

Auf einen Blick

Einleitung	23
Teil I: Kali Linux – System einrichten und kennenlernen	29
Kapitel 1: Die Grundlagen zu Kali Linux erfahren	31
Kapitel 2: Kali Linux installieren	37
Kapitel 3: Die ersten Schritte ausführen	51
Teil II: Information Gathering – verdeckte Informationen sammeln	59
Kapitel 4: Netzwerke analysieren	61
Kapitel 5: Domains und IP-Adressen auslesen	79
Kapitel 6: Server-Dienste untersuchen und testen	87
Kapitel 7: Öffentliche Informationen (OSINT)	99
Teil III: Password Attacks – Passwörter knacken	111
Kapitel 8: Angriffsmethoden gegen Passwörter nutzen	113
Kapitel 9: FTP-, SSH- und Web-Logins angreifen	133
Kapitel 10: Passwort-Hashes auslesen und berechnen	143
Teil IV: Web Application Analysis – Websites untersuchen	155
Kapitel 11: Webrisiken verstehen	157
Kapitel 12: Potenzielle Webziele finden und identifizieren	163
Kapitel 13: Web-Kommunikation analysieren	175
Kapitel 14: Auf bekannte Fehlkonfigurationen und Schwachstellen testen	191
Teil V: Wireless Attacks – WLANs angreifen / Sicherheit testen	239
Kapitel 15: WLAN-Equipment vorbereiten	241
Kapitel 16: Versteckte Netzwerke finden	247
Kapitel 17: WPA/2-Passwörter angreifen	253
Kapitel 18: Fake-Netzwerke erstellen	267
Teil VI: Sniffing und Spoofing – Netzwerke unterwandern	289
Kapitel 19: Netzwerke angreifen	291
Kapitel 20: Netzwerkverkehr aufzeichnen	295
Kapitel 21: Datenströme umleiten	301
Kapitel 22: Netzwerkverkehr manipulieren	311
Teil VII: Forensics – IT-Forensik-Analysen	319
Kapitel 23: Sicherungskopie erstellen	321
Kapitel 24: Gelöschte Dateien wiederherstellen	333
Kapitel 25: Versteckte Informationen in Dateien	345
Kapitel 26: Betriebssysteme und Anwendungen analysieren	361

Teil VIII: Der Top-Ten-Teil..... 375

Kapitel 27: Top-Ten-Tools im Überblick..... 377

Kapitel 28: Top-Ten-Alternativen zu Kali Linux..... 391

Abbildungsverzeichnis..... 395

Stichwortverzeichnis..... 405

Inhaltsverzeichnis

<https://github.com/0x00sec/0x00sec.github.io>

Einleitung	23
Über dieses Buch	23
Törichte Annahmen über den Leser	24
Wie dieses Buch aufgebaut ist	25
Teil I: Erste Schritte mit Kali Linux	25
Teil II: Information Gathering – verdeckte Informationen sammeln	25
Teil III: Password Attacks – Passwörter knacken	25
Teil IV: Web Application Analysis – Websites untersuchen	25
Teil V: Wireless Attacks – WLANs angreifen / Sicherheit testen	26
Teil VI: Sniffing und Spoofing – Netzwerke unterwandern	26
Teil VII: Forensic Tools – IT-Forensik Analysen	26
Teil VIII: Der Top-Ten-Teil	26
Symbole, die in diesem Buch verwendet werden	26
Konventionen in diesem Buch	27
Wie es weitergeht	28
 TEIL I	
KALI LINUX – SYSTEM EINRICHTEN UND KENNENLERNEN	29
Kapitel 1	
Die Grundlagen zu Kali Linux erfahren	31
Die Einsatzzwecke von Kali Linux verstehen	31
Verschiedene Varianten von Kali Linux kennenlernen	32
Mehr über Kali Linux herausfinden	36
 Kapitel 2	
Kali Linux installieren	37
Einen Hypervisor installieren	37
Kali Linux mit einer virtuellen Maschine installieren	38
Kali Linux mit einem Installer-Image installieren	39
Herunterladen des Installers	40
Erstellen einer virtuellen Maschine	40
Kali Linux installieren	42
Metasploitable 2 installieren	47
Netzwerke für Kali Linux konfigurieren	48
 Kapitel 3	
Die ersten Schritte ausführen	51
Den Menüaufbau von Kali Linux einsehen	51
Die empfohlenen Konfigurationen vornehmen	51
Zwischen Host- und Gastsystem unterscheiden	51
Automatische Displaygrößenänderungen erlauben	52
Geteilte Zwischenablage aktivieren	53

