SUKMA WARDIA NINGSIH

105841112723

5 JK-B

Bagian 1: Passive Reconnaissance (Pengintaian Pasif)

A. Passive Recon adalah tahap pengumpulan informasi tanpa berinteraksi langsung dengan sistem target.

Tujuan:

Mengidentifikasi informasi publik PT. KIMA MAKASSAR tanpa meninggalkan jejak atau *log* di sistem mereka.

B. Passive Reconnaissance (Pengintaian Pasif)

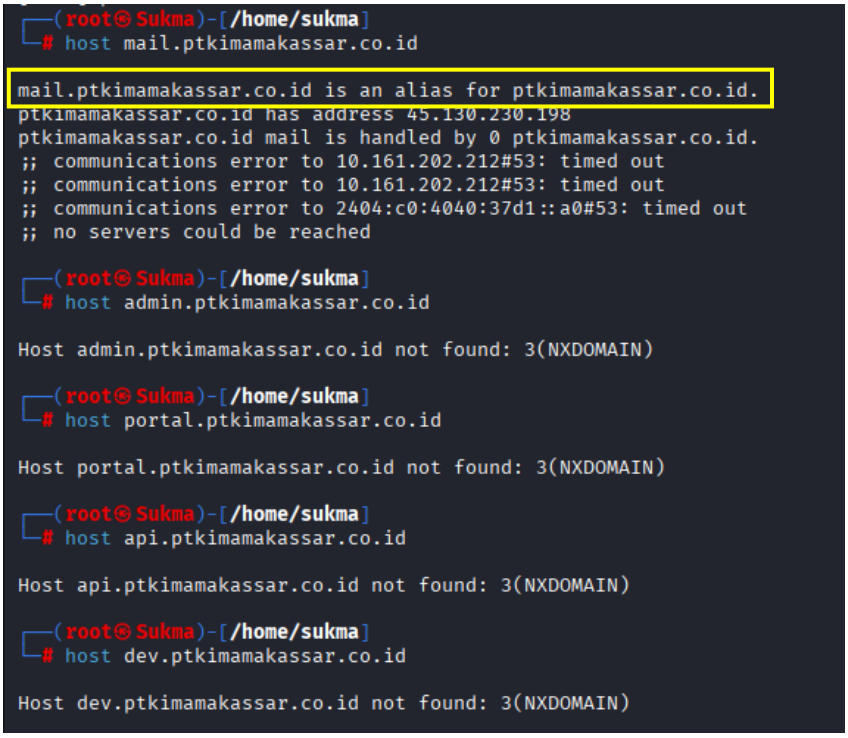
1. **kita akan masuk menggunakan firefox**

   Yang pertama kita akan mencari nama Perusahaan yang akan kita ambil sebagai bahan percobaan untuk tugas ini, kita akan masuk menggunakan firefox, lalu mencari di pencarian dengan google. Cari saja Perusahaan yang ada di makasssar sebenarnya tergantung target kita masing masing kita akan menggunakan Perusahaan, e-comerce, atau lainnya sesuai dengan arahan tugas. Disini saya langsung tertarik dengan PT. KIMA MAKASSAR jadi saya melakukan pencarian pasif dengan google dan juga virtualBox/kali linux. Saya sudah mengecek web resmi dari Perusahaan tersebut bahwasanya di sana sudah sangat lengkap sekali informasi nya dari segi Alamat. Untuk memastikan saya juga melakukan beberpa pencarian dengan virtual box.

2. **Pencarian domain dan sub-domain**

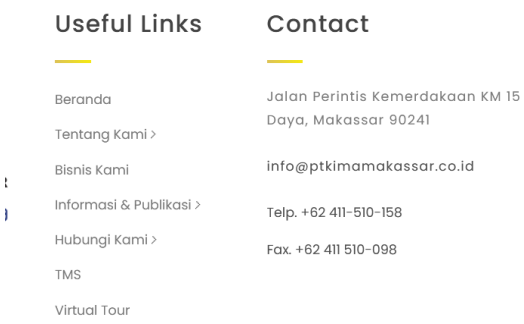
```
┌──(root㉿Sukma)-[/home/sukma]
└─# host -t mx ptkimamakassar.co.id

ptkimamakassar.co.id mail is handled by 0 ptkimamakassar.co.id.
```

   Ini Adalah email utama yang di gunakan pada PT.KIMAMAKASSAR.

