UNIWERSYTET KOMISJI EDUKACJI NARODOWEJ
W KRAKOWIE

Instytut Bezpieczeństwa i Informatyki

BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ I SYSTEMÓW STEROWANIA PRZEMYSŁOWEGO IOT

Temat numer: 9

Temat: Analiza Bezpieczeństwa i Podatności Inteligentnego Gniazdka, Przeprowadzenie analizy bezpieczeństwa
(w kontrolowanym środowisku laboratoryjnym)

Autorzy:

Imię i Nazwisko: Anna Płaczek

Imię i Nazwisko: Joanna Szewczyk

Imię i Nazwisko: Emilia Zaręba

Imię i Nazwisko: Katarzyna Zieleniewska

Numer grupy: L3

Spis treści

1. Streszczenie

Celem niniejszego raportu była analiza bezpieczeństwa inteligentnego gniazdka IoT TP-Link Tapo P100 przeprowadzona w warunkach laboratoryjnych z wykorzystaniem środowiska wirtualnego. Badania wykonano przy użyciu maszyn wirtualnych (VMware) oraz narzędzi do analizy ruchu sieciowego i rekonesansu, takich jak Wireshark, Nmap oraz arp-scan.

W pracy opisano konfigurację środowiska testowego, identyfikację urządzenia w sieci lokalnej oraz podstawową analizę jego komunikacji sieciowej. Szczególną uwagę poświęcono zagadnieniom bezpieczeństwa transmisji danych oraz potencjalnym zagrożeniom charakterystycznym dla urządzeń Internetu Rzeczy, w tym zależności od usług chmurowych i ograniczonej widoczności protokołów komunikacyjnych.

Na podstawie dostępnych informacji oraz publicznych baz podatności (CVE) dokonano oceny ryzyka związanego z eksploatacją badanego urządzenia. Raport kończy się zestawem rekomendacji mających na celu zwiększenie poziomu bezpieczeństwa urządzeń IoT w sieci lokalnej.

2. Wstęp

2.1. Cel i zakres pracy

Celem niniejszej pracy jest analiza bezpieczeństwa konsumenckiego urządzenia Internetu Rzeczy – inteligentnego gniazdka TP-Link Tapo P100 – przeprowadzona w warunkach laboratoryjnych. Badanie ma na celu ocenę potencjalnych zagrożeń związanych z eksploatacją urządzenia w sieci lokalnej oraz identyfikację podstawowych mechanizmów zabezpieczających zastosowanych przez producenta.

Zakres pracy obejmuje identyfikację urządzenia w sieci lokalnej, rekonesans sieciowy, analizę komunikacji sieciowej oraz przegląd znanych podatności bezpieczeństwa opisanych w publicznych bazach CVE. Na podstawie uzyskanych wyników sformułowano wnioski oraz rekomendacje dotyczące bezpiecznego użytkowania urządzeń IoT.

2.2. Założenia oraz ograniczenia środowiska laboratoryjnego

Analiza została przeprowadzona w kontrolowanym środowisku laboratoryjnym z wykorzystaniem maszyn wirtualnych oraz prywatnej sieci lokalnej. Badania dotyczyły wyłącznie własnego urządzenia i własnej infrastruktury sieciowej. Do analizy wykorzystano ogólnodostępne narzędzia, takie jak Wireshark, Nmap oraz arp-scan, bez ingerencji w oprogramowanie urządzenia.

Ograniczeniem analizy był brak możliwości pełnego wglądu w treść komunikacji sieciowej, wynikający z zastosowania szyfrowania TLS oraz mechanizmów zabezpieczających po stronie producenta. Dodatkowym ograniczeniem była zależność urządzenia od infrastruktury chmurowej, co utrudnia szczegółową analizę protokołów aplikacyjnych.

3. Opis badanego urządzenia IoT

3.1. Identyfikacja urządzenia (model, HW, firmware)

Badanym urządzeniem w niniejszej pracy jest inteligentne gniazdko Internetu Rzeczy TP-Link Tapo P100, należące do konsumenckiej serii urządzeń smart home firmy TP-Link. Urządzenie przeznaczone jest do użytku domowego i umożliwia zdalne sterowanie zasilaniem podłączonych odbiorników elektrycznych za pośrednictwem aplikacji mobilnej.

Identyfikacja urządzenia została przeprowadzona na podstawie informacji dostępnych w aplikacji mobilnej Tapo oraz danych producenta. W trakcie analizy ustalono następujące parametry:

- Model: TP-Link Tapo P100
- Wersja sprzętowa (HW): 2.0
- Wersja firmware: 1.2.5 (Build 240411)

Urządzenie łączy się z siecią lokalną za pośrednictwem interfejsu Wi-Fi i jest identyfikowane w sieci przez adres IP przydzielany dynamicznie (DHCP) oraz adres MAC przypisany do producenta TP-Link. W trakcie rekonesansu sieciowego możliwa była jego jednoznaczna identyfikacja na podstawie identyfikatora OUI.

3.2. Charakterystyka funkcjonalna i sposób działania

TP-Link Tapo P100 jest urządzeniem typu smart plug, którego podstawową funkcją jest zdalne włączanie i wyłączanie zasilania podłączonych urządzeń

elektrycznych. Sterowanie odbywa się za pomocą dedykowanej aplikacji mobilnej Tapo, dostępnej na platformy Android oraz iOS. Urządzenie nie posiada lokalnego interfejsu użytkownika, a jego konfiguracja i obsługa realizowane są wyłącznie poprzez aplikację.

Architektura działania gniazdka opiera się na modelu komunikacji z wykorzystaniem infrastruktury chmurowej producenta. Aplikacja mobilna komunikuje się z serwerami chmurowymi TP-Link, które następnie pośredniczą w komunikacji z urządzeniem znajdującym się w sieci lokalnej. Oznacza to, że sterowanie gniazdkiem nie odbywa się bezpośrednio w obrębie sieci LAN, lecz z wykorzystaniem połączenia zewnętrznego.

Z punktu widzenia bezpieczeństwa istotne jest, że komunikacja pomiędzy aplikacją, chmurą oraz urządzeniem realizowana jest w sposób zaszyfrowany, z wykorzystaniem protokołu TLS. Brak lokalnego interfejsu zarządzania oraz zależność od infrastruktury chmurowej wpływają zarówno na funkcjonalność urządzenia, jak i na potencjalne wektory ataku, które zostały omówione w dalszych częściach raportu.

4. Środowisko testowe i narzędzia

Środowisko testowe składało się z następujących elementów:

- komputer hosta z systemem Windows,
- oprogramowanie wirtualizacyjne VMware Workstation,
- maszyna wirtualna z systemem Linux (Kali Linux),
- inteligentne gniazdko TP-Link Tapo P100,
- smartfon z aplikacją mobilną Tapo,
- sieć Wi-Fi 2.4 GHz zapewniająca łączność urządzenia IoT.

4.1. Topologia sieci testowej

Środowisko testowe obejmowało sieć Wi-Fi 2.4 GHz z routerem pełniącym funkcję DHCP. Inteligentne gniazdko Tapo P100 oraz smartfon były podłączone do tej samej sieci Wi-Fi. Maszyna wirtualna Kali Linux działała w trybie Bridged, dzięki czemu otrzymała adres IP z tej samej podsieci i mogła pasywnie rejestrować ruch oraz wykonywać rekonesans.

4.2. Wykorzystane narzędzia

W procesie analizy bezpieczeństwa posłużono się zestawem standardowych narzędzi diagnostycznych i audytowych, umożliwiających weryfikację zabezpieczeń sieciowych oraz systemowych. Wykorzystano następujące oprogramowanie:

arp-scan - identyfikacja aktywnych hostów w sieci lokalnej poprzez analizę adresów fizycznych (MAC) i logicznych (IP).

