LAPORAN PRAKTIKUM NETWORK SECURITY Topik: Sniffing, Spoofing, Session Hijacking, dan Backdoor

Identitas Praktikan

- **Nama:** Eko Prasetyo Adi Nugroho (Client) (105841114223)

  Rizky Adhitya (Attacker) (105841114123)

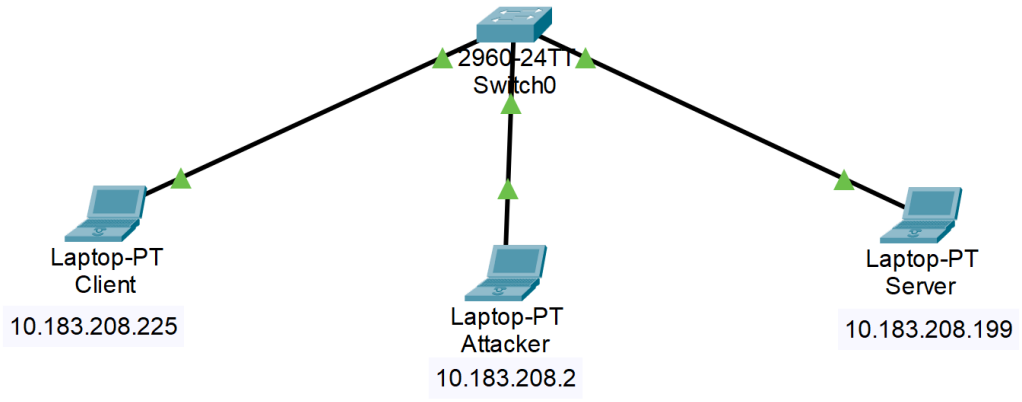
  Andi Syam Hasbullah (Server) (105841114623)
- **Kelas:** 5 JK-A

- **Mata Kuliah:** ADVANCED NETWORK SECURITY AND PROTOCOLS

I. ARP SPOOFING

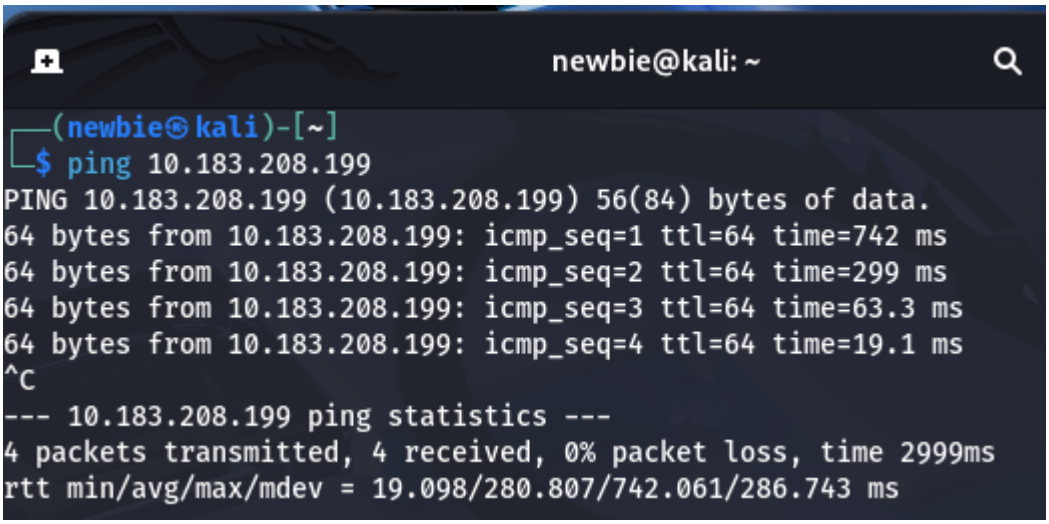
A. Gambar Topologi Jaringan beserta IP Address Topologi jaringan yang digunakan adalah jaringan lokal (Local Area Network) yang terhubung melalui Hotspot Gateway.

