



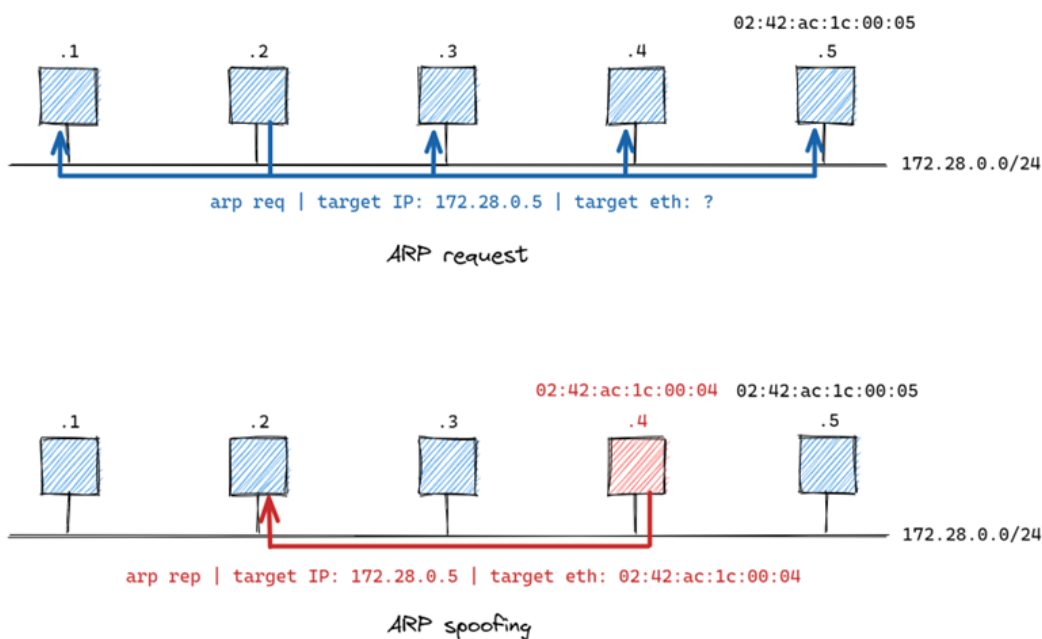
# Sigurnost i zaštita podataka

## Vježbe 1.

Iskorištavajući ranjivost ARP protokola, realizirali smo **man in the middle (MitM → ugrožen integritet)** i **denial of service (DoS → ugrožena dostupnost)** napade pomoću virtualizirane Docker mreže. Pokušaj se sastojao od tri virtualizirana Docker računala: dva su glumila žrtvu i jedan je bio napadač.

### MitM napad:

- pokrenuli smo Windows terminal i u njoj otvorili Linux terminal
- koristimo osnovne komande Windows terminala kao **cd (change directory)** i **mkdir (make directory)** kako bi kopirali sredstva iz repozitorija (naredba **git clone**) koja su nam trebala za MitM napad
- **ARP spoofing** - napadač se pretvara da je primatelj što dovodi do MitM i DoS napada



- koristili smo naredbu **ping** kako bi stvorili komunikaciju između dvije žrtve
- koristili smo naredbu **arpspoof** kako bi presleli podatke koje šalje jedno računalo drugom
- koristili smo naredbu **netcat** za prisluškivanje poruka

### **DoS napad:**

- nakon uspješnog MitM napada, proveli smo DoS napad gdje napadač prestaje slati poruke željenom primatelju
- koristili smo naredbu **echo 0** kako bi prestali slati podatke
- koristili smo naredbu **echo 1** kako bi ponovno počeli slati podatke