Nmap - skanowanie portów, enumeracja dostępnych usług sieciowych oraz detekcja wersji oprogramowania.

tcpdump - akwizycja ruchu sieciowego i jego archiwizacja w formacie PCAP do późniejszej analizy.

Wireshark - głęboka inspekcja pakietów (DPI), ze szczególnym uwzględnieniem analizy protokołów DNS, TLS oraz rozszerzeń SNI.

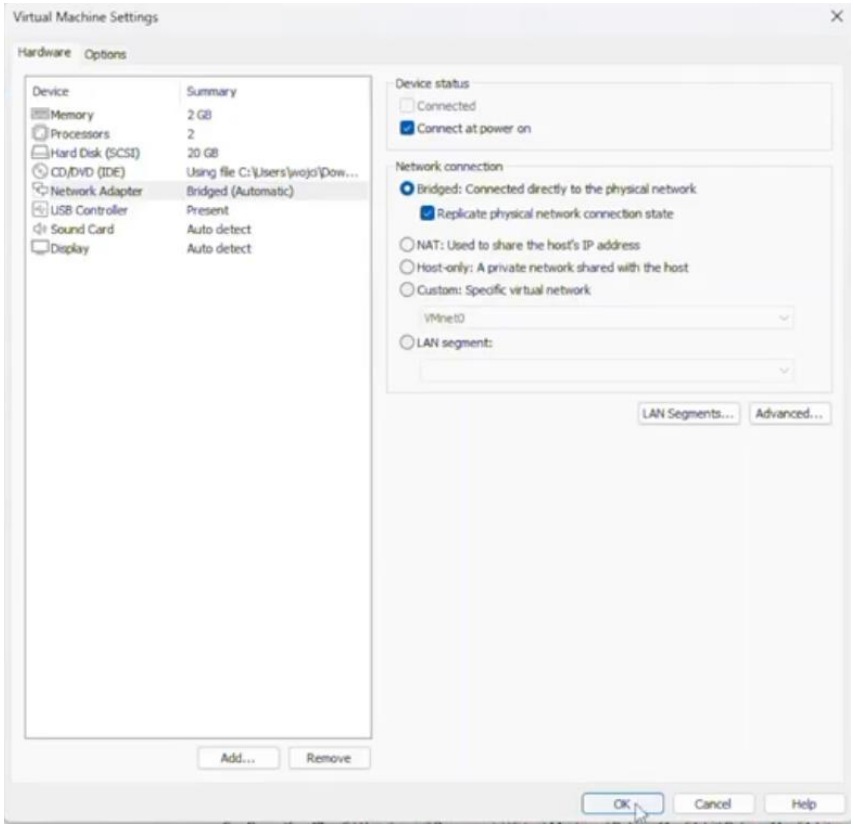
mitmproxy - weryfikacja odporności komunikacji na ataki typu Man-in-the-Middle (przechwytywanie i modyfikacja ruchu).

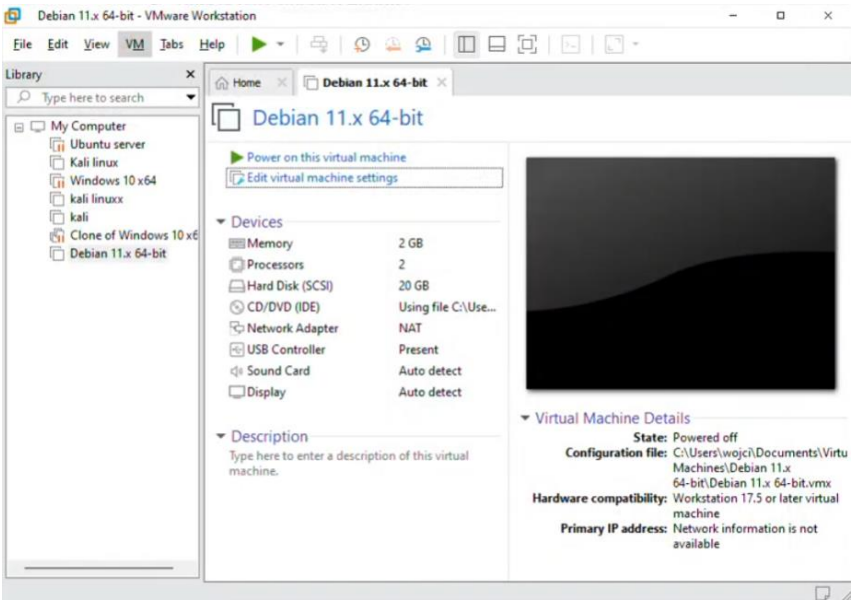
VMware Workstation - platforma wirtualizacyjna stanowiąca bazę dla środowiska testowego.

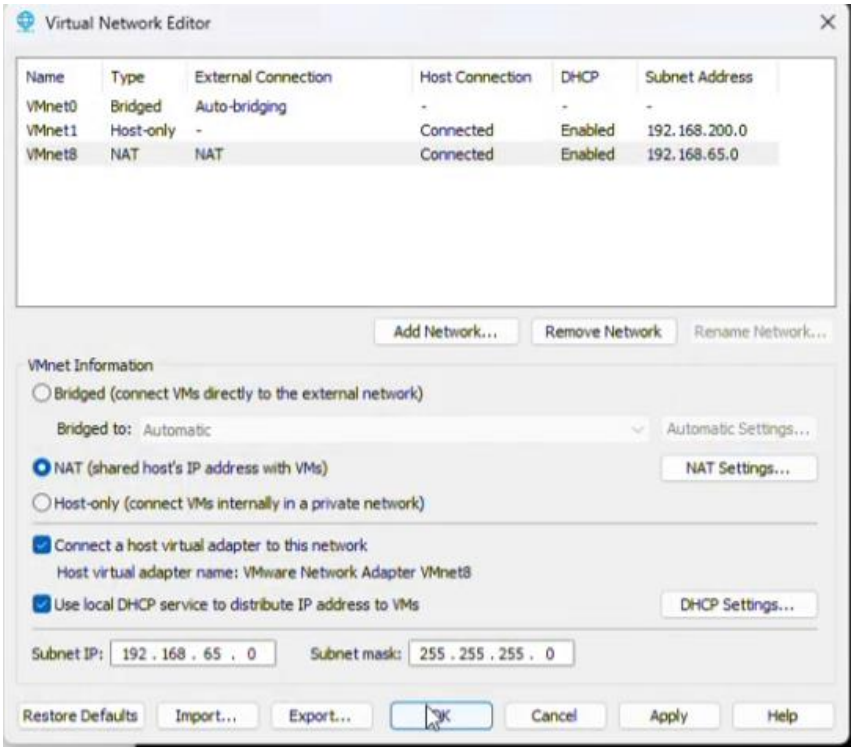
Dobór powyższych narzędzi pozwolił na kompleksową realizację fazy rekonesansu, szczegółową analizę wektorów komunikacji oraz weryfikację mechanizmów szyfrujących.