- **Server (Target 1):** IP 10.183.208.199 (OS: Kali Linux)
- **Client (Target 2):** IP 10.183.208.225 (OS: Kali Linux)
- **Attacker:** IP 10.183.208.2 (OS: Kali Linux)

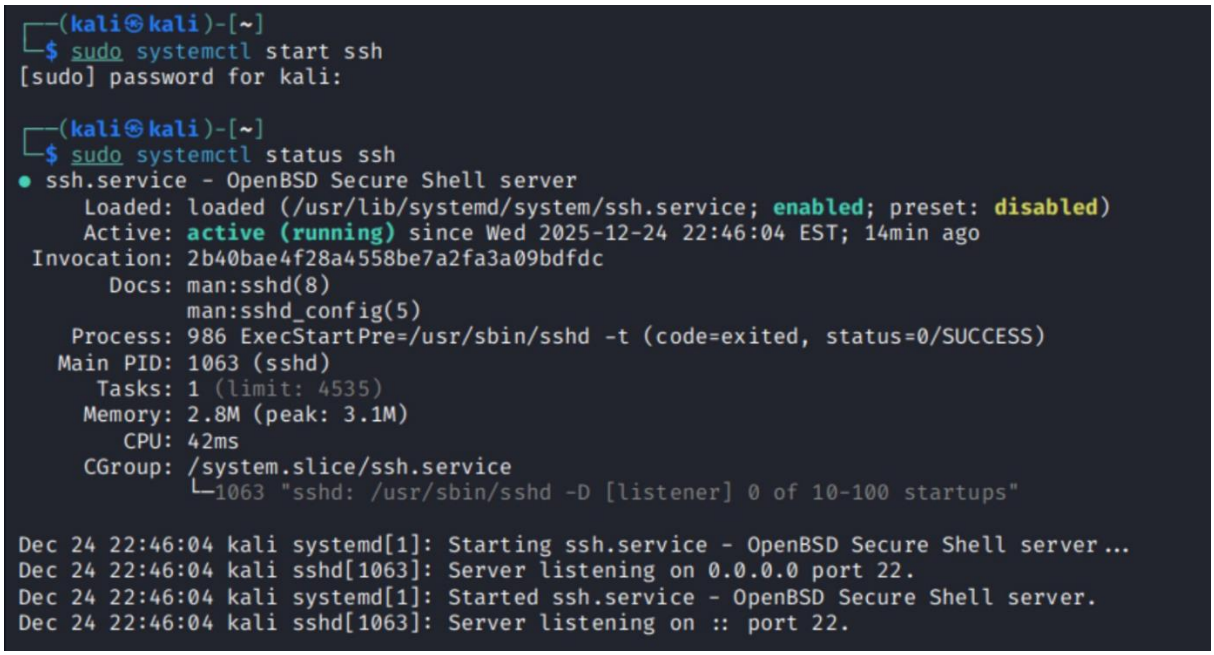


Gambar Topologi Jaringan

B. Instalasi Aplikasi Telnet & SSH dan Tes Koneksi Layanan Telnet dan SSH telah diinstal dan dijalankan pada Server (systemctl start ssh). Tes koneksi ping dari Client ke Server berhasil dengan respon *reply* yang stabil.



