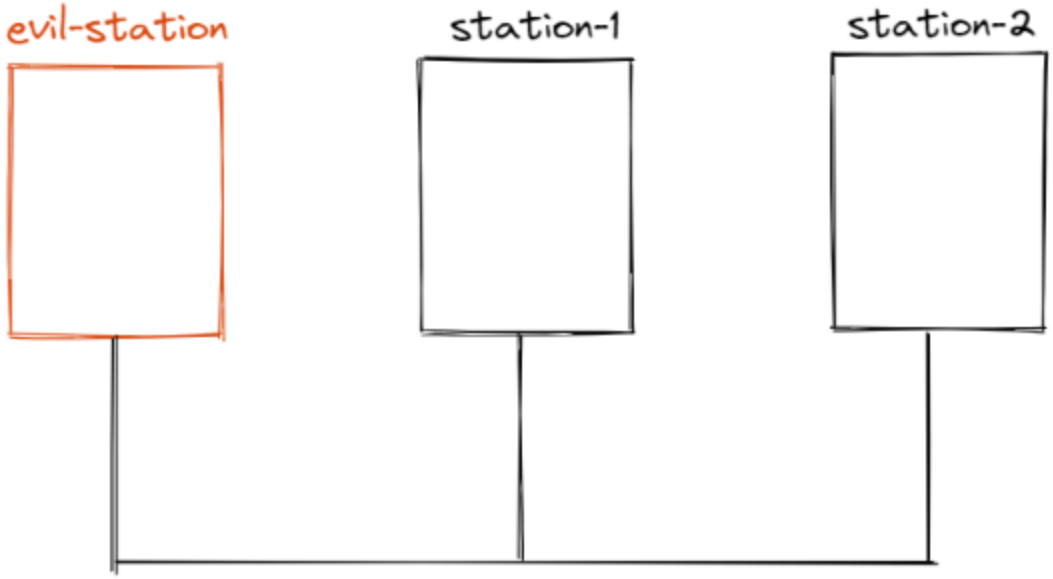
Sigurnost računala i podataka (Lab 1)

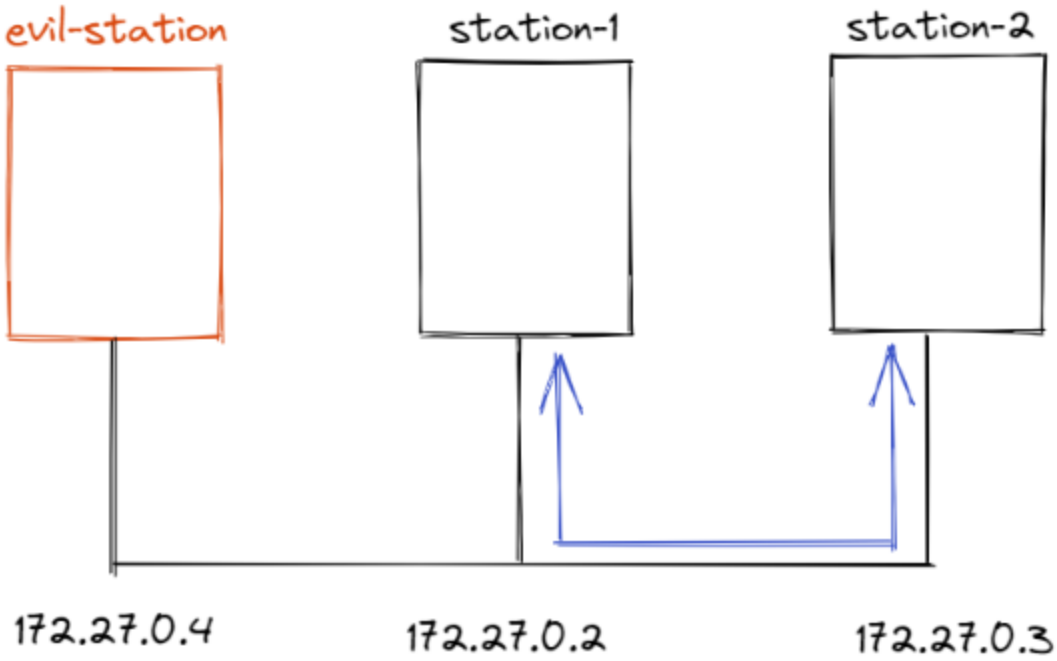
Man-in-the-middle attacks (ARP spoofing)

U ovoj vježbi smo se upoznali sa osnovnim sigurnosnim prijetnjama i ranjivostima u računalnim mrežama. Analizirali smo ranjivosti *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)*.