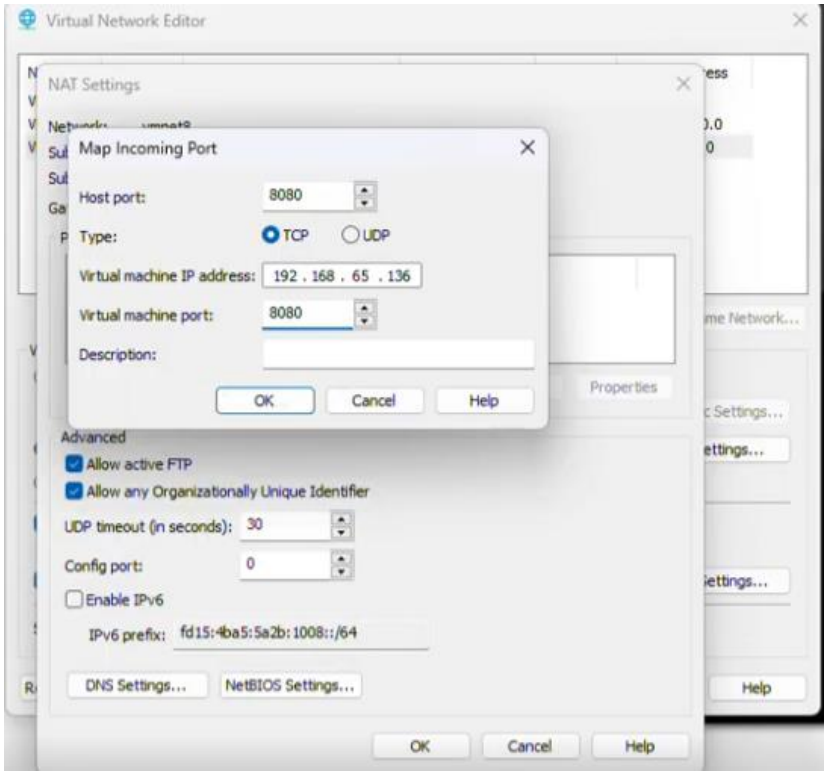
4.3. Konfiguracja środowiska wirtualnego VMware

Środowisko testowe zostało przygotowane z wykorzystaniem oprogramowania VMware Workstation. Maszyna wirtualna z systemem Linux została skonfigurowana w trybie sieciowym Bridged, co umożliwiło jej pracę w tej samej sieci lokalnej co inteligentne gniazdko TP-Link Tapo P100. Takie ustawienie pozwoliło na bezpośrednie przechwytywanie i analizę ruchu sieciowego generowanego przez badane urządzenie. Poniżej zamieszczone zostały zrzuty ekranu przedstawiające konfigurację:



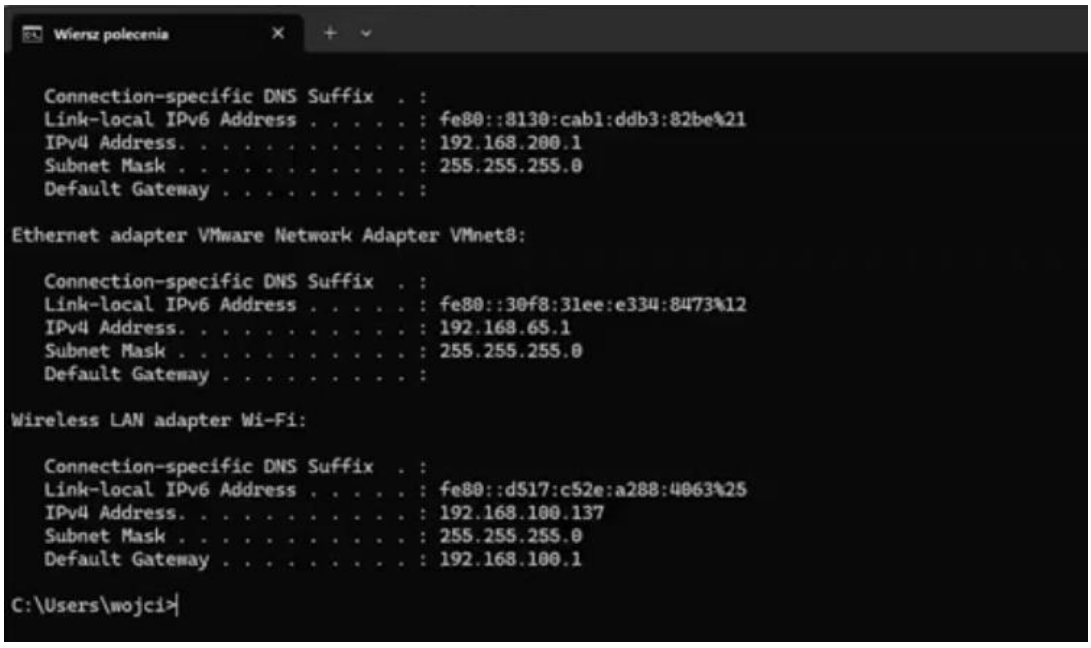

Debian 11.x 64-bit - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
Ubuntu server
Kali linux
Windows 10 x64
kali linuxx
kali
Clone of Windows 10 x6
Debian 11.x 64-bit
Home
Debian 11.x 64-bit
Debian 11.x 64-bit
Power on this virtual machine
Edit virtual machine settings
Devices
Memory 2 GB
Processors 2
Hard Disk (SCSI) 20 GB
CD/DVD (IDE) Using file C:\Use...
Network Adapter NAT
USB Controller Present
Sound Card Auto detect
Display Auto detect
Description
Type here to enter a description of this virtual machine.
Virtual Machine Details
State: Powered off
Configuration file: C:\Users\wojci\Documents\Virtu Machines\Debian 11.x 64-bit\Debian 11.x 64-bit.vmx
Hardware compatibility: Workstation 17.5 or later virtual machine
Primary IP address: Network information is not available

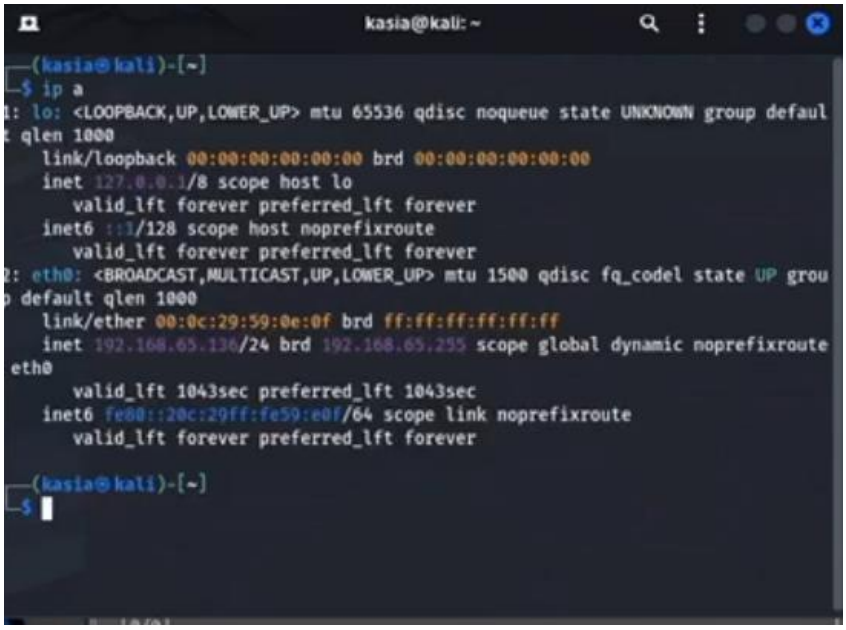

Virtual Network Editor
Name Type External Connection Host Connection DHCP Subnet Address
VMnet0 Bridged Auto-bridging - - -
VMnet1 Host-only - Connected Enabled 192.168.200.0
VMnet8 NAT NAT Connected Enabled 192.168.65.0
Add Network...
Remove Network
Rename Network...
VMnet Information
Bridged (connect VMs directly to the external network)
Bridged to: Automatic
Automatic Settings...
NAT (shared host's IP address with VMs)
NAT Settings...
Host-only (connect VMs internally in a private network)
Connect a host virtual adapter to this network
Host virtual adapter name: VMware Network Adapter VMnet8
Use local DHCP service to distribute IP address to VMs
DHCP Settings...
Subnet IP: 192 . 168 . 65 . 0
Subnet mask: 255 . 255 . 255 . 0
Restore Defaults
Import...
Export...
OK
Cancel
Apply
Help