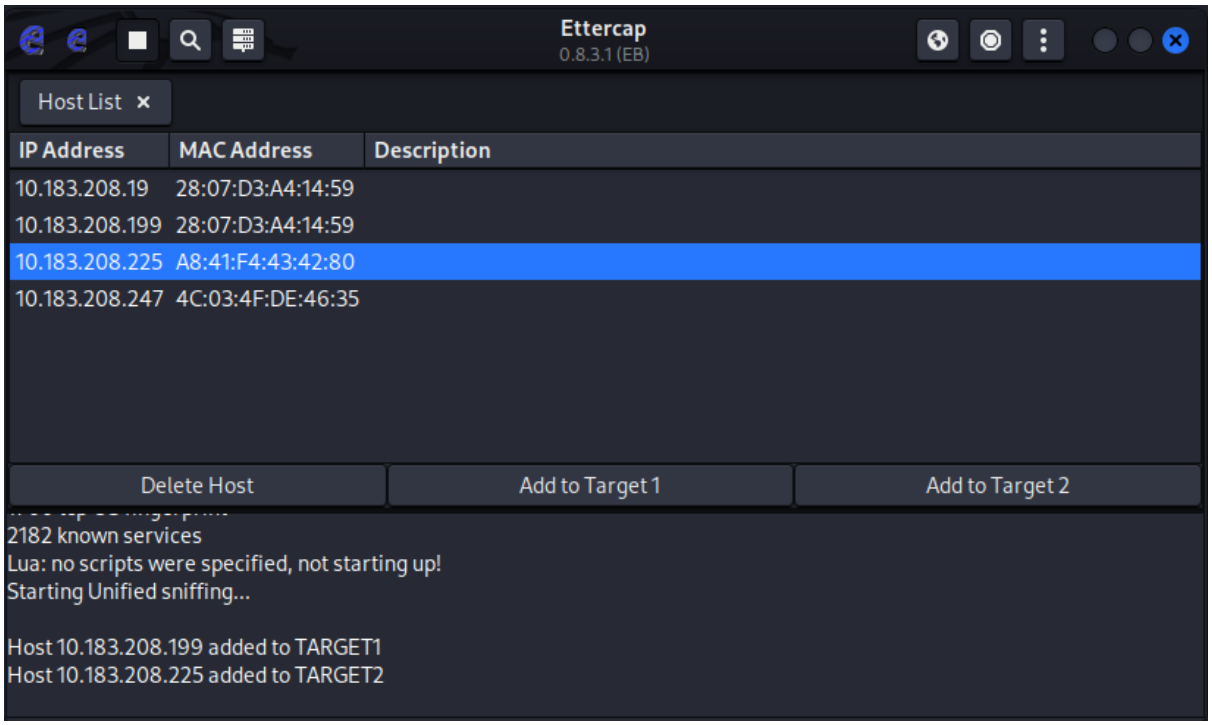
Gambar Ping Clinet Ke Server



Gambar Server Menjalankan Ssh

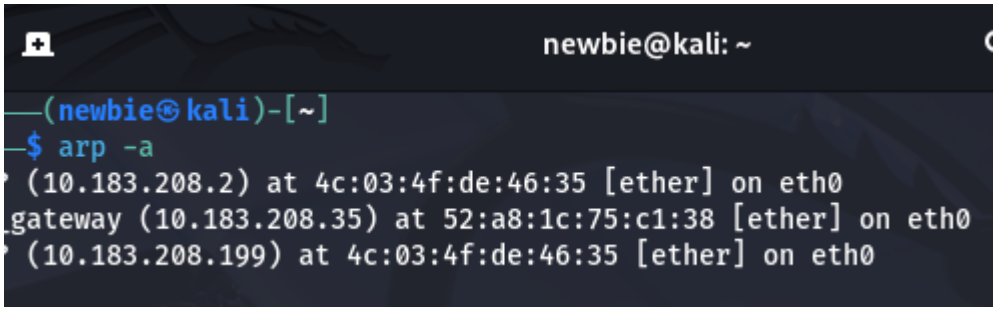
C. Catat MAC Address Client dan Server Sebelum serangan dilakukan, identitas fisik (MAC Address) perangkat terdeteksi sebagai berikut:

- MAC Address Server (.199): 28:07:D3:A4:14:59
- MAC Address Client (.225): A8:41:F4:43:42:80



Gambar Mac Address Client Dan Server Di Hostlist Ettercap

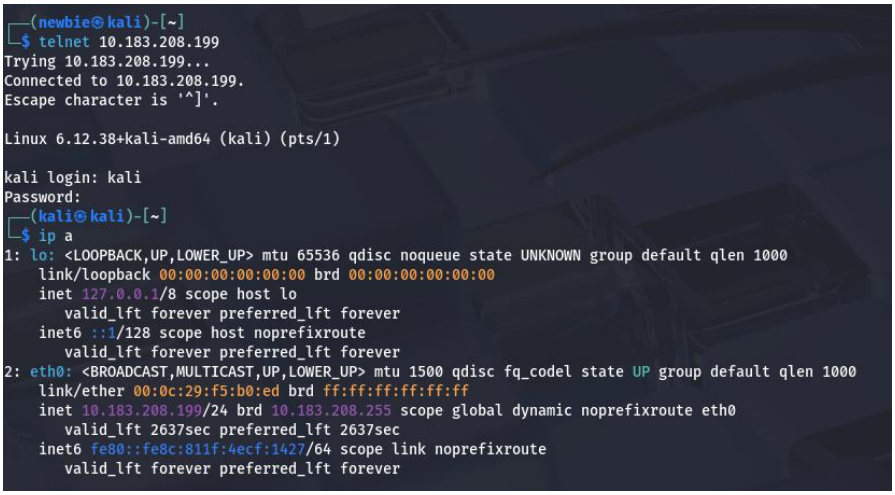
D. Catat MAC Address Setelah ARP Spoofing Serangan ARP Spoofing dilakukan menggunakan *Ettercap* dengan teknik *Man-in-the-Middle* (MITM). Tabel ARP pada Client berubah, di mana IP Server dipetakan ke MAC Address milik Attacker, sehingga lalu lintas data berbelok ke Attacker.