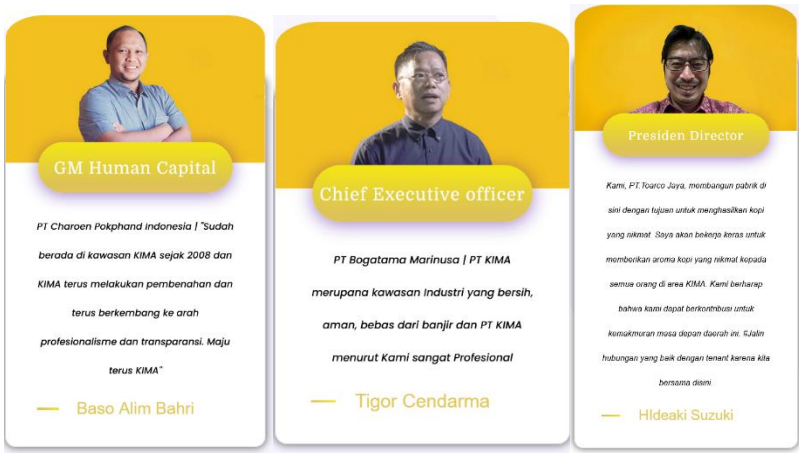


Ini Adalah sub domain satu-satunya yang aktif pada PT. KIMA MAKASSAR bisa di lihat pada gambar di atas beberapa kode dari hasil OSINT dan pemeriksaan DNS menggunakan perintah host saya coba untuk mencari sub-domain lain tetapi hasilnya not found.

3. Informasi email dan karyawan

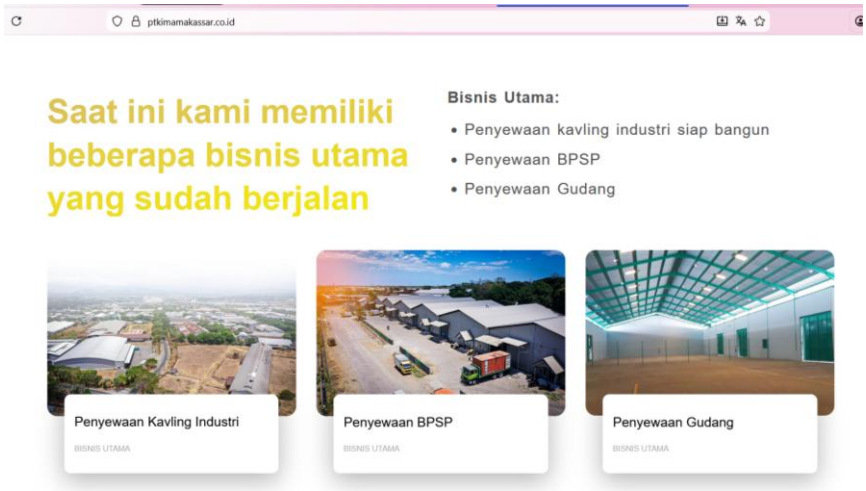


Ini merupakan format email yang yang di gunakan pada PT. KIMA MAKASSAR berdasarkan web yang ada pada Perusahaan tersebut.

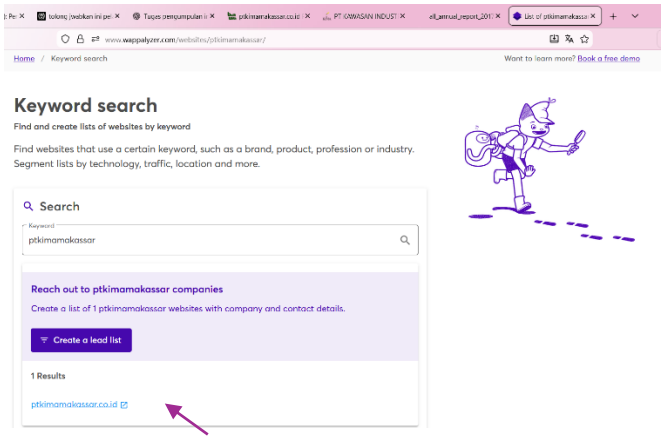


Ini merupakan karyawan penting dalam Perusahaan, saya mencari ke tiga karyawan ini langsung di dalam web resmi Perusahaan menggunakan google, (https://ptkimamakassar.co.id/) ini link resmi persuhaan tersebut.

