Analyse des Ist-Zustands	148
6.3	Strategien für Angriffe	153
6.4	Tools	156
6.5	Checklisten	160
7	Penetrationstest von Unix-Systemen	163
7.1	Potenzielle Schwachstellen	163
7.2	Informationsbeschaffung und Analyse des Ist-Zustands	170
7.3	Strategien für Angriffe	171
7.4	Tools	176
7.5	Checklisten	178
8	Penetrationstest von Mailservern	181
8.1	Potenzielle Schwachstellen	181
8.2	Informationsbeschaffung und Analyse des Ist-Zustands	182
8.3	Strategien für Angriffe	183
8.4	Tools	185
8.5	Checklisten	187
9	Penetrationstest von DNS-Servern	189
9.1	Potenzielle Schwachstellen	189
9.2	Informationsbeschaffung und Analyse des Ist-Zustands	191
9.3	Strategien für Angriffe	192
9.4	Tools	192
9.5	Checklisten	194

10	Penetrationstest von Webservern	197
10.1	Potenzielle Schwachstellen	197
10.2	Informationsbeschaffung und Analyse des Ist-Zustands	205
10.3	Strategien für Angriffe	210
10.4	Tools	220
10.5	Checklisten	228
11	Penetrationstest von Firewalls	233
11.1	Potenzielle Schwachstellen	233
11.2	Informationsbeschaffung und Analyse des Ist-Zustands	233
11.3	Strategien für Angriffe	237
11.4	Tools	238
11.5	Checklisten	238
12	Penetrationstest von Routern	241
12.1	Potenzielle Schwachstellen	241
12.2	Informationsbeschaffung und Analyse des Ist-Zustands	244
12.3	Strategien für Angriffe	245
12.4	Tools	246
12.5	Checklisten	247
13	Penetrationstest von VPNs	249
13.1	Potenzielle Schwachstellen	249
13.2	Informationsbeschaffung und Analyse des Ist-Zustands	250
13.3	Strategien für Angriffe	257
13.4	Tools	258
13.5	Checklisten	259
14	Penetrationstest von WLANs	261
14.1	Potenzielle Schwachstellen	261
14.2	Informationsbeschaffung und Analyse des Ist-Zustands	263
14.3	Strategien für Angriffe	264
14.4	Tools	266
14.5	Checklisten	267

15	Penetrationstest von Lotus Notes	269
15.1	Potenzielle Schwachstellen	269
15.2	Informationsbeschaffung und Analyse des Ist-Zustands	271
15.3	Strategien für Angriffe	271
15.4	Tools	273
15.5	Checklisten	273
16	Social Engineering	275
16.1	Potenzielle Schwachstellen	275
16.2	Informationsbeschaffung und Analyse des Ist-Zustands	276
16.3	Strategien für Angriffe	277
16.4	Checklisten	279
17	Schlusswort und Ausblick	281
A	Informationsquellen im Internet	283
A.1	Durchführung von Penetrationstests	283
A.2	Informationsbeschaffung	284
A.3	Netzwerk-Protokolle	284
A.4	Datenbanken zur Identifikation von Sicherheitslücken	286
A.5	Externe Penetrationstests	288
B	Tools	289
B.1	Informationsbeschaffung	289
B.2	Security-Scanner	289
B.3	Netzwerk-Sniffer	290
B.4	Passwort-Prüfprogramme	291
B.5	Tools zum Test auf Sicherheitslücken	292
	Stichwortverzeichnis	299