Gambar Mac Address Server Yang Dilihat Dari Client,Telah Berubah

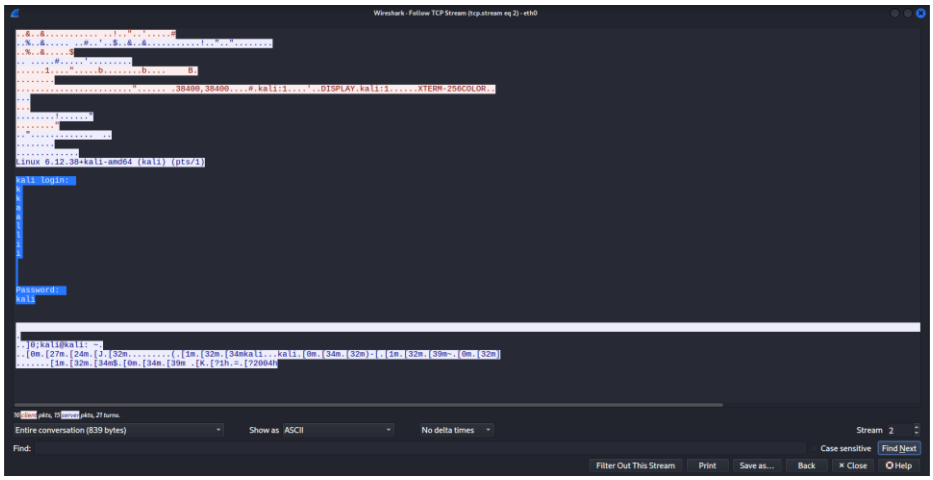
E. Catat Proses Terjadinya Session Hijacking

1. **Telnet Client-Server:** Client melakukan login ke server menggunakan perintah telnet 10.183.208.199 dan memasukkan username kali serta password kali.

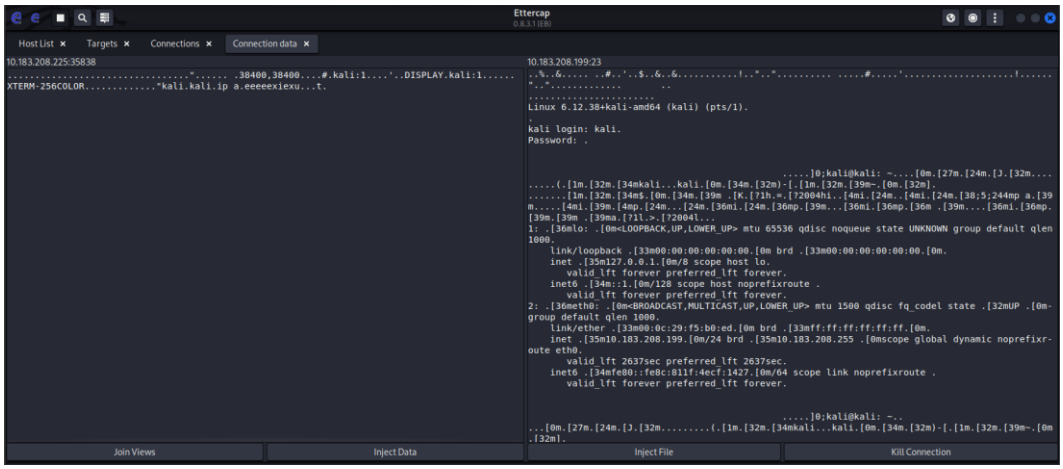


gambar client login ke server

2. **Amati pada Komputer Attacker:** Karena protokol Telnet tidak terenkripsi, Attacker berhasil menyadap komunikasi tersebut. Pada Wireshark, fitur *Follow TCP Stream* menampilkan username dan password dalam teks polos (*cleartext*).