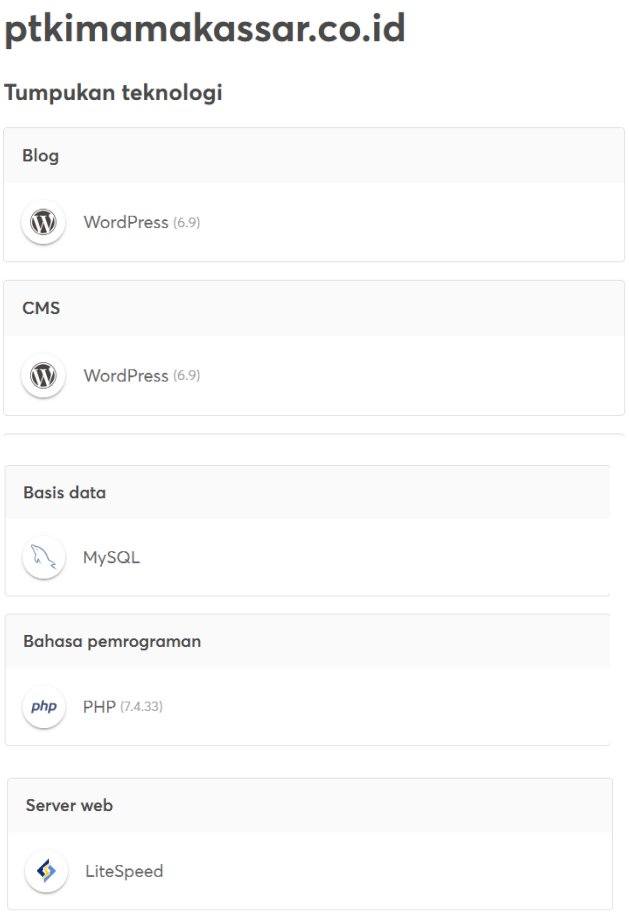
4. Teknologi yang digunakan



Ini merupakan website resmi PT. KIMA MAKASSAR saya mengunakan firefox untuk membuka websitie ini



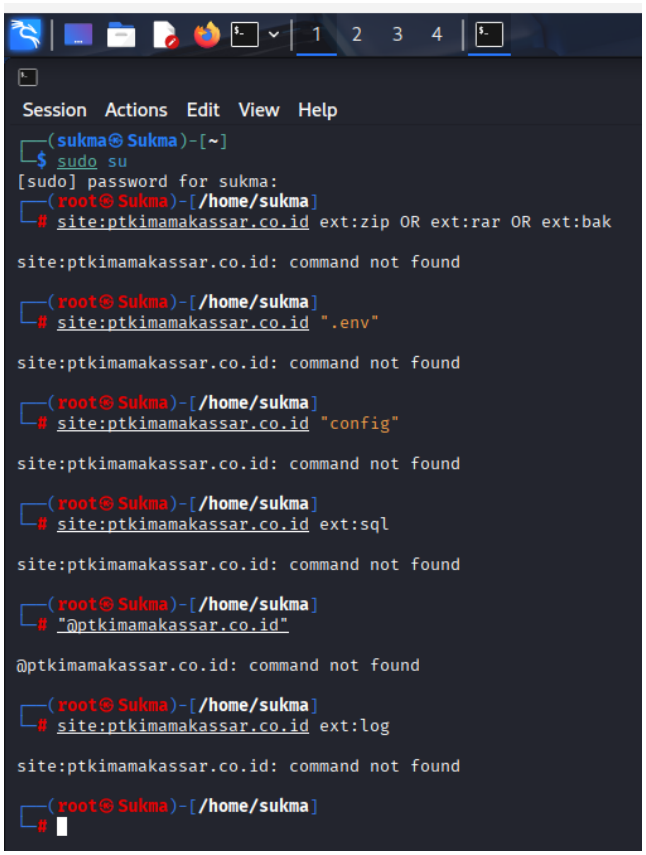
Disini saya menggunakan alat OSINT Wappalyzer bisa di lihat langsug pada gambar di atas ini. Langsung saja ketik PT. KIMA MAKASSAR lalu cari, lalu tekan result yang tulisan biru itu.



