

# Einstieg in Ethical Hacking

Penetration Testing & Hacking-Tools  
für die IT-Security

# DAS INHALTS- VERZEICHNIS

» Hier geht's  
direkt  
zum Buch

# Inhaltsverzeichnis

Einleitung.....	13
<b>Teil 1 Grundlagen des Ethical Hackings</b> .....	<b>17</b>
<b>1 Was ist (Ethical) Hacking?</b> .....	<b>19</b>
1.1 Begriffserklärung.....	19
1.2 Was ist ein Hacker?.....	20
1.3 Hackertypen und deren Motivation.....	21
1.3.1 Black Hats.....	22
1.3.2 White Hats oder Ethical Hacker.....	22
1.3.3 Grey Hats.....	22
1.3.4 Script Kiddies.....	22
1.3.5 Blue Team & Red Team.....	23
1.4 Die Rolle des Ethical Hackers.....	23
1.4.1 Hacker-Ethik.....	26
1.4.2 Ethical Hacking vs. Auditierung.....	27
1.5 Wie werde ich ein Hacker oder eine Hackerin?.....	28
1.6 Informationen zu den Tools sammeln.....	29
1.7 Richtlinien, Compliance und regulatorische Aspekte.....	30
1.8 Warum sich selbst hacken?.....	31
1.9 Vorgehensweise und Methodik im Ethical Hacking.....	32
1.10 Gefahren verstehen.....	34
1.10.1 Nicht-technische Angriffe.....	35
1.10.2 Angriffe auf das Netzwerk.....	35
1.10.3 Angriffe auf Betriebssysteme.....	35
1.11 Zusammenfassung.....	36
<b>2 Betriebssysteme für Hacker</b> .....	<b>37</b>
2.1 Kali Linux.....	37
2.2 Backbox.....	37
2.3 Parrot OS.....	38
2.4 BlackArch.....	39
2.5 Deft Linux.....	40
2.6 Pentoo Linux.....	40
2.7 CAINE.....	41
2.8 Fedora Security Spin.....	42
2.9 Zusammenfassung.....	43

<b>3</b>	<b>Vorbereitung des Betriebssystems</b> . . . . .	<b>45</b>
3.1	Kali-Linux-Installation . . . . .	45
	3.1.1 Herunterladen des ISO-Images. . . . .	45
	3.1.2 Kopieren des Images auf ein bootfähiges Medium . . . . .	46
3.2	Stand-Alone-Installation . . . . .	50
	3.2.1 Partitionierung der Festplatte . . . . .	56
	3.2.2 Konfigurieren des Package Managers (apt) . . . . .	59
	3.2.3 GRUB-Bootloader installieren . . . . .	61
	3.2.4 Installation abschließen und neu starten . . . . .	63
3.3	Kali Linux als virtuelle Maschine . . . . .	63
	3.3.1 Installation von VirtualBox . . . . .	63
	3.3.2 Kali Linux als virtuelle Maschine. . . . .	65
<b>4</b>	<b>(Kali-)Linux-Grundlagen</b> . . . . .	<b>71</b>
4.1	Was ist Linux? . . . . .	71
4.2	Hardwaresteuerung . . . . .	73
4.3	Vereinheitlichtes Dateisystem. . . . .	74
4.4	Prozessverwaltung . . . . .	75
4.5	Die Kommandozeile (Command Line) . . . . .	76
	4.5.1 Wie komme ich zur Kommandozeile? . . . . .	76
	4.5.2 Verzeichnisbaum durchsuchen und Dateien verwalten . . . . .	77
	4.5.3 Umgebungsvariablen . . . . .	79
4.6	Das Dateisystem von Kali . . . . .	79
	4.6.1 Dateisystem-Hierarchie-Standard . . . . .	79
	4.6.2 Das Home-Verzeichnis des Anwenders . . . . .	80
4.7	Rechtmanagement . . . . .	81
	4.7.1 Benutzerkategorien und Rechte . . . . .	82
	4.7.2 Rechte verwalten . . . . .	83
4.8	Hilfreiche Befehle für die Kommandozeile . . . . .	85
	4.8.1 Anzeigen und Ändern von Text-Dateien. . . . .	85
	4.8.2 Suche nach Dateien und innerhalb von Dateien . . . . .	86
	4.8.3 Prozesse verwalten . . . . .	86
	4.8.4 Systeminformationen und Logs aufrufen. . . . .	87
	4.8.5 Hardware erkennen . . . . .	88
4.9	Dienste . . . . .	89
	4.9.1 Init-Systeme . . . . .	89
	4.9.2 Starten und Beenden von Diensten. . . . .	89
	4.9.3 Auffinden und Ablegen von Diensten . . . . .	90
	4.9.4 Deaktivieren von Diensten. . . . .	90
4.10	Zusammenfassung . . . . .	90