Gambar tcp stream di wireshark



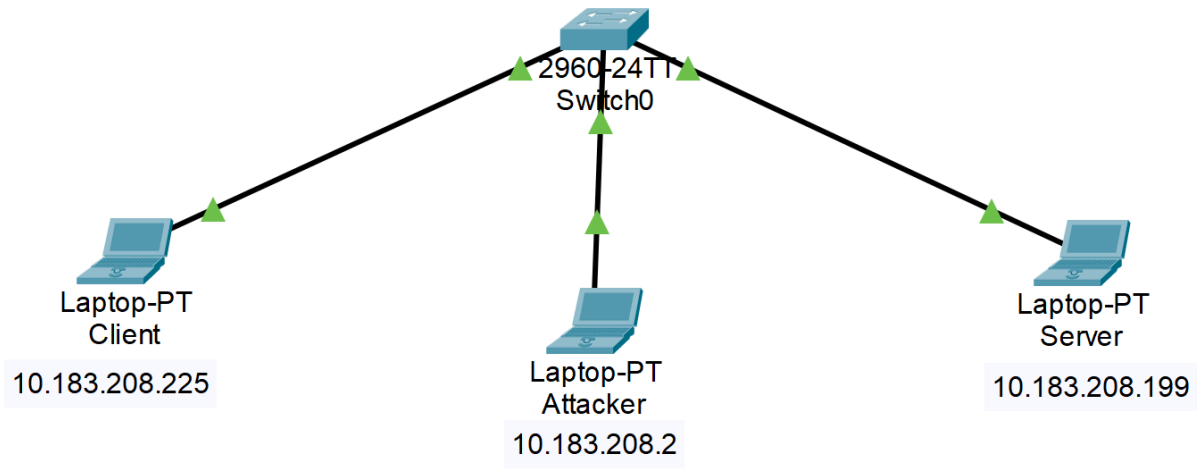
Gambar Password Dan Username Dicapat Dari Client Pada Ettercap

3. **Koneksi Client-Server setelah Hijacking:** Koneksi terlihat normal (*Established*) pada sisi korban, namun secara fisik paket data melewati mesin Attacker terlebih dahulu.

4. **Percobaan pada SSH:** Saat dilakukan pada SSH, serangan Sniffing gagal mendapatkan password karena data terenkripsi (cipher text), sehingga Session Hijacking lebih sulit dilakukan tanpa kunci dekripsi.

II. IP SPOOFING

A. Gambar Topologi Jaringan Topologi sama dengan percobaan sebelumnya. Attacker menggunakan *tools* hping3 untuk memanipulasi header paket IP.



B. Jalankan Tool IP Spoofing dan Catat Hasilnya

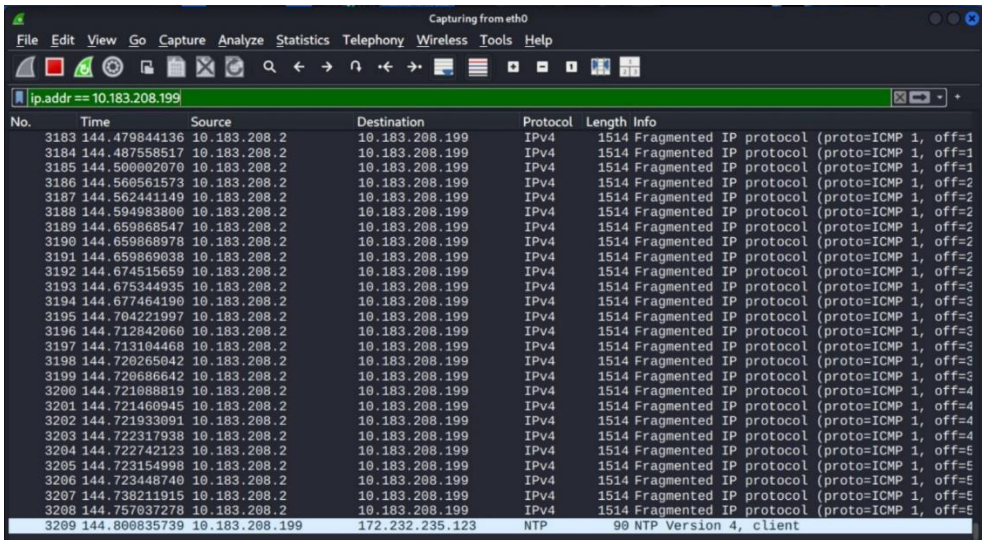
1. **Pod_spoofing (Ping of Death)**

   Perintah: sudo hping3 --icmp -d 65000 --flood 10.183.208.199

   Hasil: Mengirimkan paket ICMP berukuran raksasa (>65.000 bytes) yang terfragmentasi, membebani proses penyatuan ulang paket di server.

```
┌──(kali㉿kali)-[~]
└─$ sudo hping3 --icmp -d 65000 --flood 10.183.208.199
HPING 10.183.208.199 (eth0 10.183.208.199): icmp mode set, 28 headers + 65000 data bytes
hping in flood mode, no replies will be shown
```

