Sigurnost računala i podataka

Laboratorijska vježba 1

Man in the middle attacks (ARP spoofing)

U prvoj laboratorijskoj vježbi analizirali smo ranjivost Address Resolution Protocol-a (ARP) koja nam je omogućila da izvedemoman in the middle napad na računala koja dijele zajedničku lokalnu mrežu. Napadom presretnemo komunikaciju crypto oracle servera i računala.

Napad smo testirali koristeći vizualiziranu Docker mrežu koju su činila 3 docker računala; jedan napadač - evil-station, te dvije žrtve station-1 i station-2.

Pokrenuli smo Windows terminal aplikaciju i potom otvorili Ubuntu terminal na WSL

sustavu. Pozicionirali smo se u odgovarajući direktorij te klonirali GitHub repozitorij naredbom:

git clone https://github.com/mcagalj/SRP-2021-22

Naredbom cd ušli smo u direktorij arp-spoofing/ u kojem se nalaze

skripte start.sh i stop.sh koje služe za pokretanje i zaustavljanje docker kontejnera.

Potom smo pokrenuli shell station-1 i provjerili konfiguraciju mrežnog interface-a.

Pokretanje shella station-1

$ docker exec -it station-1 bash

Provjera konfiguracije mrežnog interface-a

$ ifconfig -a

Potom smo provjerili nalazi li se i station-2 na istoj mreži te pokrenuli shell za station2.

Provjera mreže

$ ping station-2

Pokretanje shella station-2

$ docker exec -it station-2 bash

Potom smo ostvarili konekciju između station-1 i station-2.

Station-1 → server na portu 8000

$ netcat -l -p 8000

Station 2 → client na hostname-u station-1 8000

$ netcat station-1 8000

Da bismo napali, pokrenuli smo shell za evil-station i isprobali tcpdump koji omogućava praćenje prometa i arpspoof.

Pokretanje shella evil-station

$ docker exec -it evil-station bash

Arpspoof

$ arpspoof -t station-1 station-2

Tcpdump

$ tcpdump

Na samom kraju vježbe smo u potpunosti prekinuli konekciju između station-1 i station-2 naredbom:

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