Raport

Autorzy: Piotr Klepczyk, Mateusz Laskowski

Zadania zostały wykonane na systemie operacyjnym Windows 10. Użyliśmy oto takich narzędzi:

* WireShark
* WiFi InfoView
* TraceRoute
* Funkcja Hot-spot

**Zadanie 1.**

1. Lista sieci SSID widziane przez urządzenie

|  |  |
| --- | --- |
| 41 6E 64 72 6F 69 64 | Android |
| 41 6E 64 72 6F 69 64 41 50 | AndroidAP |
| 64 75 64 75 73 40 6B | dudus@k |
| 65 64 75 72 6F 61 6D | eduroam |
| 48 55 41 57 45 49 20 50 38 | HUAWEI P8 |
| 52 65 64 6D 69 | Redmi |
| 44 32 31 2D 6B 6F 6E 66 65 72 65 6E 63 6A 61 | D21-konferencja |
| 54 65 6C 65 66 6F 6E 20 4D 49 | Telefon MI |

Za pomocą WiFi InfoView mogliśmy zobaczyć wszystkie dostępne routery WiFi, które takich sieci jak eduroam miało wiele routerów, a urządzenie (4 pozycja z tabeli) wyszukało tylko jedno, a dokładnie ten router, który miał najmocniejszą jakość połączenia.

Dzięki hot-spotowi, można znaleźć jakie jest urządzenie podłączone do sieci.

Załącznik: connect.png

1. Strony niezaszyfrowane można było odczytać dokładne URL, zaś szyfrowane albo samo IP lub również były zaszyfrowane. Załączniki w podpunkcie C).

Przykładowe wyniki:

<http://mikolaj.ovh/index.php>

<http://156.17.7.16/236618>

<http://device-control.ff.avast.com/v1/receiver>

1. Protokoły podczas przeglądania sieci:

* **UDP** – (User Datagram Protocol)  stosowany jest w warstwie transportowej modelu OSI. Nie gwarantuje dostarczenia datagramu. Jest to protokół bezpołączeniowy, więc nie ma narzutu na nawiązywanie połączenia i śledzenie sesji. Nie ma też mechanizmów kontroli przepływu i retransmisji.
* **TLSv1.3**
* **TLSv1.2**
* **TLS** – (Transport Layer Security) zapewnia poufność i integralność transmisji danych, a także uwierzytelnienie serwera, a niekiedy również klienta.
* **TCP** – (Transmission Control Protocol) połączeniowy, niezawodny, strumieniowy [protokół komunikacyjny](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_komunikacyjny) stosowany do przesyłania danych między [procesami](https://pl.wikipedia.org/wiki/Proces_(informatyka)) uruchomionymi na różnych maszynach, będący częścią szeroko wykorzystywanego obecnie [stosu TCP/IP](https://pl.wikipedia.org/wiki/Model_TCP/IP) (korzysta z usług protokołu [IP](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_internetowy) do wysyłania i odbierania danych oraz ich [fragmentacji](https://pl.wikipedia.org/wiki/Fragmentacja_IP) wtedy, gdy jest to konieczne).
* **SSLv2** - jest protokołem sieciowym używanym do bezpiecznych połączeń internetowych, przyjęto go jako standard szyfrowania na stronach WWW. Zapewnia poufność transmisji danych przesyłanych przez Internet.
* **SSDP** – (Simple Service Discovery Protocol) służy do wykrywania urządzeń UPnP\*. SSDP używa portu 1900.
* **HTTP** – (Hypertext Transfer Protocol) przesyła żądania udostępnienia dokumentów [WWW](https://pl.wikipedia.org/wiki/World_Wide_Web) i informacje o kliknięciu odnośnika oraz informacje z formularzy. Zadaniem stron [WWW](https://pl.wikipedia.org/wiki/World_Wide_Web) jest publikowanie informacji – natomiast [protokół](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_komunikacyjny) HTTP właśnie to umożliwia.
* **GQUIC**
* **DNS** – (Domain Name System) system [serwerów](https://pl.wikipedia.org/wiki/Serwer), [protokół komunikacyjny](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_komunikacyjny) oraz [usługa](https://pl.wikipedia.org/wiki/Us%C5%82uga_internetowa) obsługująca rozproszoną bazę danych adresów sieciowych. Pozwala na zamianę adresów znanych użytkownikom [Internetu](https://pl.wikipedia.org/wiki/Internet) na adresy zrozumiałe dla urządzeń tworzących [sieć komputerową](https://pl.wikipedia.org/wiki/Sie%C4%87_komputerowa).
* **ARP** – (Adress Resolution Protocol)  [protokół sieciowy](https://pl.wikipedia.org/wiki/Protok%C3%B3%C5%82_komunikacyjny) umożliwiający mapowanie logicznych adresów [warstwy sieciowej](https://pl.wikipedia.org/wiki/Model_OSI#Warstwa_sieciowa) (warstwa 3) na fizyczne adresy warstwy łącza danych (2). Protokół ten nie ogranicza się tylko do konwersji [adresów IP](https://pl.wikipedia.org/wiki/Adres_IP) na [adres MAC](https://pl.wikipedia.org/wiki/Adres_MAC) stosowany w sieciach [Ethernet](https://pl.wikipedia.org/wiki/Ethernet), lecz jest także wykorzystywany do odpytywania o adresy fizyczne
* **DHCPv6** – (Dynamic Host Configuration Protocol version 6) to protokół sieciowy do konfigurowania hostów protokołu IPv6 (IPv6) z adresami IP, prefiksami IP i innymi danymi konfiguracyjnymi wymaganymi do działania w sieci IPv6.

Można było zdobyć dane typu LOGIN i HASŁO, na niezaszyfrowanej stronie www, czyli z protokołem zabezpieczającym http, a nie https. Chciałbym zauważyć, że również program antywirusowy szyfruje dane. Oczywiście mogliśmy odczytać dokładne URL strony i zachodzące na niej eventy, przez co podsłuchaliśmy dane, które były wysyłane, a dokładniej hasło i login. Dane, które otrzymywaliśmy od https były zaszyfrowane.

Załączniki: anty.png, dane1.png, dane2.png, dane3.png, dane4.png dane5.png.

1. Z pomocą narzędzia zwanego TraceRoute uzyskaliśmy takie oto dane. Sprawdź załączniki: traceroute.png, traceroute.txt.