

Inhaltsverzeichnis

1	Basiswissen Funknetzwerke	19
1.1	Was ist WLAN?	19
1.1.1	Physikalische Grundlagen	19
1.1.2	Probleme bei drahtloser Datenübertragung.....	21
1.2	Geschichte des WLAN	22
1.2.1	IEEE 802.11	23
1.2.2	IEEE 802.11a.....	23
1.2.3	IEEE 802.11b	24
1.2.4	IEEE 802.11g.....	24
1.2.5	IEEE 802.11n	24
1.2.6	Weitere historische Standards	25
1.2.7	IEEE 802.11ac.....	25
1.2.8	IEEE 802.11ad.....	27
1.2.9	IEEE 802.11ax.....	28
1.3	WLAN ist nicht nur IEEE 802.11	28
1.3.1	Bluetooth.....	28
1.3.2	ZigBee	29
1.3.3	Z-Wave.....	29
1.3.4	HiperLAN.....	30
1.3.5	HomeRF	30
1.3.6	WiMAX	30
1.3.7	Li-Fi.....	30
2	WLAN-Grundlagen.....	33
2.1	Komponenten in WLAN-Infrastrukturen	33
2.1.1	WNIC: Wireless Network Interface Controller.....	33
2.1.2	STA: Stations.....	34
2.1.3	AP: Access Point.....	34
2.1.4	Authentication Server und Distribution System	35
2.1.5	WLAN-Controller	37
2.2	WLAN-Topologien	37
2.2.1	IBSS: Independent Basic Service Set	37
2.2.2	BBS: Basic Service Set.....	39
2.2.3	ESS: Extended Service Set	40
2.2.4	WDS: Wireless Distribution System	41
2.2.5	Drahtlose Mesh-Netzwerke	42

2.3	Bezeichnungen von WLANs	44
2.3.1	SSID: Service Set Identifier	46
2.3.2	ESSID: Extended Service Set Identifier	51
2.3.3	BSSID und MAC-Adresse.....	51
2.4	WLAN-Operationen	52
2.5	Authentifizierungsarten	53
2.5.1	Open System Authentication	53
2.5.2	Shared Key Authentication	54
2.6	Layer und Frames bei WLAN	55
2.6.1	Physical Layer	56
2.6.2	MAC-Layer	58
2.6.3	Arten von WLAN-Frames.....	61
3	Basiswissen WLAN-Sicherheit.....	69
3.1	WEP: Wired Equivalent Privacy Protocol.....	71
3.2	WPA (IEEE 802.11i/D3.0)	75
3.2.1	WPA Personal	75
3.2.2	WPA Enterprise.....	78
3.3	WPA2 (IEEE 802.11i/D9.0)	82
3.3.1	Advanced Encryption Standard.....	82
3.3.2	WPA2 Personal.....	82
3.3.3	WPA2 Enterprise.....	83
3.4	WLAN-Verschlüsselungen.....	84
3.5	WPS: Wi-Fi-Protected Setup	85
3.6	Sonderfall WAPI.....	86
3.7	Weitere Sicherheitsfeatures.....	86
3.7.1	Protected Management Frames (IEEE 802.11w)	87
3.7.2	MAC-Filter	89
3.7.3	Nutzung von verborgenen SSIDs	90
4	Vorbereitungen und Setup.....	93
4.1	Der Angreifer-PC.....	93
4.1.1	Kali Linux	94
4.1.2	Wifislax.....	102
4.2	Der Opfer-PC	105
4.2.1	Hardware	105
4.2.2	WLAN-Router.....	105
4.2.3	OpenWrt	108
4.2.4	WLAN-Karten.....	109
4.2.5	WLAN-Antennen	116
4.3	Monitormodus.....	118
4.4	Weitere WLAN-Ausstattung	120
4.4.1	WiFi Pineapple	120
4.4.2	Einrichtung und erste Schritte.....	123