Gambar Command Ping Of Death

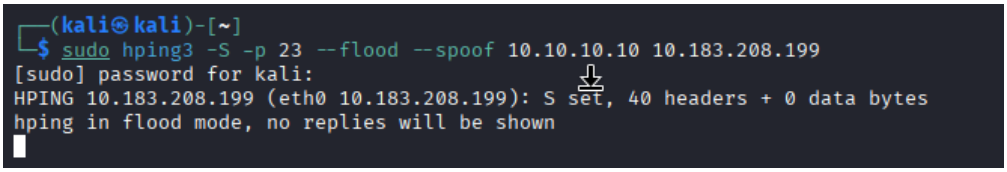


Gambar Hasil Setelah Command Di Run Pada Wireshark

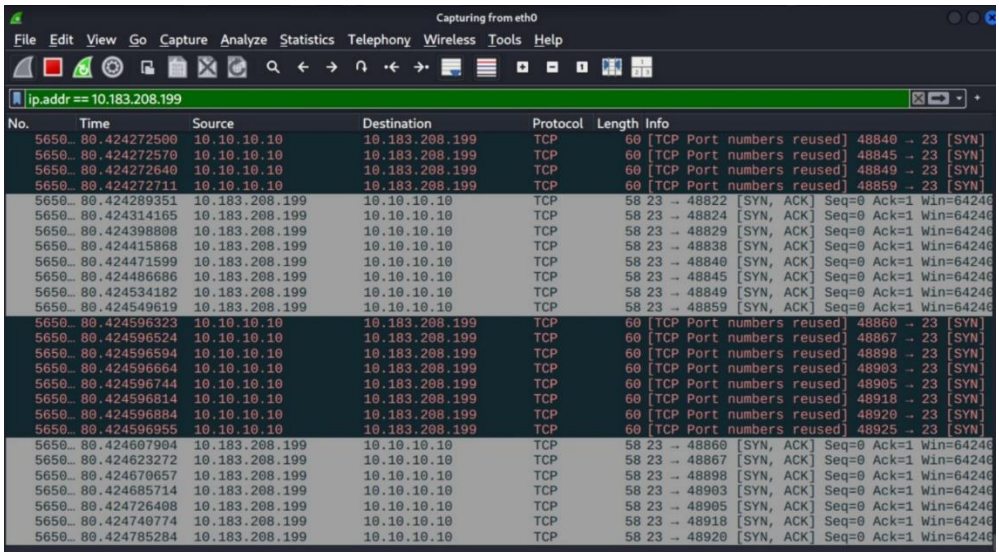
2. **Syn_flood**

Perintah: sudo hping3 -S -p 23 --flood --spoof 10.10.10.10 10.183.208.199

Hasil: Server dibanjiri permintaan koneksi (SYN) palsu dari IP 10.10.10.10. Hal ini memenuhi tabel koneksi server (*half-open connection*).



Gambar Command Syn Flood

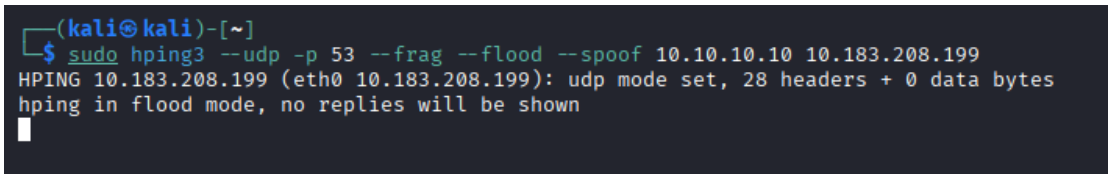


Gambar Hasil Command Setelah Di Run Pada Wireshark

3. Teardrop Attack + Spoofing

- **Perintah:** sudo hping3 --udp -p 53 --frag --flood --spoof 10.10.10.10 10.183.208.199

  Hasil: Serangan ini mengeksploitasi mekanisme re-assembly paket pada target. Penyerang mengirimkan paket data yang telah dipecah (terfragmentasi) dengan IP palsu (10.10.10.10). Server target dipaksa mengalokasikan sumber daya CPU untuk mencoba menyatukan kembali fragmen-fragmen tersebut. Pada sistem operasi lawas yang rentan, hal ini dapat menyebabkan Crash atau Blue Screen of Death karena ketidakmampuan menangani overlapping offset pada fragmen paket.

