Lab 1

- CIA → povjerljivost,integritet i dostupnost
  - ARP (Adress Resolution Protocol) je protokol koji se koristi kod LAN mreža, a sadrži ARP tablicu u kojoj su povezane IP adrese nekog računala sa MAC (fizičkim) adresama
  - 3 osnovne kategorije iskorištavanja ARP ranjivosti:

  1. skupljanje inf. → narušena povjerljivost
  2. posrednik (Man in the middle) → narušena povjerljivost podataka i **integritet**
  3. uskraćivanje usluge (Denial of service) → narušena dostupnost

- zaštita povjerljivosti ne osigurava zaštitu integriteta
- aktivnim napadom se narušava integritet → Man-in-the-middle napad
- ARP spoofing → narušen integritet (netko se lažno predstavlja)
- DoS napad → uskraćivanje usluge, narušena dostupnost
- ranjivost ARP-a → man in the middle i DoS napadi preko LAN-a
- Docker mreža → station-1, station-2, evil-station
- Pokretanje mreže:

▼ **Windows terminal aplikacija → Ubuntu terminal na WSL sustavu**

▼ **mkd dir_(ime direktorija) → stvaranje direktorija i poddirektorija**

▼ **cd_(ime direktorija) → pozicioniranje u odgovarajući direktorij**

▼ **3 Docker računala → station-1, station-2 i evil-station**

▼ **provjera dostupnosti servera → ping**

▼ **netcat → uspostava komunikacijskog kanala između Docker računala (station-1 i station-2)**

▼ **arpspoof → evil-station tako prisluškuje komunikaciju između dva računala**

▼ **tcpdump -i etho → evil-station ispisuje sve što čuje**

ZAKLJUČAK

- Napadač iskorištava ranjivost sustava kako bi istom nanio štetu → narušavanje osnovnih sigurnosnih zahtjeva (povjerljivost, integritet i dostupnost)
- Kod ARP spoofinga napadač osluškuje višeodredišni ARP zahtjev u LAN mreži te nakon što je zahtjev poslan, napadač šalje lažni ARP odgovor sa svojom MAC adresom
- Kod MITM napada napadač preusmjerava komunikaciju između dva računala preko sebe ,lažno se predstavljajući, tako da se sve poruke između dva računala prvo šalju napadaču koji s njima radi što god želi i potom ih prosljeđuje žrtvi čime narušava integritet podataka.