5	Informationsbeschaffung	135
5.1	Scanning-Methoden	135
5.1.1	Passives Scanning.....	136
5.1.2	Aktives Scanning.....	136
5.2	WLANs der Umgebung analysieren	137
5.2.1	airodump-ng	138
5.2.2	MetaGeek inSSIDer	141
5.2.3	Acrylic Wi-Fi Professional.....	142
5.2.4	Wifi Analyzer	143
5.3	WLAN-Abdeckung überprüfen	146
5.3.1	Acrylic Wi-Fi HeatMaps	146
5.3.2	Ekahau Site Survey.....	147
5.4	Nicht digitale Informationsbeschaffung.....	148
5.4.1	Social Engineering	149
5.4.2	Gegenmaßnahmen zum Social Engineering	150
5.5	Ergebnisse dokumentieren	150
6	Sniffing und Analyse	153
6.1	Netzwerkverkehr aufzeichnen	153
6.2	Sniffing mit Remote-Interface	156
6.2.1	Passives Sniffing mit tcpdump	156
6.2.2	Passives Sniffing mit tcpdump und Wireshark.....	158
6.3	WLAN-Verkehr untersuchen und Netzwerke aufspüren	161
6.4	Verbindungen zu verborgenen SSIDs.....	164
6.4.1	Ermitteln verborgener SSIDs durch passives Sniffing.....	168
6.4.2	Ermitteln verborgener SSIDs durch Brute Force.....	170
6.5	Packet Capture	180
7	Störangriffe auf WLAN	183
7.1	Angriffe auf physikalischer Ebene	183
7.1.1	Experiment: Störangriffe durch Frequenzüberlagerung	183
7.1.2	WLAN-Jammer und Wi-Fi-Jammer	187
7.1.3	Gegenmaßnahmen zu Störangriffen und Wi-Fi-Jammern	188
7.2	Angriffe auf Netzwerkebene.....	192
7.2.1	DoS durch IP-Adressen-Allokation.....	192
7.2.2	Gegenmaßnahmen zu Angriffen auf Netzwerkebene.....	196
7.3	DoS durch Authentication Request Flooding.....	196
7.3.1	DoS durch Beacon Flooding.....	202
7.3.2	DoS durch Disassociation Attack.....	209
7.3.3	DoS durch Deauthentication Flooding.....	222
7.3.4	DoS durch Disassociation und Deauthentication Flooding	228
7.3.5	DoS durch CTS-Frame-Angriffe.....	229
7.3.6	Gegenmaßnahmen mithilfe des IEEE-802.11-Protokolls	238

8	WLAN-Authentifizierung umgehen	241
8.1	WLAN-Passwörter bei physischem Gerätezugriff auslesen	241
8.1.1	Windows: Passwort auslesen.....	241
8.1.2	Linux: Passwort auslesen	243
8.1.3	macOS: Passwort auslesen.....	244
8.1.4	Android: Passwort auslesen	244
8.1.5	iOS: Passwort auslesen	246
8.2	Verwendung von Standardpasswörtern	246
8.3	MAC-Spoofing – Umgehen von MAC-Filtern.....	259
8.3.1	MAC-Spoofing unter Windows	260
8.3.2	MAC-Spoofing unter Linux.....	262
8.3.3	MAC-Spoofing unter macOS.....	263
8.3.4	Beispiele von MAC-Filtern und ihrer Umgehung	263
8.4	Angriffe auf WEP.....	271
8.4.1	WEP-Schlüssel durch AP und STA(s) ermitteln	271
8.4.2	WEP-Schlüssel nur durch AP ermitteln.....	280
8.4.3	WEP-Schlüssel durch STA ermitteln (mit Hirte Attack)	292
8.4.4	Empfehlungen zu WEP	299
8.5	Angriffe auf WPS.....	299
8.5.1	Pixie Dust.....	302
8.5.2	reaver	304
8.5.3	Wenn der Angriff fehlschlägt.....	307
8.6	Angriffe auf WPA/WPA2	313
8.6.1	Access Point und Client in Reichweite	317
8.6.2	Wenn nur der Client verfügbar ist.....	323
8.6.3	Beschleunigung des Cracking-Vorgangs	331
8.6.4	Kryptografische Angriffe gegen WPA.....	338
8.6.5	Abwehrmaßnahmen	339
8.7	Angriffe auf WLAN-Infrastrukturen.....	340
8.7.1	Malicious SSID	340
8.7.2	Rogue Access Points.....	341
8.7.3	Fake-AP unter Kali Linux	344
8.7.4	Evil-Twin-Angriff.....	356
8.7.5	Evil Twin in der Praxis	358
9	Fortgeschrittene Angriffsszenarien	373
9.1	WLAN-Verkehr mitschneiden und entschlüsseln	373
9.1.1	Gegenmaßnahmen zu Sniffing.....	381
9.2	DNS-Spoofing.....	383
9.3	Windows-Rechner im WLAN übernehmen	398
9.4	Verbindung von einzelnen Endgeräten trennen.....	406
10	WLAN-Security-Monitoring	415
10.1	WIDS/WIPS-Infrastruktur	415
10.1.1	WIDS/WIPS-Komponenten.....	415