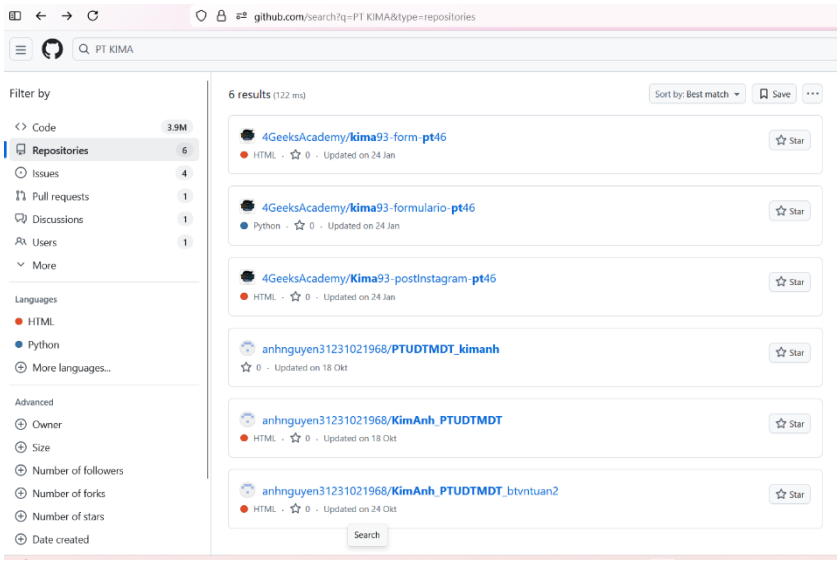
Ini salah satu tampilan yang ada pada wappalyzer, langsung ke penjelasan saja

- **Blog: WordPress 6.9** Menunjukkan fitur blog di situs tersebut dibangun dengan CMS WordPress versi 6.9; ini berarti ada modul blogging dan panel admin WordPress di backend
- **CMS: WordPress 6.9** Berarti seluruh konten utama website (halaman, posting, menu) dikelola oleh WordPress sebagai Content Management System, sehingga struktur folder dan endpoint WordPress (wp-admin, wp-content, dll.) kemungkinan ada dan bisa jadi target recon
- **Basis data: MySQL** Data website (artikel, user, konfigurasi) disimpan di database MySQL; bagi penyerang, informasi ini penting untuk mencari celah di koneksi PHP–MySQL atau backup database yang mungkin bocor
- **Bahasa pemrograman: PHP (7.4.33)** Script sisi server ditulis dengan PHP versi 7.4.33; versi PHP yang sudah mendekati end-of-life bisa memiliki banyak CVE, sehingga versi detail ini sangat berguna untuk analisis kerentanan.
- **Server web: LiteSpeed** HTTP server yang melayani request ke situs adalah LiteSpeed, bukan Apache/NGINX; ini mempengaruhi cara konfigurasi, modul keamanan (seperti mod_security), dan potensi misconfig yang dapat dieksploitasi.

5. **Informasi sensitif yang terpapar**



Pada gambar di atas bisa dilihat sendiri tidak ada sama sekali keobocoran data yang di timbulkan oleh Perusahaan tersebut.



Pada saat saya mencari di github tampil beberapa kode yang ada di sini namun setelah saya buka satu per satu tidak ada isi tentang kebocoran data atau apapun itu. Isi dalam file pencarian ini hanya menampilkan kode program saja.

Table output passive

Informasi yang ditemukan	**Alat/website**	**Alasan relevensi**
Web browser	Forefox	Saya sudah biasa mengunakan ini dan juga ada banyak sekali tools yang sudah saya simpan di browser ini.
Domain utama dan subdomain PT KIMA Makassar	Pencarian DNS, perintah host	Mengetahui domain & subdomain membantu mengidentifikasi permukaan serangan (attack surface) dan layanan apa saja yang terekspos publik.
Email utama perusahaan	Website resmi PT KIMA Makassar	Email publik sering menjadi titik awal serangan seperti phishing, social engineering, atau enumerasi akun.