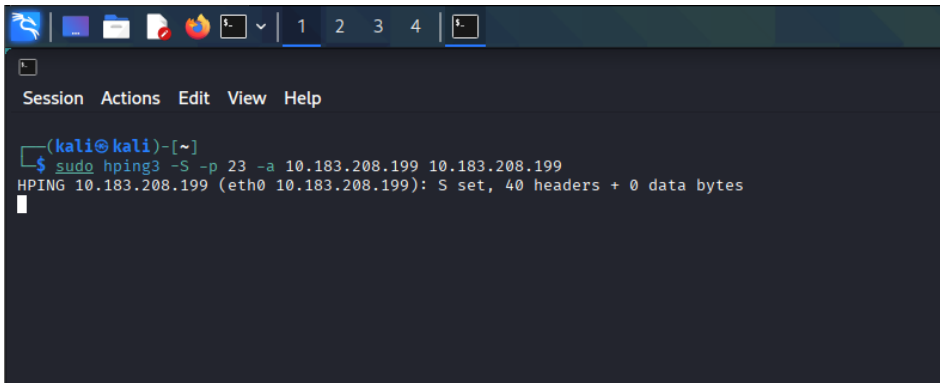


Gambar Command Teardrop+Spoofing

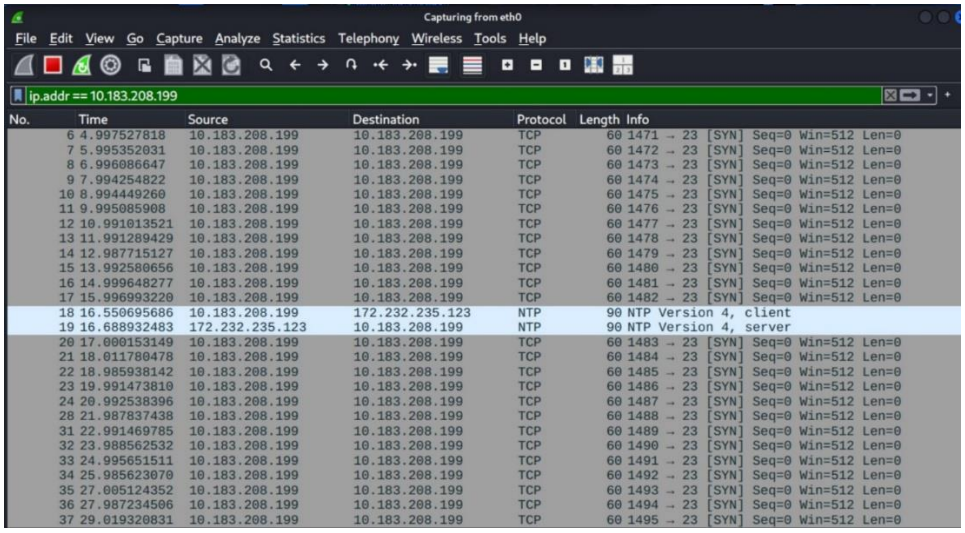
3. **Land_attack**

Perintah: sudo hping3 -S -p 23 -a 10.183.208.199 10.183.208.199

Hasil: Paket dikirim dengan IP Asal yang sama dengan IP Tujuan (.199). Server menjadi bingung karena membalas paket ke dirinya sendiri secara berulang (*looping*).



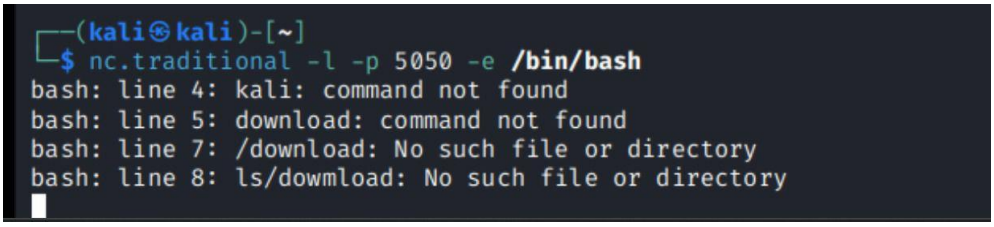
Gambar Command Land Stack



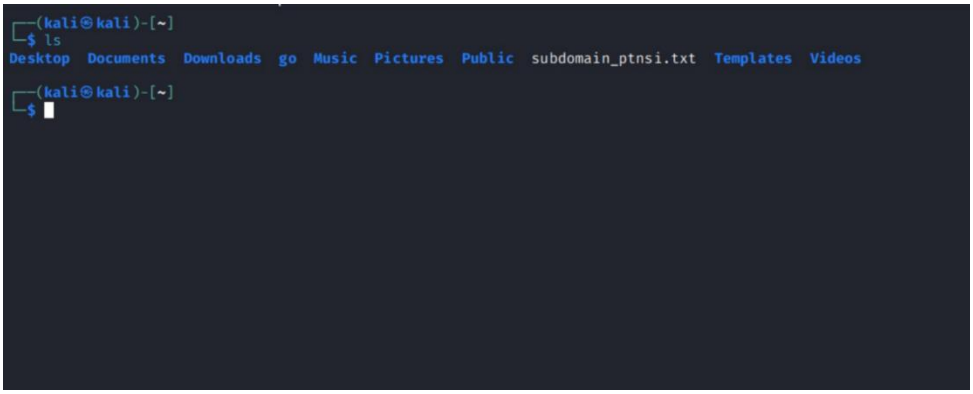
Gambar Hasil Command Setelah Di Run Pada Wireshark

