

Spis treści

O autorach	13
O współautorach	13
O korektorze merytorycznym	14
PRZEDMOWA	15
PODZIĘKOWANIA	17
WPROWADZENIE	19
Koncepcja książki	19
Dla kogo jest ta książka?	20
Kali Linux	21
Struktura książki	21
 Część I. Krajobraz zagrożeń IoT	 25
 i	
BEZPIECZEŃSTWO W ŚWIECIE IOT	27
Dlaczego bezpieczeństwo IoT jest ważne?	28
Czym różni się bezpieczeństwo IoT od tradycyjnego bezpieczeństwa IT?	30
Co jest specjalnego w hakowaniu IoT?	31
Normy, regulacje i wytyczne	32
Studium przypadku: identyfikowanie, zgłaszanie i ujawnianie problemów z bezpieczeństwem IoT	36
Zdaniem eksperta: poruszanie się po świecie IoT	37
Regulacje dotyczące hakowania IoT	37
Rola rządu w bezpieczeństwie IoT	39
Bezpieczeństwo urządzeń medycznych z perspektywy pacjentów	40
Podsumowanie	42
 2	
MODELOWANIE ZAGROŻEŃ	43
Modelowanie zagrożeń IoT	43
Regulacje dotyczące modelowania zagrożeń	44
Identyfikacja architektury urządzenia	45
Podział architektury na komponenty	46

Określenie zagrożeń	47
Wykrywanie zagrożeń za pomocą drzewa ataku	54
Ocena zagrożenia przy użyciu klasyfikacji DREAD	55
Inne modele zagrożeń, podejścia i narzędzia	56
Typowe zagrożenia IoT	57
Zakłócanie sygnału	58
Odtwarzanie danych	58
Zniekształcanie ustawień	58
Naruszenie integralności sprzętu	58
Klonowanie węzłów	58
Naruszenie bezpieczeństwa i prywatności danych	59
Niska świadomość zagrożeń	59
Podsumowanie	59

3

METODYKA TESTÓW BEZPIECZEŃSTWA.....60

Pasywny rekonesans	62
Warstwa fizyczna lub sprzętowa	65
Interfejsy peryferyjne	65
Środowisko rozruchowe	66
Blokady	66
Zabezpieczenia przed modyfikacjami i wykrywanie modyfikacji	66
Oprogramowanie układowe	67
Interfejsy diagnostyczne	67
Fizyczna odporność	67
Warstwa sieciowa	68
Rekonesans	68
Ataki na protokoły i usługi sieciowe	71
Testy protokołów bezprzewodowych	72
Testy aplikacji WWW	73
Tworzenie mapy aplikacji	73
Kontrolki klienckie	74
Uwierzytelnianie użytkowników	74
Zarządzanie sesjami	75
Kontrola dostępu i autoryzacja	75
Weryfikacja danych wejściowych	75
Błędy w algorytmie	76
Serwer aplikacyjny	76
Przegląd konfiguracji hosta	76
Konta użytkowników	76
Siła haseł	77
Uprawnienia kont	77
Poziom poprawek	78
Zdalne utrzymanie	78
Kontrola dostępu do systemu plików	79
Szyfrowanie danych	79
Błędy w konfiguracji serwera	79
Testy aplikacji przenośnych i chmurowych	80
Podsumowanie	81

Część II. Hakowanie sieci

83

4

OCENIANIE SIECI.....	85
Skok w sieć IoT	85
Sieci VLAN i przełączniki sieciowe	86
Imitowanie przełącznika	87
Podwójne tagowanie	90
Imitowanie urządzeń VoIP	91
Identyfikowanie urządzeń IoT w sieci	93
Uzyskiwanie haseł poprzez badanie odpowiedzi usług	94
Tworzenie własnych sygnatur usług	98
Hakowanie protokołu MQTT	100
Przygotowanie środowiska testowego	102
Tworzenie modułu dla programu Ncrack do hakowania poświadczeń w protokole MQTT	104
Test modułu MQTT	114
Podsumowanie	114

5

ANALIZA PROTOKOŁÓW SIECIOWYCH.....	115
Badanie protokołów sieciowych	116
Gromadzenie informacji	116
Analiza	118
Prototypowanie i tworzenie narzędzi	119
Ocena bezpieczeństwa protokołu	119
Tworzenie dekodera protokołu DICOM w języku Lua dla programu Wireshark	121
Język lua	121
Protokół DICOM	121
Generowanie ruchu DICOM	123
Włączenie języka Lua w programie Wireshark	123
Zdefiniowanie dekodera	125
Zdefiniowanie głównej funkcji dekodera	125
Skompletowanie dekodera	126
Tworzenie dekodera żądań C-ECHO	127
Wyodrębnienie ciągów znaków z tytułu jednostki aplikacji	128
Uzupełnienie funkcji dekodującej	128
Analiza pól o zmiennych długościach	129
Test dekodera	130
Tworzenie skanera usługi DICOM dla silnika skryptowego Nmap	131
Utworzenie biblioteki Nmap dla protokołu DICOM	131
Identyfikatory DICOM i stałe wartości	132
Zdefiniowanie funkcji tworzącej i usuwającej gniazdo sieciowe	133
Zdefiniowanie funkcji wysyłającej i odbierającej pakiet DICOM	134
Utworzenie nagłówka pakietu DICOM	135
Utworzenie funkcji wysyłającej żądanie A-ASSOCIATE	136
Odczytanie parametrów skryptu w silniku Nmap	138
Zdefiniowanie struktury żądania A-ASSOCIATE	138
Analiza odpowiedzi A-ASSOCIATE	140
Utworzenie finalnego skryptu	140
Podsumowanie	142

