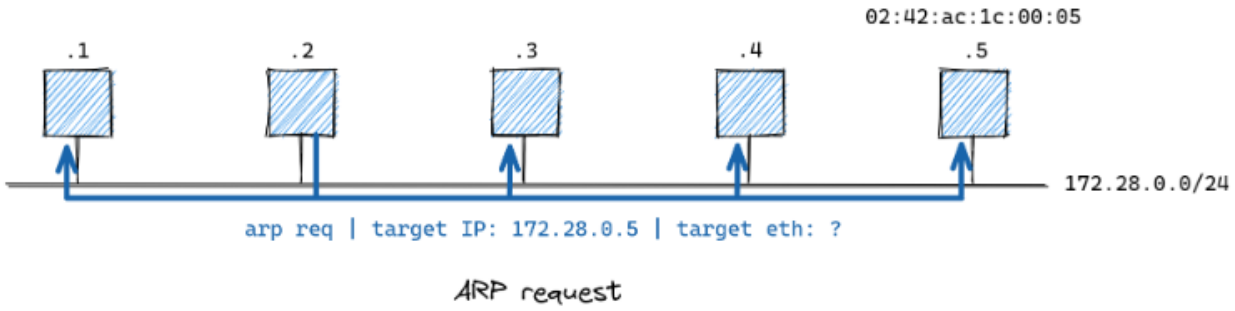
Prva laboratorijska vjezba

Na prvoj laboratorijskoj vježbi smo pokazali slabosti ARP-a (Adress resolution protocol) te simulirali “Man in the middle attack (MitM)”.

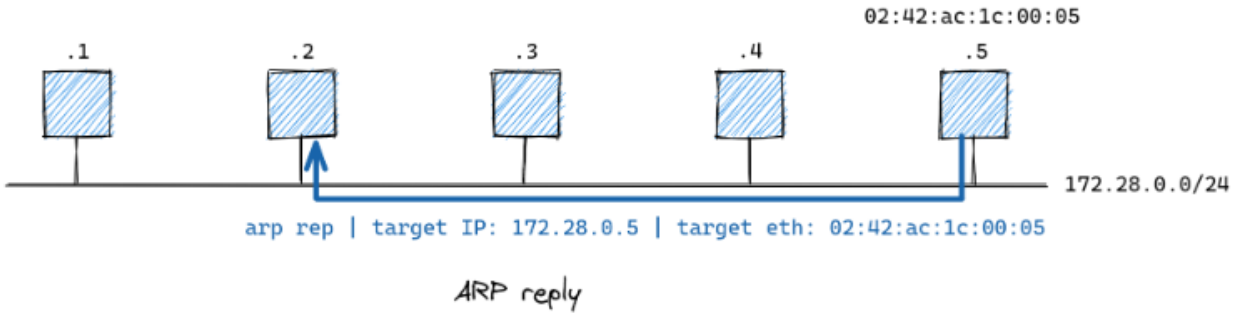
Adress resolution protocol se koristi priliko prijenosa podataka s jednog računala u mreži na drugo. Računalo pošiljatelj šalje na mrežu Arp zahtjev u kojem navodi svoje IP i MAC adrese te IP adresu primatelja poruke, a natrag traži MAC adresu primatelja kako bi mogao izvršiti slanje podataka.

“Man in the middle” napad funkcionira na način da se neko drugo računalo u mreži (”evil station” u ovom primjeru) lažno predstavi kao primatelj poruke te pošalje svoju MAC adresu pošiljatelju. Na taj način podaci dolaze do “evil station-a” te ih on može pročitati, a zatim ima i izbor: proslijediti poruke prema ciljanom primatelju ili ne.

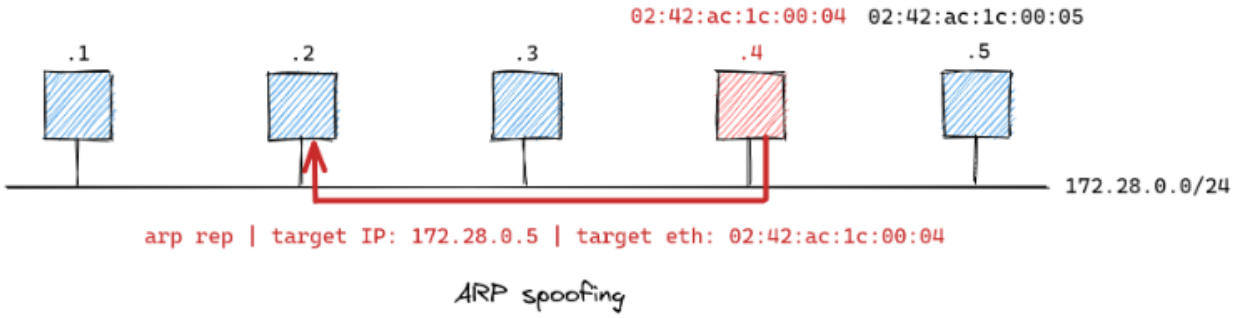
Ovakav napad se još naziva i “ARP spoofing”.



ARP request



ARP reply



ARP spoofing

Simulaciju smo izveli pomoću Docker containera u Wsl-u(Windows subsystem for Linux). Koristili smo tri “računala”, station1, station2 te evil station.

Koristili smo naredbe poput:

- $ ./start.sh → pokretanje
- $ ./stop.sh → zaustavljanje

- $ docker exec -it station-1 bash → pokretanje station1
- docker exec -it station-2 bash → pokretanje station2
- $ netcat -l -p 8000 → station1 je server na portu 8000
- $ netcat station-1 8000 → station2 je client
- $ docker exec -it evil-station bash → pokretanje evil stationa
- $ arpspoof -t station-1 station-2
- $ tcpdump