<b>5</b>	<b>Erste Schritte &amp; Hacking-Labor einrichten mit Kali Linux. . . . .</b>	<b>91</b>
5.1	Erste Schritte mit Kali Linux. . . . .	91
5.1.1	Verwalten von Diensten in Kali Linux . . . . .	91
5.1.2	Übung macht den Meister: Hacking-Labor einrichten . . . . .	94
5.2	Installation von Tools und Updates . . . . .	97
5.2.1	(Kali) Linux updaten. . . . .	97
5.2.2	OpenVAS zur Schwachstellenanalyse. . . . .	97
5.2.3	Dns2proxy. . . . .	101
<b>6</b>	<b>Einführung in Security-Assessments. . . . .</b>	<b>103</b>
6.1	Was bedeutet »Sicherheit« im Umgang mit Informationssystemen? . . . . .	103
6.2	Arten von Assessments. . . . .	105
6.2.1	Schwachstellenanalyse . . . . .	107
6.2.2	Compliance-Test. . . . .	112
6.2.3	Traditioneller Penetrationstest . . . . .	113
6.2.4	Applikations-Assessment. . . . .	115
6.3	Normierung der Assessments . . . . .	117
6.4	Arten von Attacks . . . . .	118
6.4.1	Denial of Service (DoS) . . . . .	118
6.4.2	Speicherbeschädigungen . . . . .	119
6.4.3	Schwachstellen von Webseiten . . . . .	120
6.4.4	Passwort-Attacks . . . . .	121
6.4.5	Clientseitige Angriffe . . . . .	121
6.5	Zusammenfassung . . . . .	122
<b>7</b>	<b>Einführung in Programmierung &amp; Shell-Skripte . . . . .</b>	<b>125</b>
7.1	Programmiersprachen für Ethical Hacking . . . . .	125
7.2	Programmieren mit Python . . . . .	127
7.2.1	Erste Befehle . . . . .	128
7.2.2	Datentypen und Variablen. . . . .	129
7.2.3	Bedingte Anweisungen (Verzweigungen) . . . . .	132
7.2.4	Schleifen . . . . .	133
7.3	Bash-Skripte . . . . .	135
7.3.1	Skript ausführbar und verfügbar machen . . . . .	137
7.3.2	Ausgaben und Variablen . . . . .	138
7.3.3	Schleifen in Skripten . . . . .	139
7.4	Zusammenfassung . . . . .	141

**Teil 2 Durchführung von Penetrationstests** 143

<b>8</b>	<b>Der Penetrationstest</b> . . . . .	145
8.1	Umfang des Penetrationstests (Scope) . . . . .	149
8.1.1	Umfang des Projekts definieren . . . . .	150
8.1.2	Metriken für die Zeitschätzung . . . . .	151
8.1.3	Zusätzlicher Support und Scope Creep . . . . .	152
8.2	Fragen zur Erhebung des Umfangs des Penetrationstests . . . . .	153
8.2.1	Netzwerk-Penetrationstest . . . . .	153
8.2.2	Penetrationstest für Webanwendungen . . . . .	154
8.2.3	Wireless-Netzwerk-Penetrationstests . . . . .	154
8.2.4	Physischer Penetrationstest . . . . .	155
8.2.5	Social Engineering . . . . .	156
8.2.6	Fragen an den Abteilungs-/Geschäftsstellenleiter . . . . .	156
8.2.7	Fragen an Systemadministratoren . . . . .	156
8.3	Ziele . . . . .	157
8.3.1	Primär . . . . .	157
8.3.2	Sekundär . . . . .	157
8.4	Geschäftsanalyse . . . . .	157
8.5	Angeben von IP-Bereichen und Domänen . . . . .	158
8.6	Umgang mit Dritten . . . . .	158
8.6.1	Cloud-Dienste . . . . .	159
8.6.2	Internetdienstanbieter (ISP) . . . . .	159
8.6.3	Managed Security Service Provider (MSSPs) . . . . .	159
8.6.4	Länder, in denen Server gehostet werden . . . . .	160
8.7	Definition akzeptabler Social-Engineering-Vorwände . . . . .	160
8.8	DoS-Tests . . . . .	160
8.9	Zahlungsbedingungen . . . . .	160
8.10	Kommunikationswege einrichten . . . . .	161
8.10.1	Kontaktinformationen für Notfälle . . . . .	161
8.10.2	Incident-Reporting-Prozess . . . . .	162
8.10.3	Definition von Vorfällen . . . . .	162
8.10.4	Häufigkeit von Statusberichten . . . . .	163
8.10.5	Verschlüsselung und Alternativen . . . . .	163
8.11	Regeln für den Auftrag . . . . .	164
8.11.1	Zeitleiste . . . . .	164
8.11.2	Orte . . . . .	164
8.11.3	Sensible Informationen schützen . . . . .	164
8.11.4	Umgang mit Beweismitteln . . . . .	165
8.11.5	Regelmäßige Statusbesprechungen . . . . .	165
8.11.6	Uhrzeit zum Testen . . . . .	166

