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

U zadatku smo realizirali man in the middle(MitM) i denial of service (DoS) napade iskorištavanjem ranjivosti ARP protokola na istoj lokalnoj mreži.

Testirali smo napad u virtualiziranoj Docker mreži koju čine 3 virtualizirana Docker računala:

-dvije žrtve: station-1 i station-2

-napadač: evil-station

Opis zadatka:

- Pokrenuli smo Windows terminal aplikacije i Ubuntu terminala na WSL

- Klonirali smo GitHub repozitorij u navedeni direktorij

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

- Mijenjali smo direktorij

  `cd SRP-2022-23/arp-spoofing/` ,a pokretanje/zaustavljanje virtualiziranog mrežnog scenarija smo vršili pomoću naredbi `start.sh` i `stop.sh`

- Pokrenuli smo shell (bash) za station-1

  `docker exec -it station-1 bash`

- Pokrenuli smo shell (bash) za station-2
  `docker exec -it station-2 bash`

- S naredbom `ipconfig` smo saznali IP i MAC adresu

- Korištenjem naredbe `ping station-2` provjerili smo nalazi li se station-2 na istoj mreži

- Station-1 smo postavili za server pomoću naredbe `netcat -l -p 8080` ,a pomoću naredbe `netcat station-2 8080` postavili smo station-2 za client

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

  smo pokrenuli shell za evil-station

- Evil-station smo predstavili stationu-1 kao station-2 koristeći `arpspoof -t station-1 station-2` i `tcdump`. Time se narušio integritet i povjerljivost.

- Naredbom `echo 1 > /proc/sys/net/ipv4/ip_forward` izvodi se DoS napad u slučaju da presretene poruke evil-station nre proslijedi stationu-2