5. Rekonesans sieciowy urządzenia

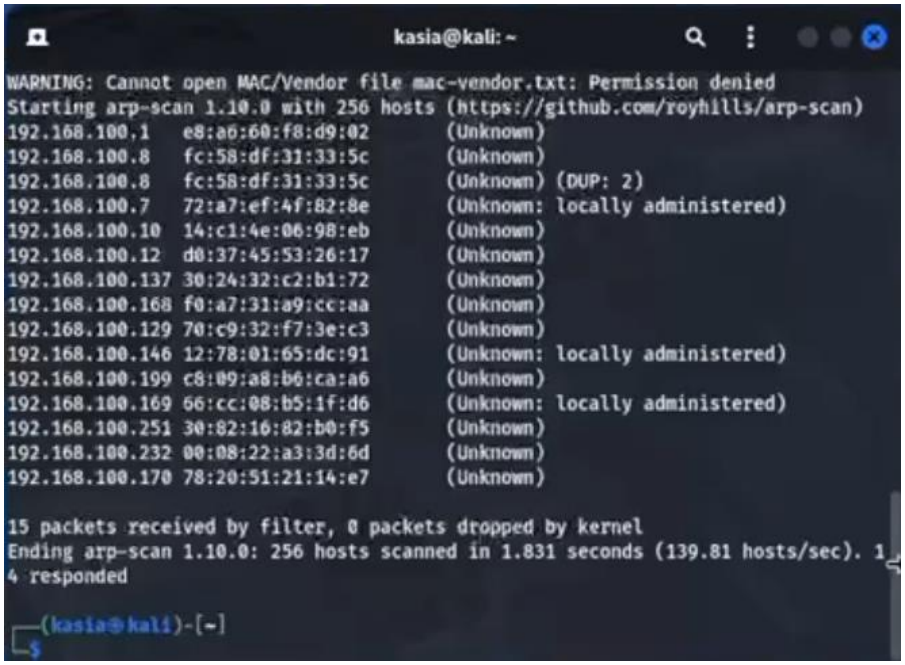
5.1. Identyfikacja hosta i gościa w sieci





5.2. Skanowanie portów i identyfikacja usług

Identyfikację hostów wykonano przy użyciu arp-scan



5.3. Wnioski z rekonesansu

Rekonesans potwierdził obecność urządzenia Tapo P100 w sieci oraz brak typowych interfejsów administracyjnych. Wyniki skanowania Nmap wykazały jedynie ograniczony zestaw portów wykorzystywanych do komunikacji urządzenia. Taka charakterystyka zmniejsza liczbę klasycznych wektorów ataku, ale nie eliminuje ryzyka podatności w usługach niestandardowych.

6. Analiza komunikacji sieciowej

6.1. Przechwytywanie ruchu sieciowego

Użyta komenda:

```
sudo tcpdump -i eth0 host 192.168.100.170 -w tapo_bridge.pcap
```

Polecenie tcpdump zostało wykorzystane do przechwytywania ruchu sieciowego generowanego przez inteligentne gniazdko TP-Link Tapo P100. Parametr -i eth0 wskazuje interfejs sieciowy maszyny wirtualnej, natomiast filtr host 192.168.100.170 ogranicza przechwytywanie wyłącznie do pakietów wysyłanych i odbieranych przez badane urządzenie. Zarejestrowany ruch zapisano do pliku tapo_bridge.pcap w celu dalszej analizy w narzędziu Wireshark. W celu jego otwarcia używamy następującej komendy:

```
wireshark tapo_bridge.pcap
```

Polecenie uruchamia narzędzie Wireshark i wczytuje zapisany wcześniej plik przechwyconego ruchu sieciowego. Pozwoliło to na szczegółową analizę pakietów, w tym identyfikację protokołów komunikacyjnych, takich jak TLS, oraz obserwację procesu zestawiania połączeń sieciowych.

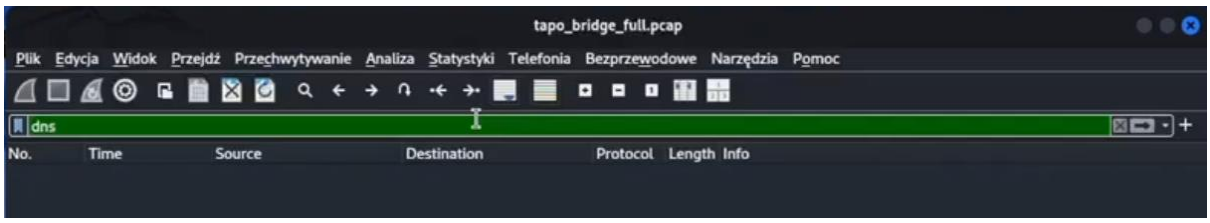
Aby wykonać pełne przechwytywanie ruchu przechodzącego przez interfejs sieciowy maszyny wirtualnej wpisujemy komendę:

```
sudo tcpdump -i eth0 -w tapo_bridge_full.pcap
```

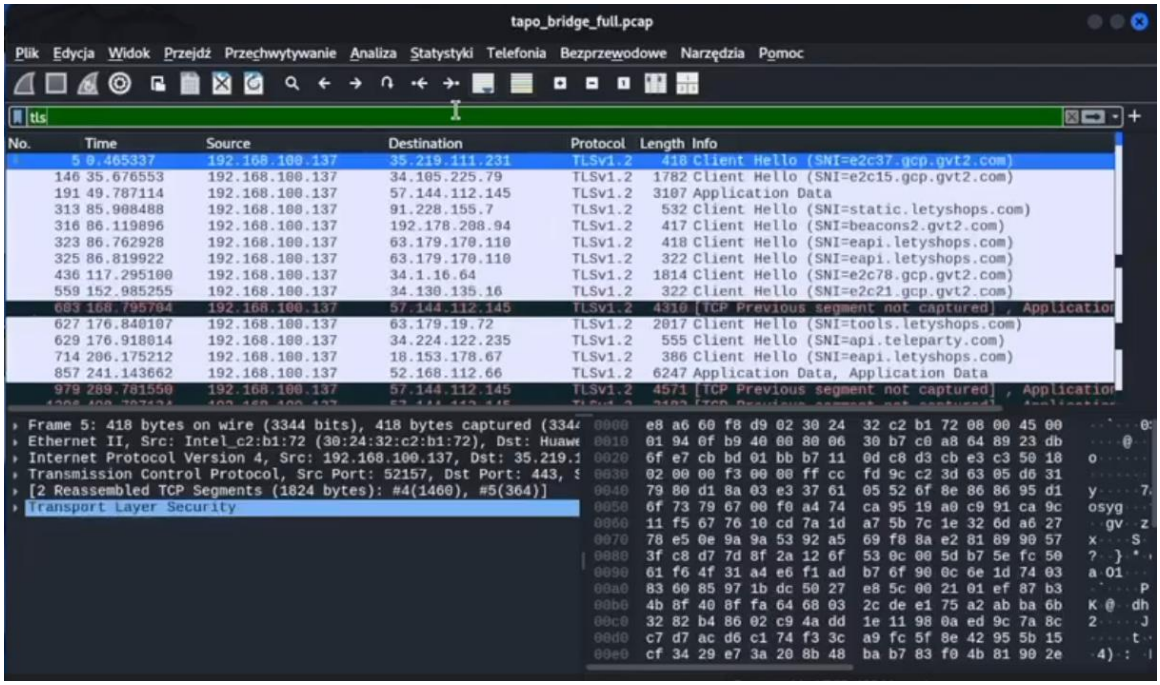
Plik tapo_bridge_full.pcap zawiera wszystkie pakiety zarejestrowane w sieci lokalnej, co umożliwiło późniejszą selekcję interesujących połączeń bez użycia filtrów podczas zapisu.