Systemsprache beibehalten.....	53
Tastaturlayout ändern.....	54
Administrative Befehle ausführen.....	56
Paket-Updates durchführen.....	56
Verwundbare Applikationen installieren.....	57

TEIL II	
INFORMATION GATHERING – VERDECKTE INFORMATIONEN SAMMELN	59

Kapitel 4	
Netzwerke analysieren	61
arping – Verbindungen zu Systemen mit ARP-Requests überprüfen.....	63
Nicht erreichbare Systeme erkennen	65
Kompakte Darstellung verwenden.....	65
arp-scan – lokales Netzwerk analysieren.....	66
Gesamtes Netzwerk scannen.....	66
Netzwerkbereich analysieren.....	67
fping – erweiterte Ping-Abfrage.....	68
Erreichbarkeit testen.....	68
Komplettes Netzwerk überprüfen	69
netdiscover – Netzwerke passiv scannen.....	69
So führen Sie einen passiven Scan durch.....	70
Und so einen aktiven Scan.....	70
Ergebnisse im interaktiven Modus betrachten	71
Nmap – Netzwerke vielfältig scannen.....	71
Den ICMP-Echo-Ping-Scan verwenden.....	72
Den TCP-Ping-Scan einsetzen.....	72
Zenmap – Graphen eines Netzwerkes erstellen	73
Graph des Netzwerkes erzeugen	74
Einen intensiven Scan durchführen (»Intense Scan«).....	75
Alle Zwischenstationen mit Traceroute analysieren.....	76
mtr – Kommunikationswege analysieren	77
Interface von mtr einsetzen.....	77
Ohne grafische Oberfläche nutzen	78

Kapitel 5	
Domains und IP-Adressen auslesen	79
DNSRecon – DNS-Einträge auslesen.....	79
DNS-Einträge einer Domain auslesen	80
dnsmap – Subdomains finden	82
Liste mit Stichwörtern einsetzen, um Subdomains zu finden.....	83
dmitry – IP- und Domain-Informationen ermitteln	84
Informationen zu einer Domain abfragen.....	84
Informationen zu einer IP-Adresse abfragen.....	84

IPGeoLocation – IP-Adressen lokalisieren	85
Gefundene Informationen nutzen	86

Kapitel 6

Server-Dienste untersuchen und testen	87
Nmap – Informationen über Dienste gewinnen	88
Unauffällig scannen mit Null-Scan	88
Mit TCP-SYN-Scan offene Ports finden	88
Mit einem UDP-Scan weitere Ports aufspüren	90
Das Betriebssystem herausfinden	91
Die Version von Diensten ermitteln	92
Kompletten Scan durchführen	93
hping3 – Analyse der Erreichbarkeit	95
Potenzielle Filterungen aufspüren	95
Metasploit – Schwachstellen in Diensten ausnutzen	96
Nach Schwachstellen suchen	96
Passenden Exploit suchen	97
Exploit auswählen und ausführen	98

Kapitel 7

Öffentliche Informationen (OSINT)	99
theHarvester – gezielt nach E-Mail-Adressen suchen	99
Auf allen unterstützten Plattformen suchen	100
Suche nach Firmennamen	101
SpiderFoot – automatisierte Analyse	101
SpiderFoot starten	102
Neue Suche durchführen	102
Ergebnisse der Suche auswerten	104
OSRFramework – flexible Suche auf verschiedenen Plattformen	105
Accounts bei Social-Media-Diensten und Online-Plattformen suchen	106
Maryam – modulares OSINT Framework nutzen	107
Informationen zu einzelnen Modulen erhalten	107
Eine Domain analysieren	108
Maltego – Umfangreiche Recherche nach Informationen durchführen	109
Neuen Graphen für eine Analyse anlegen	109

TEIL III

PASSWORD ATTACKS – PASSWÖRTER KNACKEN	111
--	------------

Kapitel 8

Angriffsmethoden gegen Passwörter nutzen	113
wordlists – Listen mit Passwörtern nutzen	114
Bekannte Passwortliste RockYou nutzen	115
Passwortlisten generieren und modifizieren	116
crunch – Passwortlisten erzeugen	116
CeWL – Passwortlisten aus Websites erzeugen	121