Daftar karyawan penting	Website resmi PT KIMA Makassar	Informasi struktur organisasi relevan untuk memprediksi target potensial dalam serangan sosial atau rekayasa sosial (CEO Fraud, whaling attack).
Domain utama dan subdomain PT KIMA Makassar	Linux: host, dig	Alat DNS di Linux memudahkan mengidentifikasi domain/subdomain aktif untuk memetakan attack surface awal.
Bahasa, cms, database, server yang di temukan dalam web resmi perusahaan	Wappalyzer	Informasi server membantu menganalisis konfigurasi keamanan dan modul proteksi.

C. Active Reconnaissance (Pengintaian Aktif)

Active Recon adalah tahap pengumpulan informasi yang melibatkan interaksi langsung dengan sistem target.

Tujuan

Memetakan topologi jaringan dan mengidentifikasi layanan/port yang terbuka pada target secara terstruktur.

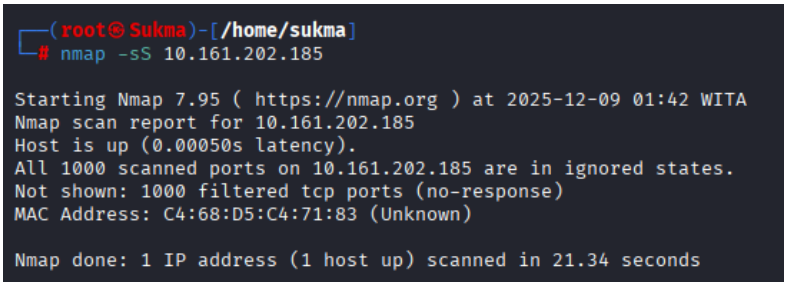
Peringatan Etis

● *Asumsi:* Anda telah mendapatkan **izin tertulis (Rules of Engagement)** untuk melakukan pemindaian pada alamat IP target spesifik (Asumsikan IP target adalah: **192.168.1.100**).

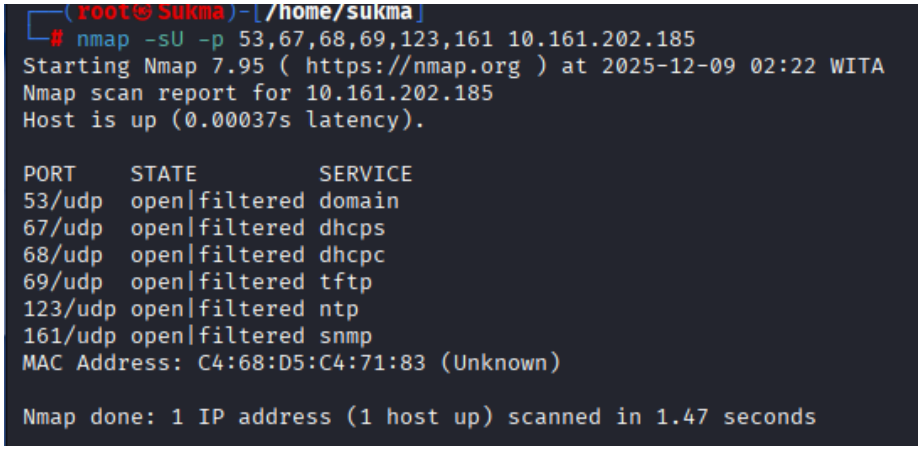
● Anda hanya boleh melakukan pemindaian pada IP yang ditentukan dalam skenario ini.

Tugas yang harus dilakukan

1. **Host Discovery dan Port Scanning:**



Jalankan pemindaian SYN Scan (-sS) untuk mengidentifikasi semua port TCP yang terbuka (open ports). Hasil scan menunjukkan bahwa host terdeteksi aktif (Host is up) dengan latensi sangat rendah, namun seluruh 1000 port TCP yang dipindai berada dalam keadaan filtered (no-response), sehingga tidak ada satu pun port yang teridentifikasi sebagai open maupun closed



Jalankan pemindaian **UDP Scan** (-sU) untuk mencari setidaknya **satu (1) port UDP** yang terbuka atau tersaring (*filtered*). Pemindaian UDP terarah dilakukan ke port 53, 67, 68, 69, 123, dan 161 pada IP 10.161.202.185. Hasilnya, keenam port tersebut berada pada status open|filtered dengan layanan yang terdeteksi masing-masing adalah DNS (53/udp), DHCP server (67/udp), DHCP client (68/udp), TFTP (69/udp), NTP (123/udp), dan SNMP (161/udp). Status open|filtered menunjukkan bahwa port-port ini tidak merespons sebagai