6	
EKSPLORACJA SIECI SAMOKONFIGURACYJNYCH.....	143
Eksploracja protokołu UPnP	144
Stos protokołu UPnP	145
Typowe wady protokołu UPnP	146
Otwieranie przejść w zaporze sieciowej	147
Atakowanie protokołu UPnP poprzez interfejs WAN	153
Inne ataki na protokół UPnP	158
Eksploracja protokołów mDNS i DNS-SD	158
Jak działa protokół mDNS?	159
Jak działa protokół DNS-SD?	159
Rekonesans przy użyciu protokołów mDNS i DNS-SD	160
Atak na operację sondowania w protokole mDNS	162
Ataki typu „człowiek pośrodku” na protokoły mDNS i DNS-SD	163
Eksploracja protokołu WS-Discovery	172
Jak działa protokół WS-Discovery?	172
Imitowanie kamery	173
Ataki na protokół WS-Discovery	180
Podsumowanie	181

Część III. Hakowanie sprzętu 183

7	
EKSPLORACJA UART, JTAG I SWD.....	185
Interfejs UART	186
Narzędzia sprzętowe wykorzystujące interfejs UART	187
Identyfikacja pinów interfejsu UART	187
Określenie prędkości transmisji interfejsu UART	191
Interfejsy JTAG i SWD	192
Interfejs JTAG	192
Jak działa interfejs SWD?	193
Narzędzia sprzętowe wykorzystujące interfejsy JTAG i SWD	193
Identyfikacja pinów interfejsu JTAG	194
Hakowanie urządzenia za pomocą interfejsów UART i SWD	196
Hakowanie mikrokontrolera STM32F103C8T6 (black pili)	197
Przygotowanie środowiska diagnostycznego	198
Utworzenie programu w środowisku Arduino IDE	200
Załadowanie i uruchomienie programu	203
Diagnozowanie urządzenia	209
Podsumowanie	217
8	
INTERFEJSY SPI I I²C.....	218
Narzędzia do komunikacji z interfejsami SPI i I ² C	219
Interfejs SPI	220
Jak działa interfejs SPI?	220
Odczyt zawartości pamięci EEPROM/flash za pomocą interfejsu SPI	221
Interfejs I ² C	226
Jak działa interfejs I ² C?	226
Utworzenie szyny I ² C typu kontroler - urządzenie peryferyjne	227
Hakowanie interfejsu I ² C za pomocą urządzenia Bus Pirate	232
Podsumowanie	236

HAKOWANIE OPROGRAMOWANIA UKŁADOWEGO.....	237
Oprogramowanie układowe i system operacyjny	237
Uzyskanie oprogramowania układowego	238
Hakowanie routera Wi-Fi	241
Wyodrębnienie systemu plików	242
Statyczna analiza zawartości systemu plików	243
Emulacja oprogramowania układowego	246
Analiza dynamiczna	252
Otwieranie ukrytych wejść do oprogramowania układowego	254
Hakowanie mechanizmu aktualizacji oprogramowania układowego	259
Kompilacja i konfiguracja	260
Kod klienta	261
Uruchomienie usługi aktualizacji	264
Luki w bezpieczeństwie usługi aktualizacji oprogramowania	265
Podsumowanie	267

Część IV. Hakowanie radia

269

RADIO KRÓTKIEGO ZASIĘGU: NADUŻYWANIE RFID.....	271
Jak działa RFID?	271
Zakresy częstotliwości radiowych	272
Pasywne i aktywne technologie RFID	273
Architektura tagu RFID	275
Tagi RFID niskiej częstotliwości	276
Tagi RFID wysokiej częstotliwości	277
Atakowanie systemów RFID za pomocą urządzenia Proxmark3	277
Przygotowanie narzędzia Proxmark3	278
Aktualizacja urządzenia Proxmark3	278
Identyfikacja tagów niskiej i wysokiej częstotliwości	280
Klonowanie tagu niskiej częstotliwości	281
Klonowanie tagu wysokiej częstotliwości	282
Symulowanie tagu RFID	287
Modyfikacja tagu RFID	287
Atakowanie karty MIFARE za pomocą aplikacji Android	288
Ogólne polecenia dla nieoznaczonych i niekomercyjnych tagów RFID	289
Podłuchiwanie komunikacji między tagiem a czytnikiem	293
Wyodrębnianie klucza sektora z zarejestrowanych danych	294
Atakowanie czytnika RFID	295
Automatyzacja ataków przy użyciu skryptów Proxmark3	296
Zakłócanie czytnika RFID za pomocą własnego skryptu	297
Podsumowanie	301