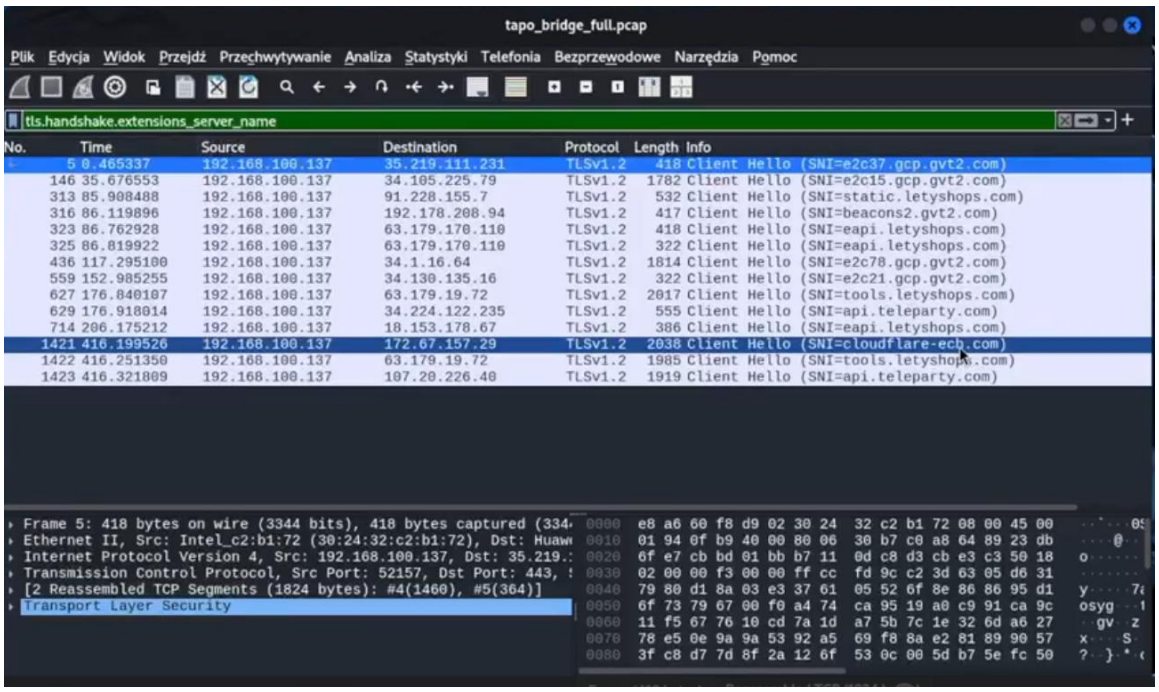
6.2. Analiza DNS

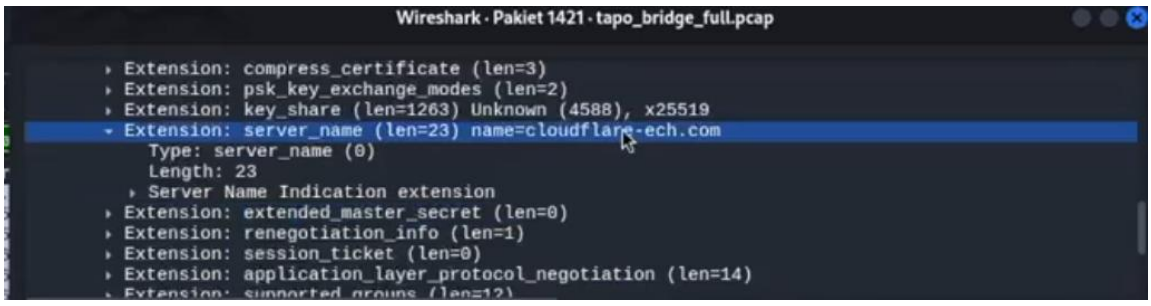
W przechwyconym ruchu urządzenia nie zaobserwowano pakietów DNS w postaci klasycznych zapytań UDP/TCP na port 53.