‘closed’, namun kemungkinan dilindungi oleh firewall sehingga responnya tidak dapat dibedakan secara pasti

2. **Service and Version Detection:**

```
┌──(root㉿Sukma)-[/home/sukma]
└─# nmap -sV 10.161.202.185

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 02:27 WITA
Nmap scan report for 10.161.202.185
Host is up (0.00064s latency).
All 1000 scanned ports on 10.161.202.185 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: C4:68:D5:C4:71:83 (Unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.58 seconds
```

Setelah mengidentifikasi bahwa seluruh port TCP pada IP 10.161.202.185 berada dalam kondisi ter-filter, dilakukan pemindaian service dan versi menggunakan perintah nmap -sV 10.161.202.185. Hasil scan menunjukkan bahwa Nmap tidak dapat mengidentifikasi layanan maupun versi perangkat lunak apa pun, karena seluruh 1000 port TCP yang diperiksa berada pada status filtered (no-response) dan tidak ada port dengan status open. Hal ini mengindikasikan bahwa firewall pada host atau jaringan menutup seluruh akses TCP dari luar, sehingga teknik service/version detection tidak menghasilkan informasi spesifik seperti contoh Apache HTTPD 2.4.41 pada soal.

3. **Os finger print**

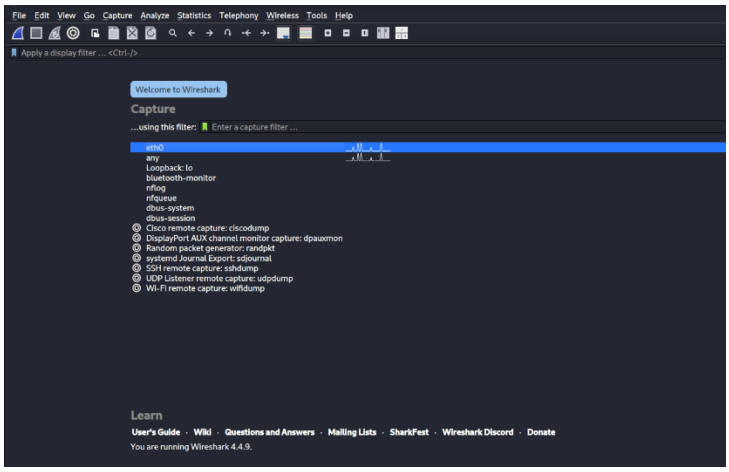
```
┌──(root㉿Sukma)-[/home/sukma]
└─# nmap -O 10.161.202.185

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 01:33 WITA
Nmap scan report for 10.161.202.185
Host is up (0.00044s latency).
All 1000 scanned ports on 10.161.202.185 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: C4:68:D5:C4:71:83 (Unknown)
Too many fingerprints match this host to give specific OS details
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.91 seconds
```

OS fingerprinting dilakukan dengan perintah nmap -O 10.161.202.185. Hasil scan menunjukkan bahwa seluruh port TCP berada pada status filtered sehingga tidak tersedia kombinasi port open/closed yang cukup untuk fingerprinting.

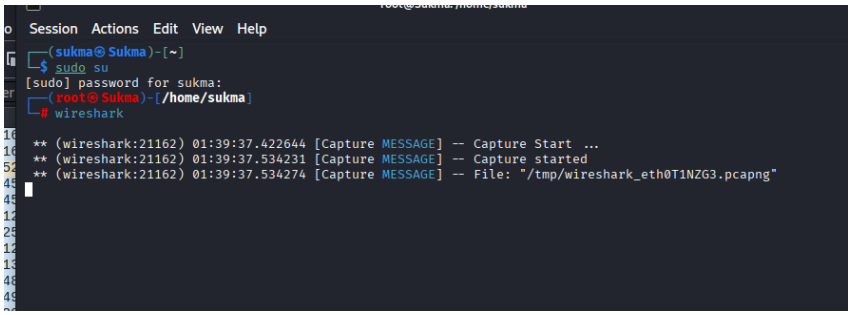
Nmap menampilkan pesan ‘Too many fingerprints match this host to give specific OS details’ dan tidak memberikan estimasi OS yang spesifik, sehingga sistem operasi target tidak dapat diidentifikasi hanya dari respon jaringan ini.

