19,10.2018 Michał Osman 236627

Zadanie wykonano dnia 19,10.2018 w pociągu na trasie Wrocław – Kielce.

Na początku w pociągu z Wrocławia do Katowic po ustawieniu karty sieciowej w tryb monitor sprawdzono za pomocą programu Wireshark, z jakimi ssid chcą się połączyć urządzenia na dworcu głównym. Pośród powtarzających się nazw były między innymi Pizzeria Planka, dreadwerkz, MiejskiInternet oraz PWR-WiFi. Następnie ustawiono kartę sieciową ponownie w normalny tryb pracy, ale aktywowano tryb promisc za pomocą programu airodump-ng oraz rozpoczęto udostępnianie otwartej sieci WIFI o nazwie Pizzeria Planka, kiedy pociąg ruszył oraz monitorowanie ruchu w sieci za pomocą laptopa Jednak takie ssid sieci nie okazało się wystarczająco zachęcające i kiedy po dłuższym czasie żadne nowe urządzenie się z nią nie połączyło, postanowiono zmienić nazwę sieci. Wybrano ssid PKP WiFi, ponieważ w pociągu nie było żadnej sieci bezprzewodowej udostępnianej przez przewoźnika (PKP intercity).

Po chwili połączyło się pierwsze urządzenie, telefon marki Huawei i przechwycono wiadomości ARP przeznie transmitowane. Następnie udało się przechwycić MDNS z zapytaniem _spotify-connetc._tcp. Oprócz tego urządzenie wysłało pakied UDP (no 1329). Do sieci podłaczyło się jeszcze jedno urządzenie, ale jedyne co udało się przechwycić, to pakiet ARP (no 772). Za pomocą programu tcpdump udało się również przechwycic kilka pakietów MDNS wysłanych z pierwszego urządzenia, jednak ciężko rozczytać, czego dokładnie one dotyczyły.

Kolejny test przeprowadzono w galerii katowickiej tego samego dnia w okolicach godziny 19:00. Pośród poszukiwanych ssid sieci przechwyconych w trybie monitor za pomocą programu wireshark, było bardzo dużo zapytań o sieć „katowicka”, ponieważ tak nazywała się otwarta sieć dostępna w tym miejscu. Zatem wybrano taką nazwę jako nowe ssid udostępnianej sieci. Po chwili z siecią połączyło się bardzo dużo telefonów komórkowych, które rozsyłały zapytania ARP. Niestety zanim zaczęły one wysyłać jakieś ciekawsze pakiety, nasłuchiwanie musiało zostać przerwane z powodu braku czasu.

Trzecim miejscem, w którym przeprowadzono nasłuchiwanie, był pociąg regio z Katowic do Kielc. Po ustawieniu karty sieciowej w tryb monitor można było zaobserwować bardzo dużą ilość przesyłanych pakietów. Poza poszukiwanymi SSID udało się przechwycić całkiem sporą liczbę pakietów ARP, DHCP, DNS, GQUIC, HTTP, ICMP, MDNS, NBNS, SSDP oraz najwięcej TCP. Następnie rozpoczęto udostępnianie sieci o SSID takim samym, jak w poprzednim pociągu. Niestety nie przyniosło to zbyt dużych rezultatów, prawdopodobnie dlatego, że w pociągu znajdowały się inne sieci WiFi udostępniane przez przewoźnika, a które miały inaczej skonstruowane nazwy. Były to odpowiednio 36WEa-024-C oraz 36WEa-024-B, zatem zmieniono SSID sieci na 36WEa-024-A, aby bardziej je przyponinało. W efekcie do sieci podłączyło się parę telefonów komórkowych, jednak nie zaobserwowano jakiegoś wzmożonego ruchu w sieci, być może ze względu na słabą prędkością internetu, który nawet momentami zupełnie tracił zasięg.

Jeśli chodzi o poszukiwane strony, to z przechwyconych pakietów ciężko było jakieś wydobyć, ponieważ większość nich była przesyłana po szyfrowanym połączeniu oraz ze względu na relatywnie mały ruch w sieci. Większość urządzeń, jeśli nie wszystkie, które się połączyły z siecią, była smartfonami, a prędkość udostępnianego internetu była dość niska, stąd zapewne użytkownicy sieci korzystali również z własnego internetu, co tłumaczyłoby mały ruch w udostępnianej sieci.

1. SSID poszukiwanych sieci

1.1 Wrocław - Katowice

- Pizzeria Planka
- 4WSK_hotspot
- HP-Print-FD-Laser Jet Pro MFP
- AndroidAP
- Multikebab
- CITYFIT
- Mazurki
- pm
- Funbox-F390
- ALFAX.COM_K31
- UPCE2E6666
- Free LTE
- dreadwerkz
- MiejskiInternet
- TP-Link_DD34
- iPhone (Agnieszka)
- _PKP_WIFI
- Hotspot
- FreeCityInternet
- HotSpot-KD
- IMPULS
- AndroidAP5601
- UPC197382
- PKS_W_OLAWIE_16
- Livebox-7C9B
- PWR-WiFi
- FunBox3-8A90
- FunBox3-A2C2
- AANET 12
- Hilda_Lapac
- GoatsLand
- multimedia_internet
- Dziadek
- Pieczara
- clenik2009
- trolololo
- niemaopcji
- HUAWEI-DB12
- MORENA
- HotSpot IC
- NETIASPOT-913EC0
- UPC7602250
- UPC6335554
- CornerHostel_new

1.2 Katowice

- APK-LINK
- Bed092013
- katowicka
- Hexa_Katowice
- wifi_1
- eSW
- LAVARD 141
- NETGEAR_DR2

1.3 Katowice – Kielce

- 36WEa-024-C
- FON_NETIA_FREE_INTERNET
- Polsta
- UPC6613099
- PLAY INTERNET 4G LTE-D11A
- UPC5597BEB
- UPC2A17522
- Vodafone-46147042
- A4366F77
- 9DF6A65
- meskon

2. Nazwa sieci

Pizzeria Planka – 1 (ARP, telefon Huawei)

PKP_WiFi – 3, z czego 1 rzeczywiście aktywny
MDNS, UDP, ARP;
spotify_connect, google_cast_tcp_local

PKP_WIFI [Katowice – Kielce]
1 ARP

katowicka ~ 20 – same ARP
ARP, DHCP (transaction ID)

36WEa-024-A – 5 urządzeń
NBNS, ARP, DHCP

3. Mapa

Katowice – Kielce monitor:
22.22.190.35.bc.googleusercontent.com (35.190.22.22) – US, United States
orangepolska-21.gw.opentransit.net (193.251.250.14) – FR, France
waw02s05-in-f14.1e100.net (216.58.209.46) – US, United States
108.177.126.106 (108.177.126.106) – US, United States
a95-101-182-185.deploy.static.akamaitechnologies.com (95.101.182.185) – EU, Europe
frcch1-vip-bx-003.aaplimg.com (17.253.109.203) – US, United States
22.22.190.35.bc.googleusercontent.com (35.190.22.22) – US, United States
edge-mqtt-shv-01-waw1.facebook.com (31.13.81.5) – IE, Ireland
edge-video-shv-02-frt3.fbcdn.net (157.240.20.16) – US, United States
185.60.216.52 (185.60.216.52) – IE, Ireland