lab 1

Sigurnost računala i podataka (Lab 1)

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

Zadatak

Realizirati *man in the middle* napad iskorištavanjem ranjivosti ARP protokola. Student će testirati napad u virtualiziranoj Docker mreži (Docker container networking) koju čine 3 virtualizirana Docker računala (eng. *container*): dvije *žrtve* `station-1` i `station-2` te napadač `evil-station`.

Prvo otvorimo repozitorij SRP-2021-22 i zatim idemo u direktorij arp-spoofing

1. Uđemo u direktorij

cd SRP-2021-22/arp-spoofing/

2. Pokretanje i zaustavljanje docker containera smo izvršili sa $ ./start.sh i $ ./stop.sh
3. docker ps nam omogućuje da vidimo izlist trenutnih containera
4. $ docker ps exec -it sh ——> ovo omogućava pokretanje shella za station-1
5. ifconfig -a ——> dobijamo status mreže
6. ping station-2 omogućuje da vidimo dijeli li on mrežu sa station-1
7. Zatim otvaramo shell za station-2 sa exec naredbom
8. na stationu-2 izvršavamo naredbu netcat
9. Pokrećemo shell za evil-station ($ docker exec -it evil-station sh)

10. U evil-station pokrećemo arp spoofing——→ $ arpspoof -t station-1 station-2
11. pokrećemo tcpdump i pratimo što se događa izmedu dva stationa
12. gasimo arp spoofing izmedu dva station sa ($ echo 0 > /proc/sys/net/ipv4/ip_forward)