

# Inhaltsverzeichnis

	<b>Vorwort</b> .....	9
	<b>Einleitung</b> .....	11
	<b>Über die Autoren</b> .....	15
	<b>Danksagungen</b> .....	17
<b>1</b>	<b>Vorbereitung</b> .....	19
1.1	Organisatorische Vorbereitungen.....	19
1.2	Grundlegender Ablauf des Penetration Tests.....	20
1.3	Das Labor.....	24
1.4	Werkzeuge.....	26
1.4.1	Labornetzgerät.....	26
1.4.2	Multimeter.....	29
1.4.3	Computer.....	32
1.4.4	Oszilloskop.....	32
1.4.5	Logic Analyzer.....	32
1.4.6	Raspberry Pi als Universaltool.....	36
1.4.7	Abgreifklemmen und Adapter.....	41
<b>2</b>	<b>OSINT</b> .....	45
2.1	OSINT-Quellen.....	46
2.2	OSINT-Ziele im Produktumfeld.....	46
2.3	OSINT-Analyse.....	47
2.3.1	Hardware.....	48
2.3.2	Apps.....	51
2.3.3	Operations.....	55
2.3.4	Community.....	59
<b>3</b>	<b>Hardware</b> .....	61
3.1	Elektronikgrundlagen.....	61
3.1.1	Stromstärke, Spannung und Widerstand.....	62
3.2	Kleine Bausteinkunde.....	62
3.2.1	Diskrete Bauelemente.....	62
3.2.2	Integrierte Bauelemente (Integrated Circuit – IC).....	67

3.2.3	Bussysteme und Schnittstellen . . . . .	74
3.3	Schaltpläne und Layouts . . . . .	78
3.4	Datenblätter . . . . .	79
<b>4</b>	<b>Physische Sicherheit</b> . . . . .	<b>83</b>
4.1	Gehäuse . . . . .	84
4.1.1	Spezialschrauben . . . . .	86
4.1.2	Verklebungen . . . . .	86
4.1.3	Verschweißung (Kunststoff) . . . . .	87
4.1.4	Siegel und Plomben . . . . .	87
4.1.5	Elektronik und Elektromechanik. . . . .	88
4.1.6	Bausteinverblendung . . . . .	89
4.2	Designgrundlagen . . . . .	95
4.2.1	8-Bit-Controller mit HL-Kommunikationsbaustein. . . . .	96
4.2.2	32-Bit-Controller . . . . .	98
4.2.3	Android Embedded Device . . . . .	99
4.2.4	All-in-One-SoC . . . . .	100
4.2.5	Kombinationen . . . . .	100
4.3	Praktische Analyse . . . . .	100
4.3.1	Visuelles Hilfsdokument . . . . .	100
4.3.2	Entfernen des Schutzlacks . . . . .	104
4.4	Firmware-Extraktion am Gerät . . . . .	105
4.4.1	JTAG . . . . .	106
4.4.2	SWD. . . . .	107
4.4.3	Serielle Konsole (UART) . . . . .	114
4.4.4	USB . . . . .	122
4.4.5	SPI . . . . .	123
4.4.6	Bus Sniffing & Injection . . . . .	126
<b>5</b>	<b>Firmware</b> . . . . .	<b>131</b>
5.1	Dateisysteme . . . . .	133
5.2	Quellen von Firmware-Images . . . . .	135
5.2.1	Download des Firmware-Images aus dem Internet. . . . .	135
5.3	Firmware-Image entpacken . . . . .	138
5.3.1	Entpacken vorbereiten . . . . .	138
5.3.2	Manuelles Entpacken . . . . .	139
5.3.3	Toolgestütztes Entpacken. . . . .	142
5.3.4	Besondere Firmware-Images . . . . .	143

5.4	Statische Firmware-Analyse .....	145
5.4.1	Manuelle Analyse .....	147
5.4.2	Toolgestützte Analyse .....	149
5.5	Firmware-Emulation .....	150
5.6	Dynamische Firmware-Analyse .....	154
5.7	Firmware-Manipulation .....	157
<b>6</b>	<b>IoT-Referenzarchitekturen und Netzwerkprotokolle .....</b>	<b>163</b>
6.1	Einführung in Protokolle .....	163
6.2	IoT-Referenzarchitekturen .....	164
6.3	Bluetooth Low Energy .....	167
6.3.1	Protokoll-Stack .....	168
6.3.2	Kommunikation zwischen Geräten .....	169
6.3.3	Bluetooth LE – Sicherheit .....	178
6.3.4	Klassische Bluetooth-Angriffe .....	179
6.3.5	Praktische Bluetooth-LE-Angriffe .....	180
6.4	Zigbee .....	195
6.4.1	Protokoll-Stack .....	195
6.4.2	Netzwerk .....	197
6.4.3	Zigbee-Schwachstellen .....	200
<b>7</b>	<b>MQTT .....</b>	<b>205</b>
7.1	Funktionsweise .....	206
7.2	Quality of Service (QoS) .....	209
7.3	Retained Messages .....	209
7.4	Last Will and Testament .....	210
7.5	Pakettypen .....	210
<b>8</b>	<b>Apps .....</b>	<b>217</b>
8.1	OWASP MASVS .....	218
8.2	Die App herunterladen .....	219
8.2.1	iOS .....	220
8.2.2	Android .....	221
8.3	Statische Analyse .....	222
8.4	Dynamische Analyse .....	224
8.4.1	BlackBox .....	225
<b>9</b>	<b>Backend, Web und Cloud .....</b>	<b>233</b>
9.1	Vorbereitung .....	233
9.1.1	Microsoft Azure .....	235

Inhaltsverzeichnis

9.1.2	Amazon Web Service (AWS) .....	236
9.1.3	Google Cloud Service .....	237
9.2	Testen von Webapplikationen .....	237
9.2.1	OWASP Top 10 2017 .....	238
9.2.2	OWASP Testing Guide .....	242
	<b>Stichwortverzeichnis</b> .....	<b>249</b>