

Spis treści

O autorze	13
O korektorach merytorycznych	14
Wstęp	15
Część I. Zapoznanie ze sprzętem	19
Rozdział 1. Przygotowanie laboratorium do testów penetracyjnych i zasady bezpieczeństwa	21
Podstawowe wymagania — co będzie potrzebne?	22
Języki programowania	22
Umiejętności związane ze sprzętem	22
Konfiguracja systemu	23
Przygotowanie podstawowego laboratorium	24
Bezpieczeństwo	24
Zakup wyposażenia testowego	25
Laboratorium domowe kontra firmowe	26
Wybór urządzeń	26
Co kupić, po co i kiedy?	27
Drobne narzędzia i sprzęt	36
Wynajem i zakup przyrządów	37
Zapas elementów elektronicznych	38
Przechowywanie	38
Zapas	38

Przykładowe laboratoria	39
Poziom początkującego	40
Poziom amatora	40
Poziom profesjonalisty	41
Podsumowanie	42
Pytania	42
Rozdział 2. Przedmiot testu	43
Blok procesora	44
Zadania procesora	44
Typowe rodzaje procesorów stosowanych w systemach wbudowanych	44
Blok pamięci	47
Pamięć RAM	47
Pamięć programu	47
Pamięć danych	47
Blok zasilania	48
Blok zasilania z perspektywy testów penetracyjnych	48
Blok sieci	48
Typowe protokoły komunikacyjne stosowane w systemach wbudowanych	49
Blok czujników	53
Czujniki analogowe	53
Czujniki cyfrowe	54
Blok urządzeń wykonawczych	55
Blok interfejsów	55
Podsumowanie	56
Pytania	56
Dalsza lektura	56
Rozdział 3. Komponenty testowanego systemu	57
Wymagania techniczne	57
Pozyskiwanie informacji z instrukcji obsługi	58
Podejście analityczne	58
Analiza instrukcji do zabawki	59
Pozyskiwanie informacji z internetu	60
Informacje o zabawce	60
Utworzenie diagramu systemu	63
Diagram zabawki	64
Eksplorowanie systemu — identyfikowanie komponentów i umieszczanie ich na diagramie	65
Otwarcie zabawki	65
Manipulowanie systemem	65
Demontaż zabawki	66
Identyfikacja układów	66
Układy zastosowane w zabawce	66
Identyfikacja nieoznaczonych i tajemniczych układów	70
Tajemnicza zawartość zabawki	71
Granice bloków funkcjonalnych	77
Podsumowanie	77
Pytania	78

Rozdział 4. Planowanie i przygotowanie testu	79
Metodyka STRIDE	79
Wyszukiwanie celów ataków w badanym systemie	81
Aspekty bezpieczeństwa — czego należy oczekiwać?	84
Komunikacja	84
Utrzymanie	85
Spójność systemu i auto-testy	85
Ochrona poufnych danych i środków bezpieczeństwa	85
Jakie są ataki i ich skutki?	86
Metodyka STRIDE w analizie bezpieczeństwa komponentów systemu	86
Przykładowy system: zabawka Furby	87
Planowanie testu	89
Wybór scenariusza	90
Podsumowanie	94
Pytania	94
Dalsza lektura	94

Część II. Atakowanie sprzętu **95**

Rozdział 5. Główna platforma ataku	97
Wymagania techniczne	97
Wprowadzenie do płytki bluepill	98
Do czego służy płytka bluepill?	98
Co to jest?	98
Dlaczego język C, a nie Arduino?	99
Dokumentacja	100
Rejestry pamięci	101
Narzędzia programistyczne	101
Proces kompilacji	101
Przebieg kompilacji	102
Programowanie układu	104
Praktyczne zastosowanie płytki bluepill	104
Wprowadzenie do języka C	106
Operatory	106
Typy danych	108
Ten okropny wskaźnik	108
Dyrektywy preprocesora	109
Funkcje	110
Podsumowanie	110
Pytania	110
Dalsza lektura	111

Rozdział 6. Podśluchiwanie i atakowanie najpopularniejszych protokołów	112
Wymagania techniczne	112
Sprzęt	113
Protokół I²C	113
Tryby pracy	114
Podśluchiwanie transmisji	120
Wstrzykiwanie danych	124
Atak typu „człowiek pośrodku”	125
Protokół SPI	125
Tryby pracy	126
Podśluchiwanie transmisji	128
Wstrzykiwanie danych	129
Atak typu „człowiek pośrodku”	129
Protokół UART	130
Tryby pracy	131
Podśluchiwanie transmisji	132
Wstrzykiwanie danych	132
Atak typu „człowiek pośrodku”	133
Protokół D1W	134
Tryby pracy	134
Podśluchiwanie transmisji	135
Wstrzykiwanie danych	136
Atak typu „człowiek pośrodku”	137
Podsumowanie	137
Pytania	137
Rozdział 7. Wyodrębnianie i modyfikowanie pamięci	139
Wymagania techniczne	139
Wyszukiwanie układów pamięci	140
Pamięć EEPROM	140
Pamięci EMMC i NAND/NOR flash	140
Dyski magnetyczne i SSD oraz inne nośniki	141
Wyodrębnianie danych	141
Oprogramowanie układowe	141
Pamięć wbudowana i niestandardowe interfejsy	142
Pamięć wbudowana i typowe interfejsy	142
Badanie struktury nieznanego nośnika	144
Nieznane formaty nośników	144
Znane formaty pamięci masowych	145
Zabawka Furby	145
Montowanie systemu plików	150
Przepakowanie danych	151
Podsumowanie	151
Pytania	151
Dalsza lektura	152

