Bezpieczeństwo komputerowe
Laboratorium, Lista 2

Wojciech Strzelecki, Adam Niezgoda

2021-11-07

1 Wstęp

Przeprowadzone przez nas eksperymenty zostały przeprowadzone w warunkach domowych. Do zbierania przedstawionych statystyk korzystaliśmy z programów: Tshark, Wireshark, Python.

2 Rozwiązanie i wyniki

2.1 Lista SSID

Do rozwiązania zadania posłużyliśmy się programem Tshark oraz airmon-ng, poprzez wpisanie następującej komendy:

```
tshark -i wlp0s20f3mon -Y 'wlan.fc.type_subtype eq 4' -T fields -e wlan.ssid
```

W graficznej wersji programu należy użyć filtru: wlan.exctcap.b48.

SSID	Liczba wyszukiwań
∅	53
NETWORK	5
Internet Domowy-266EED	7
V9S7D9HFGE6M	2

Pierwszy rząd z pustą nazwą to tzw. "SSID Wildcart" pozwalający na dopasowanie dowolnej nazwy sieci. Do obserwowania tego ruchu sieciowego, przełączyliśmy kartę sieciową w tryb monitorowania, używając następujących komend:

```
sudo ifconfig wlp0s20f3 down
sudo iwconfig wlp0s20f3 mode monitor
sudo ifconfig wlp0s20f3 up
sudo airmon-ng start wlp0s20f3
sudo airmon-ng stop wlp0s20f3
sudo ifconfig wlp0s20f3 up
service network-manager restart
```

2.2 Sieć

Nazwa udostępnianej przez nas sieci: wojtek-dell.
Podłączone urządzenia (adresy MAC):

- 16:93:84:f8:91:d1 - telefon Wojtka
- 3c:f7:a4:f6:64:d9 - telefon Adama
- 64:5d:86:e8:13:14 - komputer udostępniający sieć

2.3 Odwiedzane strony

Odwiedzone strony ustaliliśmy na podstawie zapytań DNS. Użyliśmy poniższej komendy:

```
sudo tshark -i wlp0s20f3 -Y dns -T fields -e dns.qry.name >
/home/wojtek/Desktop/sites_tshark
```

Domena	Liczba wystąpień
www.google.com	26
play.googleapis.com	4
teams.microsoft.com	28
zagorski.im.pwr.wroc.pl	3
cs.pwr.edu.pl	2
edukacja.pwr.wroc.pl	2
acs.aliexpress.com	2
acs.aliexpress.ru	2
www.facebook.com	2
m.alibaba.com	2
ae04.alicdn.com	2
accounts.google.com	4
ae.mmstat.com	2
lh3.googleusercontent.com	2
fonts.gstatic.com	4
play.google.com	2
wykop.pl	2
www.wykop.pl	2
auschwitz.org	4

2.4 Protokoły i usługi

Do wylistowania usług i protokołów ponownie posłużyliśmy się programem Tshark. Użyliśmy do tego następującej komendy:

```
sudo tshark -i wlp0s20f3 -T fields -e frame.protocols
```

Protokół	Liczba wystąpień
eth:ethertype:ip:udp:dns	22
eth:ethertype:ip:udp:mdns	8
eth:ethertype:ip:igmp:igmp	4
eth:ethertype:ip:tcp:tls	23
eth:ethertype:ip:tcp	86
eth:ethertype:ip:udp:data	364
eth:ethertype:arp	6
eth:ethertype:ip:udp:ntp	2
eth:ethertype:ip:icmp:data	12

Niezabezpieczonymi stronami, które udało nam się znaleźć, są:

- auschwitz.org
- pks.olawa.pl

2.5 Mapa lokalizacji

Do zadania wykorzystaliśmy bazę danych GeoIP2 oraz programu **ping** do uzyskania adresów IP odwiedzanych stron. Poniżej przedstawiliśmy lokalizacje dla kilku przykładowych domen.

Domena	Adres IP	Lokalizacja
m.alibaba.com	92.123.13.141	Wiedeń, Austria
zagorski.im.pwr.wroc.pl	156.17.7.17	Wrocław, Polska
acs.aliexpress.com	47.246.146.132	Stany Zjednoczone
teams.microsoft.com	52.113.194.132	Waszyngton, Stany Zjednoczone
aliexpress.com	47.254.177.101	Frankfurt, Niemcy