4. **Network protocol analysis**

- Masuk ke dalam wireshrak

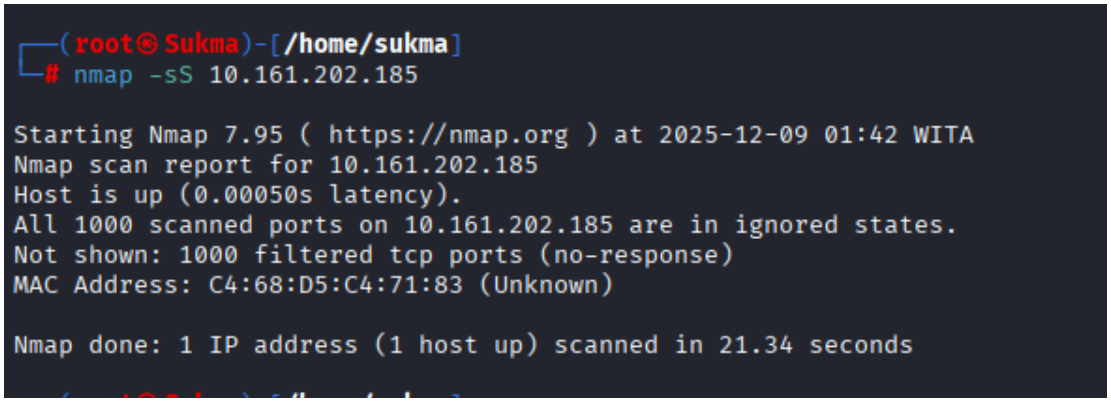


Bisa dilihat pada gambar setelah ini kita akan tekan etho untuk menjalankan nya.

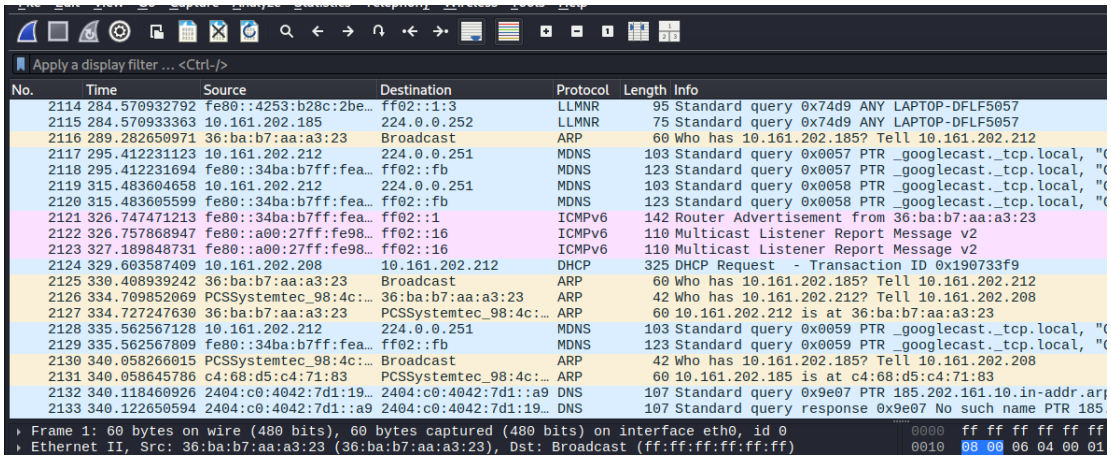


Di jendela Wireshark, pilih **eth0** dan tekan Start → Wireshark mulai menyimpan semua paket ke file pcap yang disebut di terminal. Sambil capture berjalan, kamu jalankan perintah Nmap ke target; paket-paket Nmap itu akan terekam di file capture.