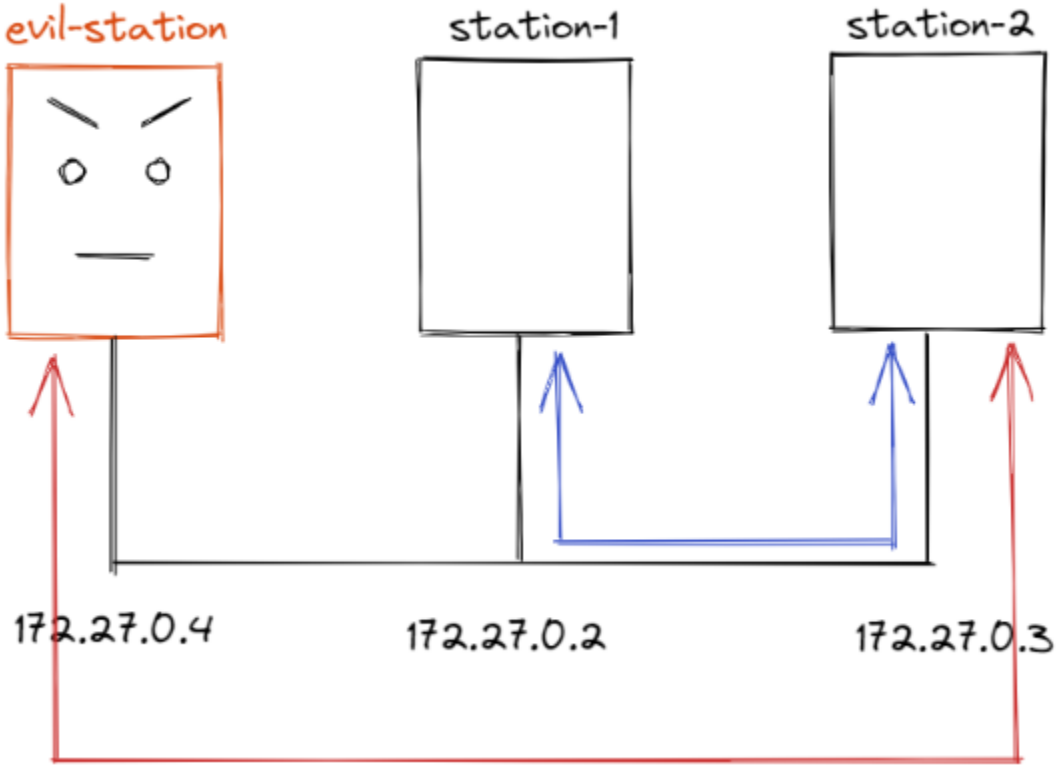
Realizirali smo main in the middle napad iskorištavanjem ranjivosti ARP protokola. To smo uradili tako da smo testirali napad u virtualiziranoj Docker mreži koju čine 3 virtualizirana Docker računala (eng.container): dvije žrtve station-1 i station-2 te napadač evil-station.



Zatim smo uspostavili komunikaciju izmedju station-1 i station-2 računala i promatrali njihovu međusobnu komunikaciju. Zahvaljujući ARP protokolu komunikacija među njima je moguća jer računala znaju IP adresu ali ne znaju MAC adresu preko koje se odvija ta komunikacija (usmjeravanje paketa).



Onda smo vidjeli kako napadač evil-station može prisluškivati tu komunikaciju tako da se lažno predstavi kao jedno od računala, u našem slučaju station-2 s kojim želi komunicirati station-1. U ovom slučaju svi paketi koji se šalju između station-a 1 i station-a 2 dolaze i do evil-stationa. Evil-sation može i sam slati, usmjeriti sebi ali i sakriti pakete od pravpg station-a kojemu se šalju paketi.



U ARP spoofing napadu je narušavanje integriteta dovelo do ovakvog napada. Ovo je primjer aktivnog napada.