IZVJEŠTAJ 1. LABORATORIJSKE VJEŽBE

U okviru sigurnog okruženja (Dockera), na laboratorijskim vježbama smo obradili ranjivost ARP (Address Resolution Protocol) protokola. Kod tog protokola, računalo koje želi poslati paket treba saznati MAC adresu računala sa kojim želi komunicirati, a već poznaje IP adresu tog računala. Ranjivost je ta što se neko računalo može lažno 'predstaviti' na temelju samog poznavanja IP adrese drugog računala te na taj način provesti:

1. Man in the Middle napad (MitM)
2. Denial of Service napad (DoS)

Kod MitM napada, bilo koje računalo može čitati sadržaj poslanih paketa između dvaju ili više računala, dok DoS napadom možemo potpuno blokirati slanje paketa od jednog računala prema drigome bez znanja pošiljatelja.

Vježbu smo izveli na sljedeći način: postavili smo 3 računala (station-1 i satiton-2 koja komuniciraju na mreži te evil-station kojim smo izvršavali napade) te smo povezali station-1 i station-2. Unutar Git repozitoria: https://github.com/mcagalj/SRP-2022-23 smo pronašli 2 skripte s kojima smo pokrenuli komunikaciju između station-1 i station-2 (start.sh i stop.sh).

2 stationa smo povezali na način da smo za server odabrali station-1 koji smo postavili na port 8080 te smo station-2 povezali na isti.

Command:

netcat –l –p 8080 //unosili u station-1

netcat station-1 8080 //unosili u station-2

Nakon što je otvorena veza između 2 računala, pokrećemo skriptu za evil-station

Command:

docker exec -it evil-station bash

Nakon što smo pokrenuli evil-station krećemo sa MitM napadom koristeći naredbe:

- arpspoof -> preusmjeravanje paketa na LAN mreži
- tcpdump -> *dump traffic-a* na mrežu

Na ovaj način smo mogli preusmjeriti i čitati sadržaj poslannih poruka između station-1 i station-2.

Kada već napravili uspješan MitM napad, samo unesemo naredbu (*) kojom jedostavno zaustavljamo slanje paketa od station-1 do station-2, već station-1 direktno šalje sve poruke evil-station-u.

*Command:

echo 0 > /proc/sys/net/ipv4/ip_forward

Kako bismo prekinuli napad tj. omogućili ponovnu komunikaciju između station-1 i station-2 koristimo naredbu:

Command:

echo 1 > /proc/sys/net/ipv4/ip_forward