8.11.7	Berechtigung zum Testen .....	166
8.11.8	Rechtliche Überlegungen .....	166
8.12	Vorhandene Funktionen und Technologien .....	166
8.13	Zusammenfassung .....	167
<b>9</b>	<b>Informationen sammeln (Aufklärung) .....</b>	<b>169</b>
9.1	Einführung. ....	169
9.2	Die Recherche .....	171
9.3	Identifikation von Zielen .....	172
9.4	Passives Scannen vs. aktives Scannen .....	173
9.5	Tools zum Sammeln von Informationen .....	173
9.5.1	HTTrack – Website als Offline-Kopie. ....	174
9.5.2	Google Dork – Hacking mit Suchanfragen .....	176
9.5.3	Newsgroups, Hilfeforen und Co. als Informationsquelle . . .	180
9.5.4	Social Media als Informationsquelle. ....	181
9.5.5	TheHarvester – E-Mail-Adressen aufspüren und ausnutzen .....	182
9.5.6	Domäne als Informationsquelle .....	184
9.5.7	Informationen von DNS-Servern abrufen .....	186
9.5.8	fierce – Falls Zonentransfer nicht möglich ist. ....	189
9.5.9	Informationen von E-Mail-Servern gewinnen .....	189
9.5.10	MetaGooFil – Metadaten extrahieren .....	190
9.5.11	Maltego – Gesammelte Daten in Beziehung setzen .....	191
9.5.12	Sherlock – Der Detektiv fürs soziale Netz .....	193
9.5.13	Social Engineering – Menschliche Schwachstellen ausnutzen .....	195
9.6	Auswertung der Informationen und nach Zielen suchen .....	196
9.7	Wie kann man diese Schritte üben? .....	197
9.8	Zusammenfassung .....	199
<b>10</b>	<b>Aktives Scannen. ....</b>	<b>201</b>
10.1	Einführung. ....	201
10.1.1	Ermitteln der aktiven Hosts mittels Ping .....	201
10.1.2	Portscan. ....	202
10.1.3	Untersuchung der Ergebnisse mittels NSE .....	203
10.1.4	Schwachstellen-Scan mit OpenVAS .....	203
10.2	Aktive Hosts mittels Ping aufspüren .....	204
10.3	Portscan .....	206
10.3.1	Scannen mit Nmap .....	207
10.3.2	Nmap Script Engine – Transformation eines Tools .....	215
10.3.3	Portscan abschließen .....	217
10.4	Automation bei der Informationsbeschaffung mit legion .....	219

10.5	Schwachstellen-Scan . . . . .	221
10.5.1	Arten von Schwachstellen-Scans und des Erkennens von Schwachstellen. . . . .	221
10.5.2	Was bewirken Schwachstellen-Scan-Tools? . . . . .	222
10.5.3	Welche Schwachstellen-Scanner gibt es? . . . . .	223
10.5.4	Scan-Ergebnisse auswerten mit Schwachstellendatenbanken . . . . .	224
10.5.5	OpenVAS – Sicherheitslücken aufdecken . . . . .	226
10.6	Siege – Performance Test von Webseiten . . . . .	231
10.6.1	Konfiguration . . . . .	232
10.7	Wie kann man diese Schritte üben? . . . . .	233
10.8	Was sind die nächsten Schritte? . . . . .	233
10.9	Zusammenfassung . . . . .	234
<b>11</b>	<b>Eindringen über das lokale Netzwerk. . . . .</b>	<b>235</b>
11.1	Zugriff auf Remotedienste . . . . .	237
11.1.1	Medusa . . . . .	237
11.2	Übernahme von Systemen . . . . .	240
11.2.1	Metasploit . . . . .	241
11.2.2	Meterpreter . . . . .	249
11.3	Passwörter hacken . . . . .	250
11.3.1	Lokales Passwort-Cracking. . . . .	252
11.3.2	Passwort-Cracking über das Netzwerk . . . . .	255
11.3.3	JtR – Passwort-Cracking. . . . .	256
11.3.4	Knacken von Linux-Passwörtern . . . . .	259
11.3.5	Abrissbirnen-Technik – Passwörter zurücksetzen. . . . .	260
11.4	Passwörter aus dem Active Directory . . . . .	263
11.4.1	LLMNR Poisoning . . . . .	263
11.4.2	SMB Relay . . . . .	265
11.5	Netzwerkverkehr ausspähen (Sniffing) . . . . .	267
11.5.1	Wie kann man den Netzwerkdatenverkehr abhören? . . . . .	267
11.5.2	dsniff – Sammlung von Werkzeugen zum Ausspionieren von Netzwerkdatenverkehr . . . . .	269
11.5.3	macof – Aus einem Switch einen Hub machen. . . . .	270
11.5.4	WireShark – Der Hai im Datenmeer . . . . .	271
11.5.5	Ettercap – Datenverkehr abfangen und manipulieren. . . . .	274
11.6	Armitage – Hacking mit dem »Maschinengewehr« . . . . .	276
11.7	Wie kann man diesen Schritt üben? . . . . .	280
11.8	Was sind die nächsten Schritte? . . . . .	281
11.9	Zusammenfassung . . . . .	283

