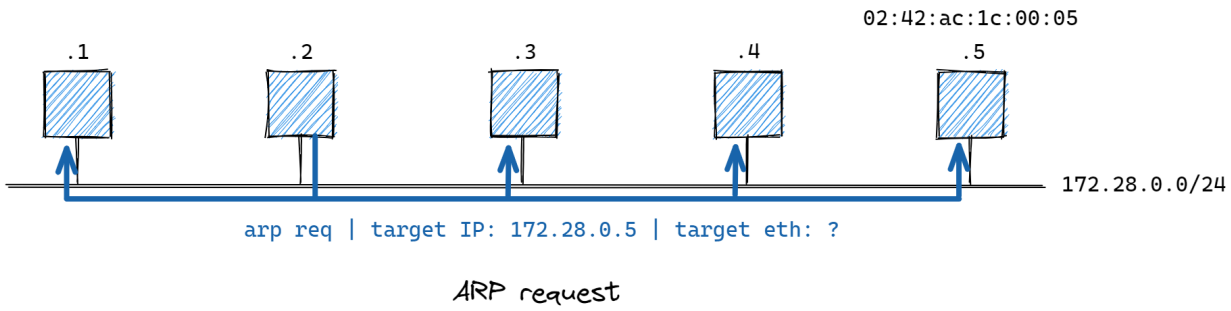
Sigurnost računala i podataka (Lab 1)

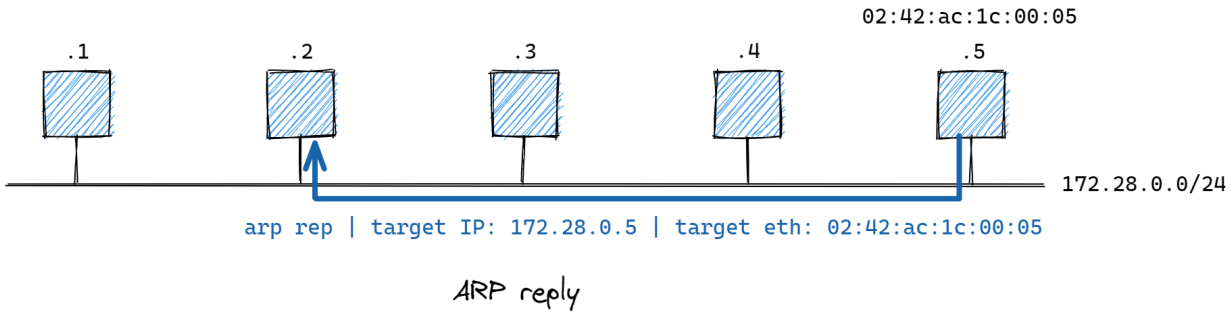
Man-in-the-middle attacks (ARP spoofing)

U okviru vježbe upoznajemo se s osnovnim sigurnosnim prijetnjama i ranjivostima u računalnim mrežama. Analizirat ćemo ranjivost *Address Resolution Protocol*-a (*ARP*) koja napadaču omogućava izvođenje *man in the middle* i *denial of service* napada na računala koja dijele zajedničku lokalnu mrežu (*LAN*).