Mentalist – Passwortlisten erweitern	123
CUPP – individuelle Passwortlisten erstellen	125
FCrackZip – ZIP-Passwörter knacken	127
Benchmark durchführen	127
ZIP-Passwörter mit Passwortlisten angreifen	127
Brute-Force-Methode zum Knacken einsetzen	128
PDFCrack – PDF-Passwörter brechen	129
Benchmark ausführen	129
User-Passwort der PDF-Datei finden	130
Owner-Passwort der PDF-Datei knacken	131
Passwortlänge festlegen	131
Passwortlisten einsetzen	131

Kapitel 9

FTP-, SSH- und Web-Logins angreifen 133

Hydra – verschiedene Anmeldeverfahren testen	133
Passwortliste mit Hydra nutzen	134
Anzahl der Anfragen erhöhen	135
Brute-Force-Methode einsetzen	135
HTTP-Logins oder Formulare angreifen	136
Ncrack – schnell Logins durchführen	137
Passwortliste mit Ncrack einsetzen	138
Vorgang beschleunigen	138
Mehrere Ziele gleichzeitig angreifen	139
Verschiedene Dienste analysieren	139
Medusa – flexiblen Brute-Forcer einsetzen	139
Passwortliste mit Medusa nutzen	140
Patator – Tool mit feingranularen Einstellungen	141
Passwortliste mit Patator verwenden	141
Weitere Module nutzen	142

Kapitel 10

Passwort-Hashes auslesen und berechnen 143

hash-identifizier – Hashes analysieren	144
Hashes zum Testen erzeugen	144
Hash analysieren lassen	144
John the Ripper – Hashes extrahieren	145
Geschwindigkeit mit Benchmark testen	145
Beispiel-Hash für Testzwecke erzeugen	146
Hash mit John knacken	146
John-the-Ripper-Tools kennenlernen	147
PDF-Passwort-Hash extrahieren	147
Passwortliste mit John nutzen	148
Brute-Force-Methode anwenden	148

hashcat – Hashes berechnen	149
Passwortliste mit hashcat einsetzen	150
Brute-Force-Methode anwenden	151
PDF-Passwort mit hashcat knacken	152

TEIL IV

WEB APPLICATION ANALYSIS – WEBSITES UNTERSUCHEN..... 155

Kapitel 11

Webrisiken verstehen..... 157

Testsysteme einsetzen	158
DVWA – verwundbare Web-App einrichten	159
Juice Shop – unsicheren Webshop installieren.....	160

Kapitel 12

Potenzielle Webziele finden und identifizieren..... 163

Ordner- und Subdomain-Enumeration	163
dirb – Unterseiten und versteckte Dateien finden	165
dirbuster – grafisch nach Dateien und Ordnern suchen	166
gobuster – schnell Ordner und Subdomains identifizieren	168
wafw00f – Web-Firewalls erkennen.....	171
whatweb – Überblick über Website verschaffen.....	172

Kapitel 13

Web-Kommunikation analysieren..... 175

Dev Tools – Parameter und Cookies finden.....	178
HTML-Elemente darstellen.....	179
Anfragen auflisten	180
(POST-)Parameter identifizieren	181
Cookies extrahieren	181
Burp Suite – eigene Server-Anfragen versenden	182
Netzwerkverkehr anpassen	183
Intercept-Modus nutzen.....	184
Repeater verwenden.....	186
Intruder einsetzen	187
Anfragen exportieren	189

Kapitel 14

Auf bekannte Fehlkonfigurationen und Schwachstellen

testen..... 191

Schwachstellen-Scanner	191
nikto – Web-Schwachstellen identifizieren	192
wapiti – umfangreiche Schwachstellen-Scans durchführen.....	196
TLS/SSL-Analyse	200
testssl – TLS/SSL-Verbindungen überprüfen.....	200
SSLyze – TLS/SSL-Verbindungen analysieren	202
ssllscan – TLS/SSL-Verbindungen schnell testen	204

