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

Na 1.lab vjezbi analizirali smo ranjivost Address Resolution Protocola koja napadaču omogućava izvođenje man in the middle (MitM)
i denial of service (DoS) napada na računala koja su dio iste lokalne mreže.

Za realizaciju napada koristili smo 3 virtualizirana Docker računala: žrtve station1 i station2 te napadača evil-station.

Man in the middle napad

Pokrenuli smo shell za station 1 i station 2 preko naredbi docker exec -it station-1 bash i docker exec -it station-2 bash Pri tome smo se uvjerili da su na istoj mreži sa naredbom ping. Te smo zatim uspostavili konekciju između stationa 1 i stationa 2 pri čemu smo koristili ove naredbe

netcat -l 8080

netcat station-1 8080

pri čemu je broj 8080 broj porta

Nakon toga smo pokrenuli shell za evil station sa naredbom docker exec -it evil-station bash

Prvo smo samo omogućili evil-stationu da pročita poruke koje station1 šalje stationu 2 jer su poruke išle preko evil-station čime smo narušili integritet a samim time i povjerljivost.

arpspoof -i eth0 -t station-1 station-2 (evil station želi prevariti station 1 kao da je station2)

tcpdump -qX host station-1 and not arp and not icmp (filtrirali što vidimo)

Zatim smo onemogućili stationu 2 da uopće dobiva poruke od stationa1 tako što smo prekinuli prosljeđivanje poruka sa evil-stationa na station2.

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

Za ponovno uspostavljanje prosljeđivanja poruka koristi se naredba echo 1 > /proc/sys/net/ipv4/ip_forward