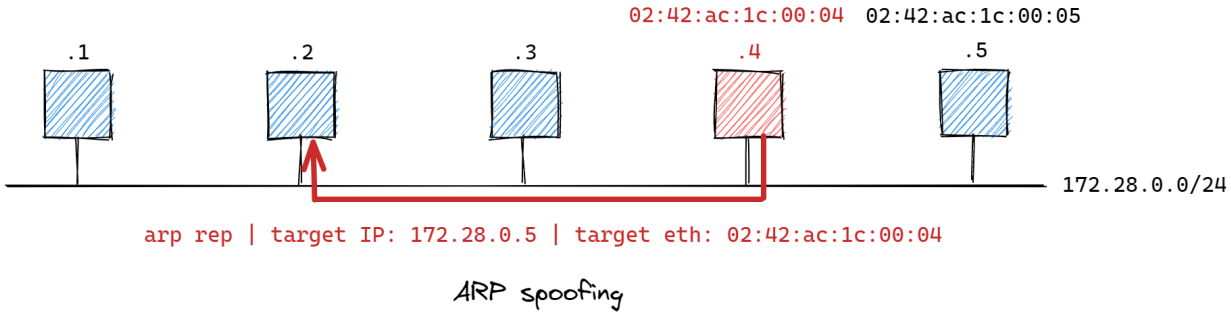
ARP spoofing



ARP request



ARP reply



ARP spoofing

Zadatak

Realizirati ***man in the middle*** napad iskorištavanjem ranjivosti ARP protokola. Student će testirati napad u virtualiziranoj Docker mreži (Docker container networking) koju čine 3 virtualizirana Docker računala (eng. *container*): dvije *žrtve* `station-1` i `station-2` te napadač `evil-station`.

Teorija

-mrežni segment s pet računala, svako ima svoju IP adresu i MAC adresu

-ako znamo samo IP adresu, a podaci se usmjeravaju preko MAC adrese, kako onda paket pronađe svoju destinaciju?

-pronađe je zahvaljujući ARP protokolu koji u osnovi mapira IP adresu u MAC adresu

—npr. računalo .2 želi poslati nešto računalu 5., zna njegovu IP adresu

u ARP requestu pita računala tko je od njih .5 i pošalje im svoju MAC adresu

.5 se javi i pošalje svoju MAC adresu u ARP replay paketu

sada .2 ima potpunu informaciju kome treba poslati paket

-ARP je ranjiv protokol

— npr. u slučaju na slici, računalo .4 se lažno predstavi i pošalje svoju MAC adresu umjesto .5

podaci će doći do napadača .4, ne do željene destinacije .5

-.4 nije nužno narušila dostupnost jer i dalje .4 može proslijediti podatke .5

-narušen je integritet (lažno predstavljenje)

Izvještaj

Pokrenuli smo Windows terminal aplikaciju i u istoj otvorili Ubuntu terminal na WSL (*Windows Subsystem for Linux*) sustavu te se pozicionirali u odgovarajući direktorij prema uputama profesora.

Klonirali smo repozitorij:

```
git clone https://github.com/mcagalj/SRP-2021-22
```

Ušli smo u direktorij `arp-spoofing/`:

```
cd SRP-2021-22/arp-spoofing/
```

U direktoriju se nalaze skripte `start.sh` i `stop.sh` koje možete pozvati za pokretanje/zaustavljanje virtualiziranog mrežnog scenarija. Ovdje se također nalaze `docker` i `docker-compose` konfiguracijske datoteke kojima su opisana Docker virtualna računala i odgovarajuća virtualna mreža.

Zatim smo napravili bildanje i pokretanje docker kontejnera.

Provjerili smo da su pokrenuti kontejnteri (station-1, station-2 i evil-station). **$ docker ps**

Pomoću **$ ifconfig -a** smo saznali IP i MAC (Ethernet) adrese.

Provjeravamo je li station-2 na istoj mreži. **$ ping station-2**

Pokretanje interaktivnog shella. **$ docker exec -it station-2 sh**

Na kontejneru station-1 pomoću netceta otvaramo server TCP socket na portu 9000. **$ netcat -lp 9000**

Na kontejneru station-2 pomoću netcata otvaramo client TCP socket na hostnameu station-1 9000. **$ netcat station-1 9000**

Pokretanje interaktivnog shella u evil-station kontejneru. **$ docker exec -it evil-station sh**

U kontejneru evil-station pokrećemo arpspoof. **$ arpspoof -t station-1 station-2** (varamo 1 da smo 2) Time je narušen integritet (cjelovitost).

Preko tcpumpa u evil-station kontejneru vidimo promet između station-1 i station-2. **$ tcpdump** Time je narušena povjerljivost.

Naredba evil-stationu da ne prosljeđuje. **echo 0 > /proc/sys/net/ipv4/ip_forward** Time je narušena dostupnost.