Lab 1

Na prvoj laboratorijskoj vjezbi zadatak je bio realizirati man in the middle i denial of service napade iskoristavanjem ranjivosti Adress Resolution Protocola.

Napad smo testirali koristeci Docker mrezu koju su sacinjavala 3 racunala, dvije zrtve, station-1 i station-2 i jedan napadac, evil-station.

Zatim smo pokrenuli Windows terminal aplikaciju i otvorili Ubuntu terminal na WSL (Windows Subsystem for Linux) sustavu, klonirali odgovarajuci GitHub repozitorij naredbom git clone https://github.com/mcagalj/SRP-2022-23

Naredbom cd SRP-2022-23/arp-spoofing/ usli smo u direktorij u kojem se nalaze skripte start.sh i stop.sh koje koristimo za pokretanje(./start.sh) i zaustavljanje(./stop.sh) virtualiziranog mrežnog scenarija. Zatim smo pokrenuli shell station-1 $ docker exec -it station-1 bash i provjerili nalazi li se station-2 na istoj mrezi(ping station-2). Pokrenuli smo shell station-2 (docker exec -it station-2 bash) i ostvarili konekciju izmedu station-1 i station-2. $ netcat -l -p 8080 $ netcat station-1 8080 Kada smo napadali pokrenuli smo shell za evil-station $ docker exec -it evil-station bash te smo koristili tcpdump i arpspoof $ arpspoof -t station-1 station-2 $ tcpdump Na kraju smo prekinili napad koristeci naredbu echo 0 > /proc/sys/net/ipv4/ip_forward.