Laboratorijske vježbe 1

Na prvim laboratorijskim vježbama radili smo osnovne napade kojim se ugrožavaju:

- povjerljivost (confidentiality)
- integritet (integrity)
- dostupnost (availability)

Radili smo dvije vrste napada, a to su **Man-in-The-Middle (MiTM)** i **Denial-of-Service (DoS).**

U Windows Terminalu smo koristeći WSL (*Windows Subsystem for Linux*) pokrenuli Ubuntu. Pozicionirali smo se u direktorij gdje se nalaze skripte *start.s*h i *stop.sh.* Zatim smo stvorili 3 virtualizirana Docker računala (**station-1**, **station-2** i **evil-station**). Koristili smo naredbe

- *docker exec -it station-1 bash*
- *docker exec -it station-2 bash*

za stvaranje 2 računala koja su žrtve napada. Provjerili smo im IP adrese i jesu li na istoj mreži naredbama *ipconfig* i *ping*. Zatim smo ih povezali naredbama:

- *netcat -l -p 8080*
- *netcat station-1 8080*

Sljedeći korak bio je pomoću 3. računala (evil-station*)* izvršiti ranije spomenute napade.

Stvoreno je naredbom *docker exec -it evil-station bash*. Pokušali smo pratiti promet između prva dva računala naredbom *tcpdump*. U početku to nije bilo moguće, pa smo morali iskoristiti ranjivost **ARP protokola** i lažno se predstaviti računalu 1 kao računalo 2. Zbog toga je sav promet od station-1 do station-2 išao preko evil-station računala i postignut je **MiTM** napad pomoću kojeg smo sada mogli pratiti sav promet naredbom *tcpdump*. Time je narušen integritet. Narušavanje dostupnosti radi se napadom **DoS** tako da se prekine slanje podataka stationu-2 naredbom *echo 0 > /proc/sys/net/ipv4/ip_forward* i sve što šalje station-1 prima samo napadač evil-station.