Man-in-the-middle

Man-in-the-middle (MiTM) napad je vrsta cyber napada u kojem napadač potajno presreće i prenosi poruke između dviju strana koje vjeruju da komuniciraju izravno jedna s drugom, ovim napadam naružavamo integritet.

User 2

User 1

Man in the middle

Na vježbama smo koristili virtualne mašine pomoću programa Docker pomoću kojega smo realizirali 3 virtualne mažine koje bii glumile ulogu user 1, user 2, man in the middle attacker

Ovo smo sve izvodili I pratili preko terminal na WSL-u te pratili upute sa git-a

* Kopirali smo: git clone <https://github.com/mcagalj/SRP-2022-23>
* Te otisli u drugi direktorij sa: cd SRP-2022-23/arp-spoofing/
* Pokrenili shell za user 1 I user 2 sa naredbama : docker exec -it user-1 bash i docker exec -it user-2 bash
* Pomocu naredbe ipconfig smo saznali ip I mac adese
* Napad smo izveli pomoču naredbe: echo 0 > /proc/sys/net/ipv4/ip\_forward