TECHNOLOGIA BLE.....	302
Jak działa technologia BLE?	303
Profile GAP i GATT	304

Korzystanie z technologii BLE	305
Urządzenia BLE	305
BlueZ	306
Konfiguracja interfejsów BLE	307
Wykrywanie urządzeń i wyświetlanie charakterystyk	308
Narzędzie GATTTool	308
Narzędzie Bettercap	309
Uzyskiwanie listy charakterystyk, usług i deskryptorów	310
Odczytywanie i zapisywanie charakterystyk	311
Hakowanie technologii BLE	312
Przygotowanie projektu BLE CTF Infinity	312
Pierwsze kroki	313
Flaga 1 — zbadanie charakterystyk i deskryptorów	315
Flaga 2 — uwierzytelnienie	316
Flaga 3 — podszycie się pod adres MAC	317
Podsumowanie	319

12

RADIO ŚREDNIEGO ZASIĘGU: HAKOWANIE WI-FI.....320

Jak działa Wi-Fi?	320
Sprzęt do oceniania bezpieczeństwa Wi-Fi	321
Ataki na klientów sieci Wi-Fi	321
Ataki dysocjacyjne i blokujące usługę	322
Ataki asocjacyjne	324
Wi-Fi Direct	329
Ataki na punkty dostępu	332
Łamanie szyfrowania WPA/WPA2	333
Łamanie szyfrowania WPA/WPA2 Enterprise i przechwytywanie poświadczeń	338
Metodyka testów bezpieczeństwa	339
Podsumowanie	340

13

RADIO DALEKIEGO ZASIĘGU: LPWAN.....341

LPWAN, LoRa i LoRaWAN	342
Przechwytywanie danych w sieci LoRaWAN	343
Przygotowanie płytki Heltec LoRa 32	343
Przygotowanie klucza LoStik	348
Klucz USB CatWAN jako rejestrator pakietów	352
Dekodowanie protokołu LoRaWAN	357
Format pakietu LoRaWAN	357
Dołączanie do sieci LoRaWAN	359
Hakowanie sieci LoRaWAN	361
Atak bit-flipping	362
Generowanie kluczy i zarządzanie nimi	365
Ataki odtworzeniowe	365
Podsłuchiwanie komunikacji	366
Fałszowanie potwierdzeń	366
Ataki aplikacyjne	366
Podsumowanie	367

Część V. Celowanie w ekosystem IoT

369

14

ATAKI NA APLIKACJE MOBILNE.....	371
Zagrożenia aplikacji mobilnych IoT	372
Komponenty środowiska aplikacji mobilnych	372
Identyfikacja zagrożeń	372
Zabezpieczenia w systemach Android i iOS	374
Ochrona danych i szyfrowany system plików	374
Odizolowane otoczenie aplikacji, bezpieczna komunikacja międzyprocesowa, usługi	375
Podpisy aplikacji	376
Uwierzytelnienie użytkownika	376
Odizolowane komponenty sprzętowe i zarządzanie kluczami	377
Zweryfikowany i bezpieczny rozruch	377
Analiza aplikacji dla systemu iOS	377
Przygotowanie środowiska testowego	378
Wyodrębnienie i ponowne podpisanie pakietu IPA	379
Analiza statyczna	380
Analiza dynamiczna	383
Wstrzykiwanie danych	390
Magazyn łańcucha kluczy	391
Dekompilacja pliku binarnego	391
Przechwytywanie i badanie danych sieciowych	393
Omijanie wykrywania włamań poprzez wprowadzanie dynamicznych zmian w kodzie	394
Omijanie wykrywania włamań poprzez wprowadzanie statycznych zmian w kodzie	395
Analiza aplikacji dla systemu Android	397
Przygotowanie środowiska testowego	397
Wyodrębnienie pliku APK	398
Analiza statyczna	399
Dekompilacja pliku binarnego	400
Analiza dynamiczna	400
Przechwytywanie i badanie danych sieciowych	405
Boczne kanały wycieku danych	405
Omijanie wykrywania włamań poprzez wprowadzanie statycznych zmian w kodzie	406
Omijanie wykrywania włamań poprzez wprowadzanie dynamicznych zmian w kodzie	408
Podsumowanie	408

15

HAKOWANIE INTELIGENTNEGO DOMU.....	409
Uzyskanie fizycznego dostępu do budynku	410
Sklonowanie karty RFID do inteligentnego zamka	410
Zakłócanie bezprzewodowego systemu alarmowego	413
Odtwarzanie strumienia wideo z kamery IP	417
Protokoły strumieniowe	418
Analiza danych przesyłanych przez kamerę IP	418
Wyodrębnienie strumienia wideo	420
Hakowanie inteligentnej bieżni treningowej	423
Inteligentna bieżnia i system Android	424
Przejęcie kontroli nad inteligentną bieżnią	425
Podsumowanie	438