Politechnika Warszawska

Wydział Fizyki

Kryptografia i bezpieczeństwo informacji dla fizyków

Sprawozdanie z zadania nr. 8 na temat:

**Pasywna identyfikacja systemów operacyjnych na podstawie własności pakietów sieciowych**

**Wykonali:**

Maciej Czarnecki

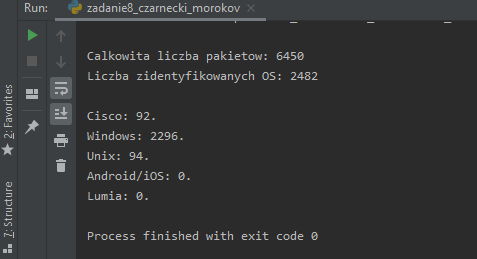
Denys Morokov

Fizyka techniczna II stopień, 2 rok

1. **Wstęp**
   1. **Cel:** celem zadania jest zidentyfikowanie systemu operacyjnego w obserwowanym ruchu sieciowym na podstawie dowolnych parametrów pakietu lub zawartości i znaleźć i uruchomić program wyszukujący i identyfikujący OS hostów w sieci lokalnej.
   2. **Wykorzystana technologia:** skrypt został zaimplementowany w Python wykorzystujący bibliotekę Scapy.Analizator ruchu sieciowego Wireshark. Pasywny skaner sieciowy p0f.
2. **Opracowanie wyników**

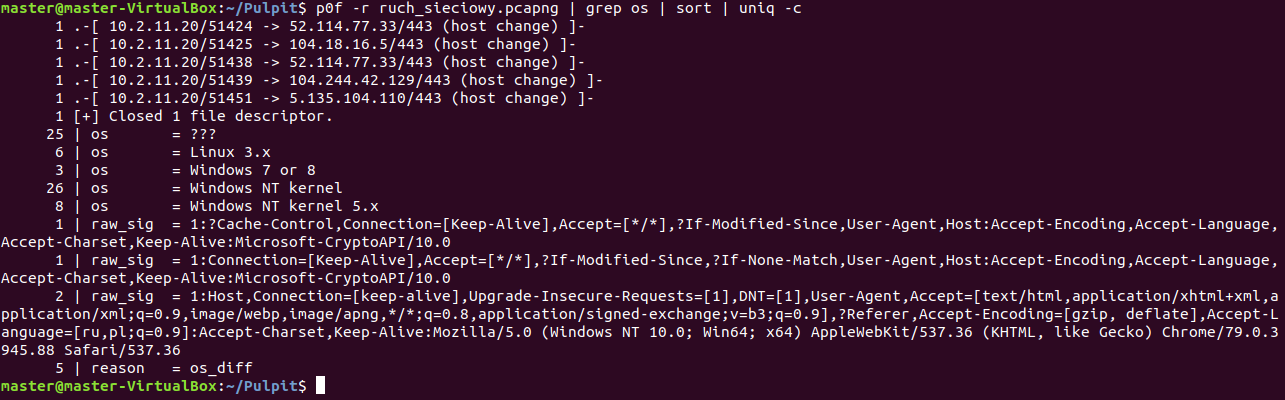
W celu stworzenia pliku, który będzie zawierał ruch sieciowy użyto Wireshark, który w ciągu 5-7 minut zapisywał ruch sieciowy, następnie uzyskane dane zapisano do pliku *ruch\_sieciowy.pcapng*. W celu zidentyfikowania systemu operacyjnego w obserwowanym ruchu zastosowani dwie metody:

**1.** Napisano skrypt w Pythonie, który na podstawie parametru TTL (Time To Life) określano system operacyjny urządzenia, z którego dany pakiet został wysłany. Wynik dla wygenerowanego pliku wyżej przedstawia rysunek 1.



Rys. 1. Wynik identyfikacji OS

**2.** Użyto pasywny skaner sieciowy p0f.



Rys. 2. Wynik identyfikacji OS przy użyciu p0f

1. **Podsumowanie**

Dla uzyskanego ruchu sieciowego zidentyfikowano systemy operacyjne na dwa sposoby: poprzez napisanie własnego skryptu w Python i przez użycie programu p0f.