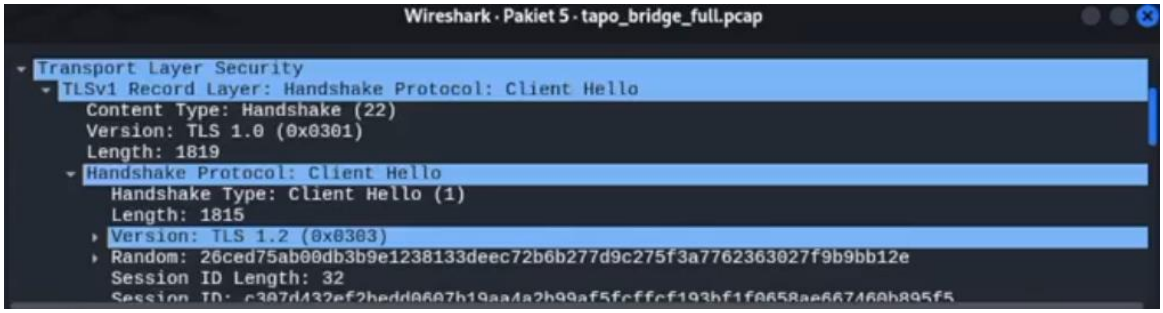


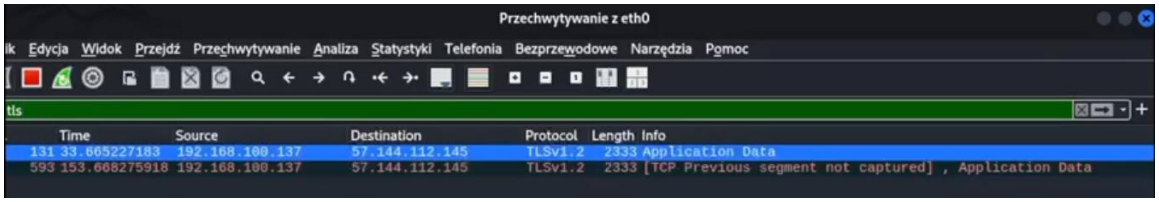
6.3. Analiza TLS i TLS handshake

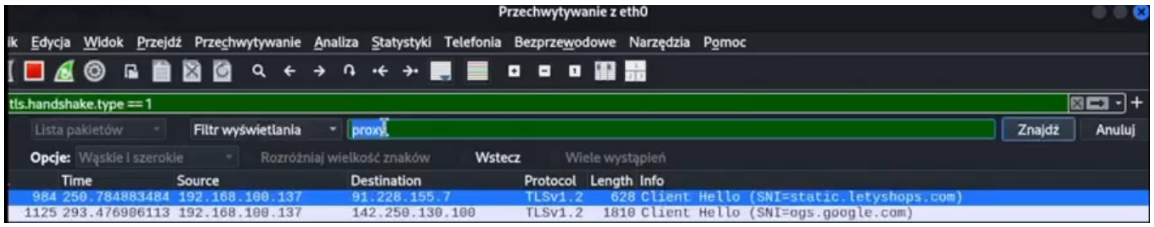

tapo_bridge_full.pcap
Plik Edycja Widok Przejdź Przechwytywanie Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
tls
No. Time Source Destination Protocol Length Info
5 0.465337 192.168.100.137 35.219.111.231 TLSv1.2 418 Client Hello (SNI=e2c37.gcp.gvt2.com)
146 35.676553 192.168.100.137 34.105.225.79 TLSv1.2 1782 Client Hello (SNI=e2c15.gcp.gvt2.com)
191 49.787114 192.168.100.137 57.144.112.145 TLSv1.2 3107 Application Data
313 85.908488 192.168.100.137 91.228.155.7 TLSv1.2 532 Client Hello (SNI=static.letyshops.com)
316 86.119896 192.168.100.137 192.178.208.94 TLSv1.2 417 Client Hello (SNI=beacons2.gvt2.com)
323 86.762928 192.168.100.137 63.179.170.110 TLSv1.2 418 Client Hello (SNI=eapi.letyshops.com)
325 86.819922 192.168.100.137 63.179.170.110 TLSv1.2 322 Client Hello (SNI=eapi.letyshops.com)
436 117.295100 192.168.100.137 34.1.16.64 TLSv1.2 1814 Client Hello (SNI=e2c78.gcp.gvt2.com)
559 152.985255 192.168.100.137 34.130.135.16 TLSv1.2 322 Client Hello (SNI=e2c21.gcp.gvt2.com)
603 168.795704 192.168.100.137 57.144.112.145 TLSv1.2 4310 [TCP Previous segment not captured] , Application
627 176.840107 192.168.100.137 63.179.19.72 TLSv1.2 2017 Client Hello (SNI=tools.letyshops.com)
629 176.918014 192.168.100.137 34.224.122.235 TLSv1.2 555 Client Hello (SNI=api.teleparty.com)
714 206.175212 192.168.100.137 18.153.178.67 TLSv1.2 386 Client Hello (SNI=eapi.letyshops.com)
857 241.143662 192.168.100.137 52.168.112.66 TLSv1.2 6247 Application Data, Application Data
979 289.781550 192.168.100.137 57.144.112.145 TLSv1.2 4571 [TCP Previous segment not captured] , Application
Frame 5: 418 bytes on wire (3344 bits), 418 bytes captured (3344
Ethernet II, Src: Intel_c2:b1:72 (30:24:32:c2:b1:72), Dst: Huawe
Internet Protocol Version 4, Src: 192.168.100.137, Dst: 35.219.1
Transmission Control Protocol, Src Port: 52157, Dst Port: 443, S
[2 Reassembled TCP Segments (1824 bytes): #4(1460), #5(364)]
Transport Layer Security
0000 e8 a6 60 f8 d9 02 30 24 32 c2 b1 72 08 00 45 00
0010 01 94 0f b9 40 00 80 06 30 b7 c0 a8 64 89 23 db
0020 6f e7 cb bd 01 bb b7 11 0d c8 d3 cb e3 c3 50 18
0030 02 00 00 f3 00 00 ff cc fd 9c c2 3d 63 05 d6 31
0040 79 80 d1 8a 03 e3 37 61 05 52 6f 8e 86 86 95 d1
0050 6f 73 79 67 00 f0 a4 74 ca 95 19 a0 c9 91 ca 9c
0060 11 f5 67 76 10 cd 7a 1d a7 5b 7c 1e 32 6d a6 27
0070 78 e5 0e 9a 9a 53 92 a5 69 f8 8a e2 81 89 90 57
0080 3f c8 d7 7d 8f 2a 12 6f 53 0c 00 5d b7 5e fc 50
0090 61 f6 4f 31 a4 e6 f1 ad b7 6f 90 0c 6e 1d 74 03
00a0 83 60 85 97 1b dc 50 27 e8 5c 00 21 01 ef 87 b3
00b0 4b 8f 40 8f fa 64 68 03 2c de e1 75 a2 ab ba 6b
00c0 32 82 b4 86 02 c9 4a dd 1e 11 98 0a ed 9c 7a 8c
00d0 c7 d7 ac d6 c1 74 f3 3c a9 fc 5f 8e 42 95 5b 15
00e0 cf 34 29 e7 3a 20 8b 48 ba b7 83 f0 4b 81 90 2e


tapo_bridge_full.pcap
Plik Edycja Widok Przejdź Przechwytywanie Analiza Statystyki Telefonia Bezprzewodowe Narzędzia Pomoc
tls.handshake.extensions_server_name
No. Time Source Destination Protocol Length Info
5 0.465337 192.168.100.137 35.219.111.231 TLSv1.2 418 Client Hello (SNI=e2c37.gcp.gvt2.com)
146 35.676553 192.168.100.137 34.105.225.79 TLSv1.2 1782 Client Hello (SNI=e2c15.gcp.gvt2.com)
313 85.908488 192.168.100.137 91.228.155.7 TLSv1.2 532 Client Hello (SNI=static.letyshops.com)
316 86.119896 192.168.100.137 192.178.208.94 TLSv1.2 417 Client Hello (SNI=beacons2.gvt2.com)
323 86.762928 192.168.100.137 63.179.170.110 TLSv1.2 418 Client Hello (SNI=eapi.letyshops.com)
325 86.819922 192.168.100.137 63.179.170.110 TLSv1.2 322 Client Hello (SNI=eapi.letyshops.com)
436 117.295100 192.168.100.137 34.1.16.64 TLSv1.2 1814 Client Hello (SNI=e2c78.gcp.gvt2.com)
559 152.985255 192.168.100.137 34.130.135.16 TLSv1.2 322 Client Hello (SNI=e2c21.gcp.gvt2.com)
627 176.840107 192.168.100.137 63.179.19.72 TLSv1.2 2017 Client Hello (SNI=tools.letyshops.com)
629 176.918014 192.168.100.137 34.224.122.235 TLSv1.2 555 Client Hello (SNI=api.teleparty.com)
714 206.175212 192.168.100.137 18.153.178.67 TLSv1.2 386 Client Hello (SNI=eapi.letyshops.com)
1421 416.199526 192.168.100.137 172.67.157.29 TLSv1.2 2038 Client Hello (SNI=cloudflare-ech.com)
1422 416.251350 192.168.100.137 63.179.19.72 TLSv1.2 1985 Client Hello (SNI=tools.letyshops.com)
1423 416.321809 192.168.100.137 107.20.226.40 TLSv1.2 1919 Client Hello (SNI=api.teleparty.com)
Frame 5: 418 bytes on wire (3344 bits), 418 bytes captured (3344
Ethernet II, Src: Intel_c2:b1:72 (30:24:32:c2:b1:72), Dst: Huawe
Internet Protocol Version 4, Src: 192.168.100.137, Dst: 35.219.1
Transmission Control Protocol, Src Port: 52157, Dst Port: 443, S
[2 Reassembled TCP Segments (1824 bytes): #4(1460), #5(364)]
Transport Layer Security
0000 e8 a6 60 f8 d9 02 30 24 32 c2 b1 72 08 00 45 00
0010 01 94 0f b9 40 00 80 06 30 b7 c0 a8 64 89 23 db
0020 6f e7 cb bd 01 bb b7 11 0d c8 d3 cb e3 c3 50 18
0030 02 00 00 f3 00 00 ff cc fd 9c c2 3d 63 05 d6 31
0040 79 80 d1 8a 03 e3 37 61 05 52 6f 8e 86 86 95 d1
0050 6f 73 79 67 00 f0 a4 74 ca 95 19 a0 c9 91 ca 9c
0060 11 f5 67 76 10 cd 7a 1d a7 5b 7c 1e 32 6d a6 27
0070 78 e5 0e 9a 9a 53 92 a5 69 f8 8a e2 81 89 90 57
0080 3f c8 d7 7d 8f 2a 12 6f 53 0c 00 5d b7 5e fc 50


Wireshark · Pakiet 1421 · tapo_bridge_full.pcap
Extension: compress_certificate (len=3)
Extension: psk_key_exchange_modes (len=2)
Extension: key_share (len=1263) Unknown (4588), x25519
Extension: server_name (len=23) name=cloudflare-ech.com
Type: server_name (0)
Length: 23
Server Name Indication extension
Extension: extended_master_secret (len=0)
Extension: renegotiation_info (len=1)
Extension: session_ticket (len=0)
Extension: application_layer_protocol_negotiation (len=14)







Analiza pakietów TLS Handshake wykazała, że inteligentne gniazdko TP-Link Tapo P100 wykorzystuje szyfrowaną komunikację z użyciem protokołu TLS w wersji 1.2. W trakcie fazy Client Hello możliwe było zidentyfikowanie domen docelowych poprzez pole Server Name Indication (SNI), jednak właściwa treść komunikacji pozostaje zaszyfrowana. Zaobserwowano wykorzystanie infrastruktury CDN, co wskazuje na chmurowy model działania urządzenia i utrudnia jednoznaczną identyfikację serwerów backendowych producenta.