Rozdział 8. Atakowanie Wi-Fi, Bluetooth i BLE	153
Wymagania techniczne	153
Podstawy komunikacji sieciowej	154
Komunikacja Wi-Fi w systemach wbudowanych	154
Wybór karty Wi-Fi	155
Utworzenie punktu dostępu	155
Przygotowanie punktu dostępu i podstawowych usług sieciowych	156
Inne ataki na sieć Wi-Fi	158
Komunikacja Bluetooth w systemach wbudowanych	158
Podstawy komunikacji Bluetooth	158
Wykrywanie urządzeń Bluetooth	159
Narzędzia Bluetooth w systemie Linux	162
Podsluchiwanie komunikacji Bluetooth na komputerze	164
Podsluchiwanie surowej komunikacji Bluetooth	165
BLE	167
Podsumowanie	171
Pytania	171
Rozdział 9. Atakowanie SDR	172
Wymagania techniczne	172
Wprowadzenie do technologii SDR	173
Opis i dobór sprzętu	173
Badanie urządzenia radiowego	174
Odbieranie sygnału: antena	174
Analiza spektrum radiowego	176
Odtwarzanie danych	178
Rozpoznawanie modulacji — edukacyjny przykład	181
AM/ASK	181
FM/FSK	182
PM/PSK	183
MSK	184
Analiza sygnału	184
Demodulacja sygnału	185
Blok Clock Recovery MM	189
Narzędzie WPCR	190
Wysyłanie sygnałów	191
Podsumowanie	191
Pytania	191
Część III. Atakowanie oprogramowania	193
Rozdział 10. Korzystanie z interfejsów diagnostycznych	195
Wymagania techniczne	195
Programowalne interfejsy diagnostyczne — czym są i do czego służą?	196
Właściwe przeznaczenie interfejsów diagnostycznych	196
Atakowanie systemu przy użyciu interfejsu JTAG	196

Identyfikowanie pinów	201
„Przyjazna” płyta drukowana	201
Trudniejszy przypadek	204
Bardzo trudny przypadek i płytka JTAGulator	204
Oprogramowanie OpenOCD	207
Instalacja	207
Plik adaptera	208
Docelowy plik	210
Praktyczny przykład	213
Podsumowanie	217
Pytania	218
 Rozdział 11. Statyczna inżynieria odwrotna i analiza	 219
Wymagania techniczne	219
Formaty plików wykonywalnych	220
Popularne formaty plików wykonywalnych	221
Formaty rzutów i obrazy pamięci	224
Struktura rzutu pamięci — przykład płytki bluepill	225
Analiza oprogramowania układowego — wprowadzenie do programu Ghidra	226
Analiza prostego programu dla systemu Linux i procesora ARM	227
Wyższy stopień wtajemniczenia — analiza surowego pliku binarnego dla płytki STM32	234
Pierwszy przebieg identyfikacyjny	237
Inżynieria odwrotna funkcji	241
Podsumowanie	242
Pytania	243
 Rozdział 12. Dynamiczna inżynieria odwrotna	 244
Wymagania techniczne	244
Dynamiczna inżynieria odwrotna i jej zastosowania	245
Zastosowanie programów OpenOCD i GDB	245
GDB? Nic o nim nie wiem!	247
Wprowadzenie do asemblera ARM	250
Ogólne informacje i składnia	250
Najbardziej przydatne instrukcje procesora ARM	253
Przykład dynamicznej inżynierii odwrotnej	258
Badanie kodu za pomocą programu Ghidra	258
Odtworzenie hasła	259
Prostsze rozwiązanie	266
Podsumowanie	267
Pytania	267
 Rozdział 13. Ocenianie i raportowanie zagrożeń	 268
Ocenianie zagrożeń	269
Raportowanie zrozumiałe dla wszystkich	271
Szablon raportu	272
Język raportu	273
Jakość raportu	273

Konfrontacja z inżynierami	274
Podsumowanie	276
Pytania	276
Rozdział 14. Podsumowanie — środki zaradcze i dobre praktyki	277
Dobre praktyki branżowe, czym są i gdzie ich szukać?	278
OWASP IoT Top 10	278
Testy porównawcze CIS	280
Wytyczne NIST dotyczące bezpieczeństwa sprzętu	280
Typowe problemy i środki zaradcze	281
Nawiązywanie zabezpieczonego połączenia między urządzeniem a zapleczem	281
Przechowywanie poufnych danych	282
Kryptografia w krytycznych aplikacjach	283
Programy rozruchowe oraz interfejsy szeregowy, JTAG i UART	283
Co dalej? Samodzielna nauka i pierwszy projekt	284
Słowo końcowe	285
Odpowiedzi	287