<b>12</b>	<b>Webgestütztes Eindringen</b> .....	285
12.1	Grundlagen des Webhackings .....	285
12.1.1	Anforderungen abfangen, die vom Browser ausgehen .....	286
12.1.2	Webseiten, Verzeichnisse und sonstige Dateien finden, die für die Webanwendung notwendig sind .....	286
12.1.3	Antworten von Webanwendungen analysieren und auf Schwachstellen durchsuchen .....	287
12.2	Schwachstellen in Webapplikationen finden .....	288
12.2.1	Nikto – Aufspüren von Schwachstellen auf Webservern ...	288
12.2.2	watobo – Mehr als nur eine hübsche Oberfläche. ....	289
12.3	WebScarab – Webseiten analysieren (Spider) .....	295
12.3.1	Konfiguration und Spiderangriff. ....	296
12.3.2	Anforderungen abfangen. ....	298
12.4	Code-Injection .....	300
12.5	Wenn Browser Webseiten vertrauen – XSS-Angriffe. ....	304
12.6	ZAP – Zed Attack Proxy, das All-in-one-Tool .....	307
12.6.1	ZAP als Proxy .....	307
12.6.2	Informationen abfangen .....	307
12.6.3	Informationen sammeln (Spiderangriff) mit ZAP .....	309
12.6.4	Schwachstellen-Scan mit ZAP. ....	310
12.7	Wie kann man diesen Schritt üben? .....	310
12.8	Was sind die nächsten Schritte? .....	312
12.9	Zusammenfassung .....	313
<b>13</b>	<b>Social Engineering</b> .....	315
13.1	Grundlagen von SET .....	315
13.2	Spear-Phishing. ....	317
13.3	Webseite als Angriffsweg .....	317
13.4	Credential Harvester .....	323
13.5	Weitere Optionen in SET .....	324
13.6	Zusammenfassung .....	327
<b>14</b>	<b>Nachbearbeitung &amp; Erhaltung des Zugriffs</b> .....	329
14.1	Netcat – Das Schweizer Taschenmesser .....	330
14.2	Cryptcat – Ein kryptischer Vetter von Netcat. ....	336
14.3	Rootkits. ....	337
14.3.1	Rootkits erkennen und abwehren .....	339
14.4	Meterpreter – Der Hammer, der aus allem einen Nagel macht ...	341
14.5	Wie kann man diesen Schritt üben? .....	344
14.6	Was sind die nächsten Schritte? .....	345
14.7	Zusammenfassung .....	346



<b>15</b>	<b>Abschluss eines Penetrationstests</b> .....	<b>347</b>
15.1	Tools für den Report .....	348
	15.1.1 Cutycapt. ....	348
	15.1.2 Faraday-IDE. ....	350
	15.1.3 Pipal. ....	354
	15.1.4 RecordMyDesktop. ....	354
15.2	Testbericht schreiben .....	355
	15.2.1 Zusammenfassung für die Geschäftsführung. ....	356
	15.2.2 Rohausgaben. ....	356
	15.2.3 Abschluss und Übermittlung des Berichts. ....	357
15.3	Was sind die nächsten Schritte? .....	359
15.4	Zusammenfassung .....	361
<b>A</b>	<b>Nachwort</b> .....	<b>363</b>
	<b>Stichwortverzeichnis</b> .....	<b>367</b>