6.4. Próba MITM

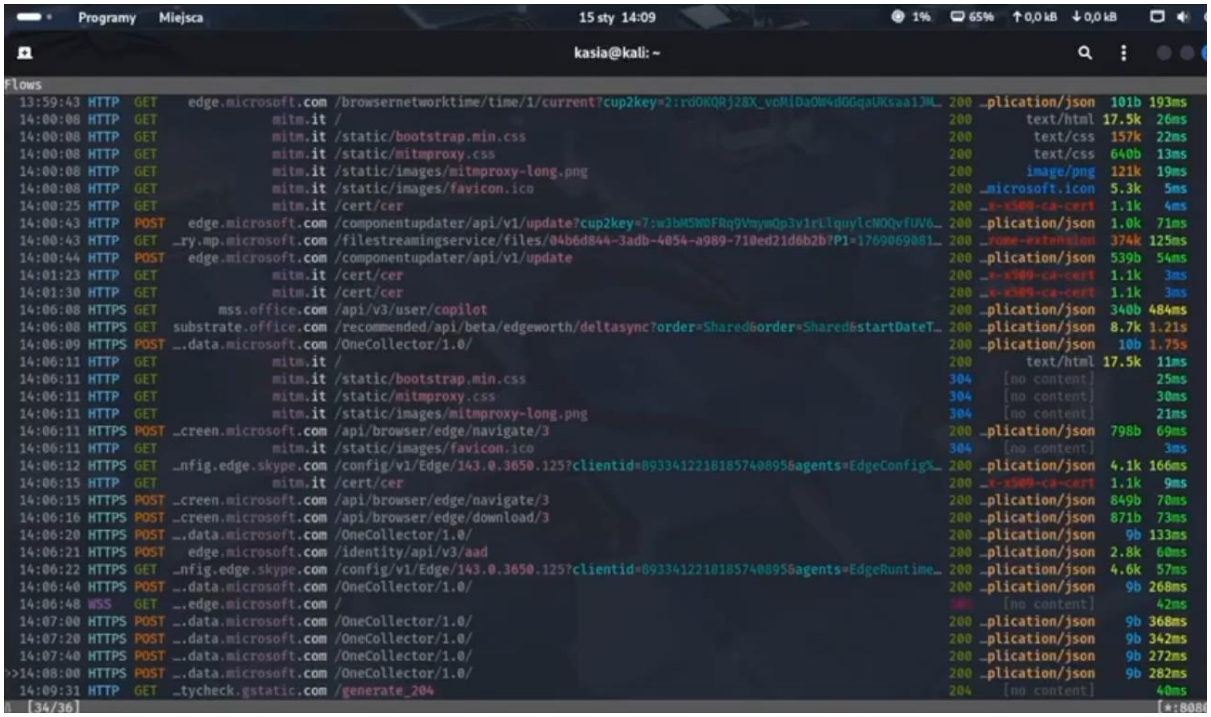
Na smartfonie ustawiono ręcznie serwer proxy Wi-Fi wskazujący na adres IP maszyny Kali oraz port 8080.

Uruchomiono mitmproxy w trybie nasłuchu przy używamy komendy:

mitmproxy –listen-host 0.0.0.0 --listen-port 8080

Podjęto próbę wykonania operacji włączania i wyłączania gniazdka w aplikacji Tapo.

Zaobserwowano następujące połączenia:



6.5. Podsumowanie analizy komunikacji

Analiza komunikacji sieciowej inteligentnego gniazdka TP-Link Tapo P100 została przeprowadzona z wykorzystaniem narzędzi tcpdump oraz Wireshark w środowisku wirtualnym działającym w trybie mostkowanym. Takie podejście umożliwiło skuteczne przechwycenie ruchu sieciowego generowanego przez urządzenie w sieci lokalnej oraz jego dalszą analizę w postaci plików PCAP.

W przechwyconych danych nie zaobserwowano transmisji informacji w postaci jawnej. Analiza ruchu nie wykazała obecności klasycznych zapytań DNS, co może wskazywać na wykorzystanie mechanizmów szyfrowanego rozwiązywania nazw lub wcześniejsze zestawienie połączeń przez aplikację mobilną. Dominującym protokołem komunikacyjnym był TLS w wersji 1.2,

wykorzystywany do zestawiania bezpiecznych połączeń z serwerami zewnętrznymi.

W trakcie analizy fazy TLS Handshake możliwe było zidentyfikowanie pakietów typu Client Hello, zawierających pole Server Name Indication (SNI). Pozwoliło to na częściową identyfikację domen docelowych, mimo że właściwa treść komunikacji pozostawała zaszyfrowana. Zaobserwowane adresy IP oraz nazwy domen wskazują na wykorzystanie infrastruktury CDN, co potwierdza chmurowy model działania urządzenia.

Na podstawie przeprowadzonej analizy można stwierdzić, że komunikacja sieciowa badanego urządzenia realizowana jest w sposób bezpieczny, z zastosowaniem aktualnych mechanizmów kryptograficznych. Jednocześnie zastosowane zabezpieczenia skutecznie ograniczają możliwość podsłuchu i analizy warstwy aplikacyjnej, umożliwiając jedynie obserwację metadanych połączeń sieciowych.

7. Analiza firmware i podatności

7.1. Identyfikacja wersji firmware i komponentów

Identyfikacja wersji firmware badanego urządzenia została przeprowadzona na podstawie informacji dostępnych w aplikacji mobilnej Tapo oraz obserwacji komunikacji sieciowej. Producent nie udostępnia publicznie obrazu firmware ani szczegółowej dokumentacji technicznej dotyczącej wewnętrznych komponentów oprogramowania, co jest typowe dla konsumenckich urządzeń Internetu Rzeczy.

Firmware urządzenia jest aktualizowany zdalnie za pośrednictwem infrastruktury chmurowej producenta. Użytkownik nie posiada możliwości ręcznej instalacji ani analizy binarnej oprogramowania. Z tego względu analiza firmware została ograniczona do identyfikacji wersji, sposobu aktualizacji oraz obserwacji zachowania urządzenia w sieci, bez ingerencji w jego oprogramowanie wewnętrzne.

7.2. Przegląd znanych podatności (CVE) dla Tapo / TP-Link

Opis podatności	Potencjalny wpływ	Rekomendacja
Podatności CVE wykryte w innych urządzeniach TP-Link (głównie routery i kamery IP), związane z błędami w interfejsach zarządzania oraz nieprawidłową walidacją danych wejściowych.	Możliwość nieautoryzowanego dostępu do urządzenia, przejęcia kontroli nad funkcjami lub naruszenia poufności danych w przypadku wystąpienia analogicznych podatności.	Regularna aktualizacja firmware urządzenia oraz stosowanie najnowszych wersji oprogramowania udostępnianych przez producenta.
Brak publicznie udokumentowanych podatności CVE bezpośrednio dla modelu Tapo P100 w analizowanej wersji firmware.	Trudność w jednoznacznej ocenie poziomu ryzyka; potencjalne zagrożenia mogą nie być jeszcze publicznie opisane.	Monitorowanie komunikatów bezpieczeństwa producenta oraz baz podatności (CVE, NVD).
Zamknięty charakter firmware i brak publicznej dokumentacji technicznej.	Ograniczona możliwość niezależnej analizy bezpieczeństwa oraz wykrywania potencjalnych podatności przez użytkowników.	Stosowanie dobrych praktyk bezpieczeństwa w sieci lokalnej (segmentacja IoT, firewall).
Zależność urządzenia od infrastruktury chmurowej producenta.	Potencjalne ryzyko w przypadku podatności po stronie usług chmurowych lub kompromitacji konta użytkownika.	Stosowanie silnych haseł, uwierzytelniania wieloskładnikowego (jeśli dostępne) oraz zabezpieczenie konta użytkownika.