18 Inhaltsverzeichnis

CMS-spezifische Scanner	204
WPScan – Schwachstellen in WordPress-Instanzen finden	205
Injection-Scanner	210
sqlmap – SQL-Injection finden und ausnutzen	214
XSSStrike – Cross-Site-Scripting-Schwachstellen aufspüren	219
commix – Command Injections finden und ausnutzen	223
Fuzzer	226
ffuf – Web-Parameter fuzzen	227
wfuzz – Parameter mit erzeugten Listen testen	233

TEIL V

WIRELESS ATTACKS – WLANS ANGREIFEN / SICHERHEIT

TESTEN 239

Kapitel 15

WLAN-Equipment vorbereiten 241

WLAN-Adapter einrichten	243
lsusb – vorhandene USB-Geräte ausgeben	243
iw – Adapter-Infos auslesen	243
airmon-ng – Monitor Mode aktivieren	244
iw – Regionseinstellung setzen	245
aireplay-ng – Packet Injection testen	245

Kapitel 16

Versteckte Netzwerke finden 247

airodump-ng – WLAN-Teilnehmende finden	248
aireplay-ng – Client(s) aus dem Netzwerk werfen	250
mdk4 – WLAN-SSIDs bruteforcen	251

Kapitel 17

WPA/2-Passwörter angreifen 253

bettercap – WPA/2-Schlüsselmaterial aufzeichnen	256
Handshake eines Clients aufzeichnen	258
PMKID verwenden	259
hcxtools – Handshakes in knackbare Hashes konvertieren	260
hashcat – WLAN-Hashes brechen	261
Modus und Zeichensätze wählen	261
Performance anpassen	261
Masking-Attack durchführen	262
Wordlist-Attack verwenden	263
airdecap-ng – Traffic-Mitschnitte entschlüsseln	264
Aufzeichnung mit Wireshark erstellen	264
Verkehr mit airodump-ng aufzeichnen	264
Aufzeichnung entschlüsseln	265

Kapitel 18

Fake-Netzwerke erstellen	267
mdk4 – Netzwerklisten fluten	267
Beacon Flooding einsetzen	268
Angriff durchführen	268
macchanger – MAC-Adresse fälschen	269
berate_ap – Evil Twins erstellen	271
MAC-Adresse spoofen	272
Internetzugang teilen	273
Passwortgeschützte (versteckte) WLANs erstellen	273
Netzwerkverkehr mit Wireshark analysieren	274
Man-in-the-middle-(MitM-)-Angriffe einsetzen	274
wifiphisher – Evil Twins mit Phishing-Seiten erzeugen	275
Captive Portals missbrauchen	275
Firmware-Upgrade-Seite nutzen	276
Browser-Plug-in-Update-Seite einsetzen	278
EAPHammer – WPA2 Enterprise angreifen	279
Kommunikationsablauf verstehen	279
Angriff durchführen	279
EAP-Methoden verstehen	280
EAPHammer einrichten	281
Angriff starten	282
Netzwerk beitreten	283
Zugangsdaten extrahieren	285
Hashes brechen	285
Gegenmaßnahmen ergreifen	287

TEIL VI**SNIFFING UND SPOOFING – NETZWERKE UNTERWANDERN ... 289****Kapitel 19**

Netzwerke angreifen	291
Man-in-the-Middle-(MitM-)Angriffe kennenlernen	291
Physikalische MitM-Angriffe	291
Logische MitM-Angriffe	292
Einschränkungen von Netzwerk-Angriffen verstehen	293
Verschlüsselung einsetzen	293
Wireless APs absichern	293
Überblick erhalten	294

Kapitel 20

Netzwerkverkehr aufzeichnen	295
tcpdump – Netzwerkverkehr aufzeichnen	295
Alle Pakete eines Netzwerkinterfaces ausgeben	295
Aufgezeichneten Netzwerkverkehr speichern	297
Aufgezeichneten Netzwerkverkehr filtern	298
Wireshark – Netzwerkinterfaces aufzeichnen und analysieren	299

Kapitel 21

Datenströme umleiten 301

- arpspoof – Netzwerkverkehr mittels ARP umleiten..... 301
 - ARP-Spoofing-Angriff vorbereiten..... 302
 - ARP-Spoofing-Angriff durchführen..... 302
 - Den umgeleiteten Netzwerkverkehr auslesen..... 304
- mitmproxy – HTTP-Requests interaktiv analysieren..... 304
 - mitmproxy-Setup vorbereiten 304
 - mitmproxy verwenden 305
- urlsnarf – besuchte Websites ausgeben..... 307
- Driftnet – besuchte Bilder anzeigen..... 308
 - Nutzung von Driftnet vorbereiten..... 308
 - Driftnet einsetzen 309

