Inhaltsverzeichnis

VORWORT 7

1 EINSTIEG IN DAS PENETRATION TESTING 9

1.1 Die richtige Hard- und Software 10
1.1.1 Kali Linux in Betrieb nehmen 13
1.1.2 Windows als Penetration-Plattform 16

1.2 Sammeln von Informationen 18

2 SCHWACHSTELLEN AUFDECKEN 25

2.1 Security Scanner im Einsatz 25

2.2 Ein erster Sicherheitscheck 27

2.3 Berichte interpretieren 28

2.4 Scan-Konfiguration 31

2.5 Administrative Aufgaben 36

3 ANGRIFFSPUNKTE PORTS 39

3.1 Alles Wichtige über Nmap 39

3.2 Mit Zenmap arbeiten 47

3.3 Scannen und auswerten 48

3.4 Netzwerktopologien 56

3.5 Der Profileditor 61

3.6 Erweiterte Zenmap-Funktionen 63

4 SCHWACHSTELLEN PRÜFEN 65

4.1 Das Grundprinzip 65

4.2 Erste Schritte mit Metasploit 66

4.3 Aktive und passive Exploits 69

4.4 Daten sammeln 72

4.5 Attack-Management mit Armitage 74

4.6 Versionswirrwarr 77

5 SCANNEN VON WEB-APPLIKATIONEN 81

5.1 Web Application Security Scanner 81

5.2 Must-have: die Burp Suite 82

5.3 Burp Suite für Einsteiger 85

5.4 Der Workflow mit der Burp Suite 87

5.5 Das Target-Tool in der Praxis 90

5.6 Verwundbarkeiten testen 92

5.7 Praxisbeispiele mit der Burp Suite 97
5.7.1 Brute Force-Attacke eines Login-Dialogs 97
5.7.2 Injection-Schwachstellen ausnutzen 101
5.7.3 Mangelhafte Sicherheitskonfigurationen aufdecken 103
5.7.4 Cross Site Scripting-Attacken mit Burp 104

6 WLAN-SICHERHEIT PRÜFEN 107

6.1 Unsicherheiten in WLANs 109

6.2 WLAN-Authentifizierung umgehen 115
6.2.1 Versteckte WLANs aufspüren 115
6.2.2 MAC-Filter aushebeln 118
6.2.3 Schlüsselauthentifizierung umgehen 119

6.3 Verschlüsselungslücken ausnutzen 121

6.4 WPA-Sicherung aushebeln 125

6.5 WEP- und WPA-Pakete entschlüsseln 128

6.6 Verbindung herstellen 129

7 WERKZEUGKASTEN – WEITERE HACKER-TOOLS 131

7.1 Zugangsdaten 131

7.2 Passwörter, WLAN-Schlüssel und mehr erlangen 133

7.3 Rechte ausweiten 136

8 SOCIAL ENGINEERING UND INFORMATIONSVERKNÜPFUNG 141

8.1 Daten kombinieren 142

8.2 Weitere Möglichkeiten 146

9 DOKUMENTATION 149

9.1 Die ideale Lösung: Docear 150

9.2 Erste Schritte 152

9.3 Informationen filtern 155

9.4 Weitere Besonderheiten 156

9.5 Sicherheit und Datenaustausch 157

ANHANG A – MORE INFO 159

ANHANG B – EIGENE TESTUMGEBUNG 161

INDEX 163

WEITERE BRAIN-MEDIA.DE-BÜCHER 169

Weitere Titel in Vorbereitung 171

Plus+ 172