Sigurnost računala i podataka

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

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).

Man in the middle (MitM) i denial of service (DoS) napadi realizirali smo u virtualiziranoj Docker mreži koja se sastojala od 3 virutalizirana Docker računala (containera) odnosno dva računala žrtve: station-1 i station-2 te napadača: evil-station.

U Windows terminal aplikaciji smo otvorili Ubuntu terminal na WSL sustavu.

U direktorij smo klonirali GitHub repozitorij te smo unutar njega ušli u direktorij arp-spoofing. Unutar tog direktorija se nalaze bash skripte start.sh i stop.sh koje služe za pokretanje i zaustavljanje mrežnog scenarija.

Pokrenuli smo shell za station-1 i station-2 preko naredbi:

$ docker exec -it station-1 bash

$ docker exec -it station-2 bash

Ostvarili smo konekciju između dva računala koji će biti žrtve napada: station-1 i station-2.

Station-1 smo postavili za server na portu 8000:

$ netcat -l -p 8000

Station-2 smo postavili za client spojen na station-1:

$ netcat station-1 8000

Da bi izvršili napad pokrenuli smo shell za evil-station:

$ docker exec -it evil-station bash

Pomoću naredbi arpspoof i tcpdump smo izvršili man in the middle napad jer su poruke izmedu station-1 i station-2 bile poslane preko evil-station koji je mogao pročitati sadržaj poslanih poruka.

$ arpspoof -t station-1 station-2

$ tcpdump

Izvršili smo denial of service napad, odnosno u potpunosti smo prekinuli prijenos poruka između station-1 i station-2 pomoću naredbe:

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