C. Amati Serangan dengan Tool

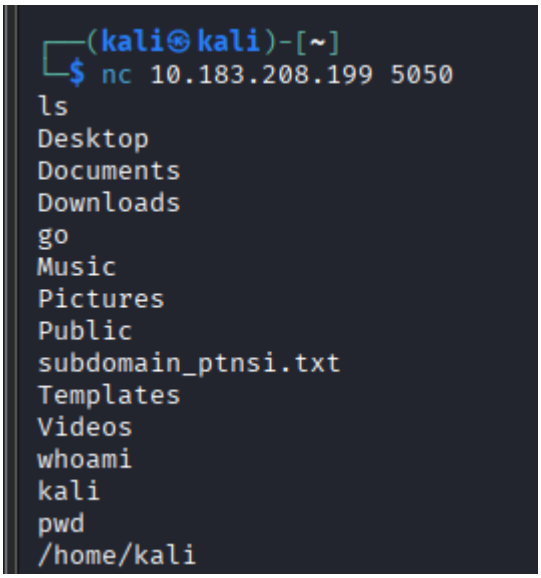
1. **Analisa Wireshark:** Wireshark menangkap anomali trafik berupa banjir paket merah/hitam (TCP Retransmission/Dup ACK) dan paket fragmentasi ICMP dalam jumlah masif.
2. **Netcat (Backdoor):** Attacker berhasil masuk ke sistem server melalui *backdoor* Netcat yang terbuka pada port 5050 tanpa proses login autentikasi. Attacker memiliki akses penuh untuk mengeksekusi perintah shell seperti ls dan whoami.



Gambar Server Menjalankan Command Nc



Gambar Directory Server



Gambar Command Dan Hasil Ls Setelah Di Run

III. KESIMPULAN DAN ANALISIS

1. Kesimpulan Hasil Praktikum Praktikum ini membuktikan bahwa protokol jaringan lawas seperti Telnet sangat tidak aman digunakan dalam jaringan publik maupun lokal karena mengirimkan data tanpa enkripsi, sehingga mudah disadap menggunakan serangan ARP Spoofing (Man-in-the-Middle). Selain itu, protokol TCP/IP memiliki kerentanan desain yang memungkinkan terjadinya pemalsuan identitas (IP Spoofing) untuk melakukan serangan Denial of Service (DoS) dan membanjiri sumber daya server.

2. Perbedaan Metode IP Spoofing

- **SYN Flood:** Menyerang memori koneksi server. Penyerang mengirim sinyal "ajakan berkenalan" (SYN) palsu terus-menerus tanpa pernah menyelesaikan prosesnya, membuat server "digantung" menunggu balasan.
- **Land Attack:** Menyerang logika server. Penyerang memalsukan alamat pengirim menjadi alamat server itu sendiri, sehingga server sibuk berbicara dengan dirinya sendiri.

- **Ping of Death:** Menyerang buffer data server. Penyerang mengirim paket data yang ukurannya melebihi kapasitas standar, memaksa server bekerja keras menyatukan pecahan paket tersebut hingga berpotensi crash.

3. Transport Layer pada IP Spoofing Tipe transport layer yang dominan digunakan dalam praktikum ini adalah **TCP (Transmission Control Protocol)**. Hal ini karena TCP memiliki mekanisme *handshake* (jabat tangan) yang mewajibkan server untuk merespons setiap permintaan koneksi (SYN) dengan balasan (SYN-ACK). Penyerang mengeksploitasi "kewajiban" server ini dengan mengirimkan permintaan palsu sebanyak-banyaknya untuk menghabiskan sumber daya server.

4. Penangkalan (Mitigasi)

- **ARP Spoofing:** Gunakan enkripsi (SSH/VPN) agar data tidak bisa dibaca walau disadap, atau gunakan fitur *DHCP Snooping* dan *Dynamic ARP Inspection* pada switch jaringan.
- **IP Spoofing:** Konfigurasi Firewall untuk memblokir paket masuk yang memiliki alamat IP asal yang mencurigakan (Ingress Filtering) dan aktifkan fitur *SYN Cookies* pada server.