7.3. Ocena wpływu podatności na badane urządzenie

Potencjalny wpływ znanych podatności związanych z ekosystemem TP-Link na badane urządzenie należy ocenić jako umiarkowany. Zastosowanie szyfrowanej komunikacji TLS oraz mechanizmów zabezpieczających, takich jak certificate pinning, znacząco utrudnia przeprowadzenie ataków polegających na podsłuchu lub modyfikacji ruchu sieciowego.

Jednocześnie zamknięty charakter firmware oraz silna zależność od infrastruktury chmurowej producenta powodują, że użytkownik ma ograniczoną możliwość niezależnej weryfikacji bezpieczeństwa oprogramowania. W przypadku wystąpienia podatności w firmware lub usługach chmurowych potencjalne skutki mogą obejmować nieautoryzowane sterowanie urządzeniem lub naruszenie prywatności użytkownika.

Z tego względu kluczowe znaczenie dla ograniczenia ryzyka mają regularne aktualizacje oprogramowania, stosowanie dobrych praktyk konfiguracyjnych oraz odpowiednie zabezpieczenie sieci lokalnej, w której urządzenie jest eksploatowane.

8. Ocena ryzyka

8.1. Potencjalne scenariusze ataku

Na podstawie przeprowadzonej analizy oraz charakterystyki badanego urządzenia IoT można wyróżnić kilka potencjalnych scenariuszy ataku. Jednym z nich jest uzyskanie nieautoryzowanego dostępu do urządzenia z poziomu sieci lokalnej, szczególnie w przypadku braku segmentacji sieci i umieszczenia urządzeń IoT w tej samej podsieci co komputery użytkownika. W takim scenariuszu atakujący, który uzyska dostęp do sieci LAN, może próbować wykorzystać błędy konfiguracyjne lub podatności w oprogramowaniu urządzenia.

Kolejnym scenariuszem jest kompromitacja konta użytkownika w usłudze chmurowej producenta, np. w wyniku użycia słabego hasła lub wycieku danych uwierzytelniających. Ze względu na zależność urządzenia od infrastruktury chmurowej, przejęcie konta może umożliwić zdalne sterowanie gniazdkiem bez dostępu do sieci lokalnej. Potencjalnym zagrożeniem jest również

wykorzystanie podatności w oprogramowaniu urządzenia lub aplikacji mobilnej, opisanych w publicznych bazach CVE.

8.2. Skutki dla użytkownika i sieci lokalnej

Skutki skutecznego ataku na urządzenie IoT mogą obejmować zarówno konsekwencje dla pojedynczego użytkownika, jak i całej sieci lokalnej. W przypadku inteligentnego gniazdka możliwe jest nieautoryzowane sterowanie zasilaniem podłączonych urządzeń, co może prowadzić do strat materialnych lub zakłóceń w pracy systemów domowych.

Z punktu widzenia sieci lokalnej urządzenie IoT może stać się punktem wejścia do dalszych ataków, umożliwiając rozpoznanie infrastruktury sieciowej lub eskalację dostępu do innych hostów. Dodatkowo zależność od infrastruktury chmurowej wiąże się z ryzykiem naruszenia prywatności użytkownika, wynikającym z przetwarzania danych przez podmioty zewnętrzne.

9. Rekomendacje i hardening

9.1. Zalecenia konfiguracyjne (konto, aplikacja, sieć)

W celu ograniczenia ryzyka związanego z eksploatacją badanego urządzenia zaleca się stosowanie silnych, unikalnych haseł do konta użytkownika w aplikacji Tapo oraz, jeśli to możliwe, włączenie dodatkowych mechanizmów uwierzytelniania. Aplikacja mobilna oraz firmware urządzenia powinny być regularnie aktualizowane do najnowszych wersji udostępnianych przez producenta.

Zaleca się również ograniczenie uprawnień aplikacji mobilnej do niezbędnego minimum oraz korzystanie wyłącznie z oficjalnych źródeł dystrybucji oprogramowania.

9.2. Zalecenia dla sieci domowej (segmentacja IoT, firewall, UPnP)

Istotnym elementem zwiększania bezpieczeństwa jest odpowiednia konfiguracja sieci domowej. Urządzenia IoT powinny być umieszczane w wydzielonej sieci lub podsieci (np. VLAN), oddzielonej od głównej sieci użytkownika. Takie rozwiązanie ogranicza możliwość rozprzestrzeniania się ataku w przypadku kompromitacji urządzenia.

Dodatkowo zaleca się stosowanie reguł zapory sieciowej (firewall), które ograniczają komunikację urządzeń IoT wyłącznie do niezbędnych adresów i portów, oraz wyłączenie mechanizmów takich jak UPnP, które mogą niepotrzebnie zwiększać powierzchnię ataku.

9.3. Dobre praktyki eksploatacyjne (aktualizacje, monitoring)

Do dobrych praktyk eksploatacyjnych należy regularne sprawdzanie dostępności aktualizacji bezpieczeństwa oraz monitorowanie urządzeń podłączonych do sieci lokalnej. Użytkownik powinien okresowo weryfikować listę aktywnych urządzeń oraz reagować na nieznane lub podejrzane połączenia.

Świadome zarządzanie urządzeniami IoT, stosowanie podstawowych zasad higieny cyberbezpieczeństwa oraz odpowiednia konfiguracja sieci znacząco zmniejszają ryzyko wystąpienia incydentów bezpieczeństwa związanych z ich użytkowaniem.

10. Wnioski końcowe

Przeprowadzona analiza bezpieczeństwa inteligentnego gniazdka TP-Link Tapo P100 pozwoliła na ocenę wybranych aspektów związanych z eksploatacją konsumenckiego urządzenia Internetu Rzeczy w sieci lokalnej. Badania wykonane w środowisku laboratoryjnym potwierdziły, że producent zastosował podstawowe mechanizmy ochrony komunikacji, w szczególności szyfrowanie transmisji z wykorzystaniem protokołu TLS oraz mechanizmy utrudniające przeprowadzenie ataków typu Man-in-the-Middle, takie jak certificate pinning.

Jednocześnie analiza wykazała, że bezpieczeństwo urządzenia IoT w dużej mierze zależy nie tylko od rozwiązań zastosowanych przez producenta, lecz również od sposobu konfiguracji sieci domowej oraz praktyk stosowanych przez użytkownika. Zależność urządzenia od infrastruktury chmurowej oraz brak bezpośredniego interfejsu lokalnego powodują, że kompromitacja konta użytkownika lub błędy w konfiguracji sieci mogą prowadzić do istotnych zagrożeń dla prywatności oraz bezpieczeństwa sieci lokalnej.

Na podstawie uzyskanych wyników można stwierdzić, że badane urządzenie spełnia podstawowe wymagania bezpieczeństwa dla urządzeń klasy konsumenckiej, jednak jego bezpieczne użytkowanie wymaga stosowania dodatkowych środków ochrony, takich jak segmentacja sieci IoT, odpowiednia

konfiguracja zapory sieciowej oraz regularne aktualizacje oprogramowania. Przeprowadzona analiza potwierdza zasadność traktowania urządzeń IoT jako potencjalnych punktów ryzyka w sieci oraz konieczność świadomego podejścia do ich wdrażania i eksploatacji.