**SPRAWOZDANIE**

**Lista nr 3, zadanie 1**

Kajetan Korzycki (236799)

Jakub Gogola (236412)

**Przechwytywanie pakietów w nieszyfrowanych sieciach WiFi**

Zgodnie z poleceniem 3. listy, wykonywanej w ramach kursu Bezpieczeństwo komputerowe, należało zbadać przepływ pakietów w otwartej, nieszyfrowanej sieci bezprzewodowej. W celu realizacji zadania dokonaliśmy analizy ruchu sieciowego w Pasażu Grunwaldzkim oraz w Strefie Kultury Studenckiej.

Lista poszukiwanych SSID sieci znajduje się w pliku “ssids.txt”. Nie wszystkie SSID udało się poprawnie odczytać (niektóre pakiety odczytywane były jako zniekształcone i tylko część SSID ma sens). Oto wybrane z nich:

|  |  |  |  |
| --- | --- | --- | --- |
| Funk Lounge Hostel | %kominek\_123 | PWR-WiFi | IKEA WiFi |
| PWr-WiFi | PWr--WiFi | PWR--WiFi | HotSpot-G.Dominikanska |
| Hala\_Stulecia | tatarhotel | virtualRouterInstaller | Akademik - dol |
| Basia | Camp de Mar | wlan\_tramwaje | iPhone (Anna) |
| Caritas | orlegniazdo3 | SSID | mBank |

Liczbę podłączonych urządzeń na podstawie DNS określić można przy użyciu komendy: *tshark -r KFC\_hotspot.pcapng -T fields -e ip.dst -Y "dns.flags.response eq 0"*.

Do 3 testowanych sieci podłączonych było kolejno:

* w Pasażu Grunwaldzkim:
  + KFC\_Hotspot: 6 urządzeń
  + “\*\*Free wifi Pasaz Grunwaldzki\*\*”: 22 urządzenia
* “eduroam” SKS: 4

Przechwycone adresu URL znajdują się w pliku urls.txt.

Dokonano również analizy protokołów, które zostały wykorzystane przez urządzenia do przesyłania bądź pobierania danych. Ich lista znajduje się w pliku proto.csv. Da się zauważyć największy udział procentowy pakietów Logical-Link Control oraz Transmission Control Protocol.

Analizując przechwycone w sieci pakiety udało się ustalić lokalizacje serwerów, do których wysłały zapytania obecne w sieci urządzenia. Oto kilka przykładowych wizualizacji wykonanych za pomocą narzędzi dostępnego na stronie <https://geotraceroute.com/>.