10.2	Analyse mithilfe von WIDS/WIPS.....	419
10.2.1	Geräteklassifizierung.....	420
10.2.2	Signaturanalyse	420
10.2.3	Verhaltensanalyse.....	421
10.2.4	Protokollanalyse	421
10.2.5	Spektrumanalyse und Performanceanalyse.....	423
10.2.6	Vorgehen bei Alarm und Mitteilung	423
11	WLAN-Security-Audits durchführen.....	425
11.1	Möglicher Ablauf eines WLAN-Security-Audits	425
11.1.1	Layer-1-Audit	425
11.1.2	Layer-2-Audit	427
11.1.3	Penetration Testing.....	428
11.1.4	Social Engineering	428
11.1.5	Sonstige Überprüfungen.....	428
11.2	Sicherheitsempfehlungen nach einem Audit	429
11.2.1	Einsatz starker Verschlüsselung.....	429
11.2.2	Durchgängig sichere Authentifizierung.....	429
11.2.3	Sensibilisierung der Mitarbeiter	430
11.2.4	Empfehlung einer WLAN-Policy	430
11.2.5	Empfehlungen zum Monitoring.....	430
11.2.6	Empfehlungen zur physischen Sicherheit.....	430
11.3	Ausrüstung für einen WLAN-Security-Audit.....	431
12	Kleinere Hacks und Tricks	433
12.1	Umgehung von Vorschaltseiten.....	433
12.2	WLAN-Adapter-Tuning.....	439
12.3	Wardriving.....	446
12.3.1	Wardriving in der Praxis.....	448
12.4	Störerhaftung – oder was davon übrig ist.....	452
12.5	Freifunk, die nicht kommerzielle Initiative.....	454
12.6	Alternative Router-Firmware	455
12.6.1	Freifunk.....	457
12.6.2	OpenWrt	459
12.6.3	DD-WRT.....	463
12.6.4	Freetz.....	469
12.6.5	Stock-Firmware wiederherstellen	470
12.6.6	Notfall-Recovery	475
12.6.7	Weitere alternative Firmware	478
12.7	Der Angreifer und seine Motive.....	479
12.7.1	Die Angreifer	479
12.7.2	Die Motive	481
12.8	Abwehrmaßnahmen kompakt	483
12.8.1	Die zehn wichtigsten Regeln beim Betrieb eines WLAN.....	483
12.8.2	Die fünf wichtigsten Regeln für eine stabile Heim-WLAN-Infrastruktur	484

14 *Inhaltsverzeichnis*

12.8.4	Sicherheit Ihres Access Point.....	484
12.8.5	Sicherheit Ihrer WLAN-Clients	485

13 **Epilog..... 487**

14 **Anhang..... 489**

14.1	Wireshark-Filter.....	489
14.1.1	Logische Operatoren	489
14.1.2	Verknüpfungsoperatoren	490
14.1.3	Filter nach Frame-Typ und Frame-Subtyp	490
14.1.4	Weitere nützliche Filter.....	490
14.1.5	Wildcards.....	491
14.2	Abkürzungsverzeichnis.....	491
14.3	Buchempfehlungen	494

15 **Literaturverzeichnis 497**

	Stichwortverzeichnis.....	503
--	---------------------------	-----