Kapitel 22

Netzwerkverkehr manipulieren..... 311

- bettercap – DNS-Anfragen fälschen..... 311
- bettercap – HTTP-Verkehr manipulieren und Code injizieren..... 313
- bettercap – manipulierte Programme einschleusen 314
 - Autopwn-Modul einsetzen..... 315

TEIL VII

FORENSICS – IT-FORENSIK-ANALYSEN 319

Kapitel 23

Sicherungskopie erstellen 321

- Die Methoden der IT-Forensik nutzen..... 322
 - Anwendungsgebiete der IT-Forensik verstehen..... 322
 - Digitale Spuren analysieren..... 323
- Forensische 1:1-Kopien erstellen..... 324
 - Write-Blocker einsetzen..... 324
 - dd – bitgenaue Kopien erstellen..... 327
 - dc3dd – forensische Sicherungen erzeugen..... 328
 - guymager – Sicherung mit grafischer Oberfläche durchführen..... 330

Kapitel 24

Gelöschte Dateien wiederherstellen..... 333

- Gelöschte Dateien retten 333
 - PhotoRec – Gelöschte Fotos wiederherstellen..... 334
 - Foremost – Suche nach gelöschten Dateien..... 336
 - Scalpel – Alternative zu Foremost einsetzen..... 338
 - Bulk Extractor – Nach Informationen suchen 339
 - extundelete – Spezialwerkzeug für Ext-Dateisysteme verwenden..... 340

Defekte Datenspeicher reparieren	340
fsck – Überprüfen und Reparieren von Laufwerken.....	340
ddrescue – Kopien von beschädigten Laufwerken anlegen.....	340
SafeCopy – Datenwiederherstellung von Laufwerken.....	341
TestDisk – Reparaturen von Partitionen.....	342

Kapitel 25

Versteckte Informationen in Dateien	345
Metadaten und weitere Zusatzinformationen auslesen.....	345
stat – Zeitstempel einer Datei ausgeben.....	346
ExifTool – Metadaten und dateispezifische Informationen.....	348
pdfid – Inhalte von PDF-Dateien analysieren.....	349
Metagoofil – Dateien aus Websites analysieren.....	349
Zusätzliche Daten in Fotos auslesen.....	351
exiv2 – Zusatz- und Metainformationen in Fotos.....	352
ExifTool – Metadaten aus digitalen Bildern auslesen.....	352
Manipulation von Fotos erkennen.....	355
Sherloq – Erkennung von Bildmanipulationen.....	355
Verborgene Informationen mittels Steganografie	357
steghide – Informationen in anderen Dateiformaten verstecken.....	358
stegextract – versteckte Informationen finden.....	359

Kapitel 26

Betriebssysteme und Anwendungen analysieren	361
The Sleuth Kit und Autopsy – automatisierte Komplettanalysen durchführen ...	361
Autopsy – forensische Analyse mit Web-Oberfläche.....	362
The Sleuth Kit – umfangreiche Sammlung von spezifischen Tools.....	367
dumpzilla – Webbrowser Mozilla Firefox analysieren.....	370
DB Browser for SQLite – Datenbanken des Firefox-Webrowsers auslesen	371
Aufgerufene URLs auslesen	372

TEIL VIII

DER TOP-TEN-TEIL	375
-------------------------------	------------

Kapitel 27

Top-Ten-Tools im Überblick	377
Information Gathering.....	377
Top-Ten-Tools Password Attacks.....	379
Top-Ten-Tools Web Application Analysis.....	382
Top-Ten-Tools Wireless Attacks	384
Top-Ten-Tools Sniffing und Spoofing.....	386
Top-Ten-Tools Forensics	388

Kapitel 28

Top-Ten-Alternativen zu Kali Linux 391

 ParrotOS 391

 BlackArch 391

 Tsurugi..... 392

 Backbox 392

 Pentoo 392

 CAINE..... 392

 Fedora Security Lab..... 392

 Network Security Toolkit..... 393

 Samurai Web Training Framework 393

 ArchStrike 393

Abbildungsverzeichnis 395

Stichwortverzeichnis 405