- **Jalankan Nmap saat tcpdump merekam**



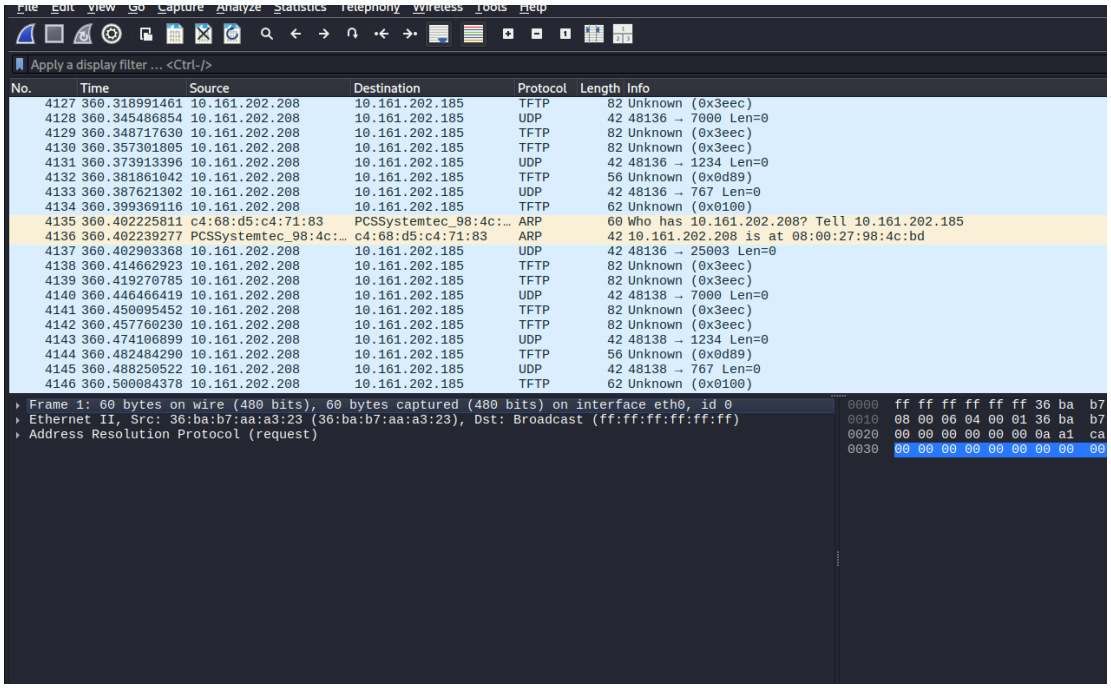
Ada banyak paket **TCP dengan flag SYN** dari 10.161.202.208 ke 10.161.202.185, yang berasal dari perintah Nmap (-sS SYN scan). Ini menunjukkan Nmap mengirim SYN ke berbagai port untuk melihat mana yang merespons.**Mengecek isi file capture.pcap di terminal**



Terlihat juga paket **ARP** (Address Resolution Protocol) seperti “Who has 10.161.202.185? Tell 10.161.202.212”, yang artinya perangkat di jaringan sedang mencari MAC address untuk IP tersebut sebelum mengirim paket.

Ada paket **ICMPv6 Neighbor Solicitation/Advertisement**, yaitu mekanisme IPv6 untuk mencari tetangga di jaringan (mirip ARP di IPv4); ini muncul karena interface-mu juga punya alamat IPv6.

LLMNR/MDNS/DNS: paket query nama host dari Windows ke jaringan (misalnya mencari nama LAPTOP-... atau layanan _googlecast._tcp.local). Ini contoh protokol level aplikasi yang menggunakan UDP untuk resolusi nama di jaringan lokal.



Banyak paket **TFTP dan UDP** dari 10.161.202.208 ke 10.161.202.185; ini kemungkinan lalu lintas aplikasi atau efek dari scan yang kamu jalankan ke port UDP tertentu.

Ada paket **ARP** dengan info “Who has 10.161.202.208? Tell 10.161.202.185” dan balasan “10.161.202.208 is at 08:00:27:98:4c:bd”, yang artinya perangkat di jaringan sedang mencari dan menjawab **alamat MAC** untuk IP tersebut sebelum mengirim paket.

- **Output**

Command Nmap	**Hasil output (port, layanan, versi)**	**Potensi kerentanan / analisis**
`nmap -sS 10.161.202.185`	Host terdeteksi up, namun seluruh 1000 port TCP berada pada status `filtered (no-response)` sehingga tidak ada port TCP yang teridentifikasi sebagai open maupun closed.	Firewall host/jaringan menutup semua akses TCP dari luar. Dari sisi penyerang ini menyulitkan enumerasi service, tetapi jika konfigurasi firewall salah (misalnya hanya mengizinkan port tertentu dari IP tertentu) maka serangan bisa diarahkan ke jalur yang diizinkan tersebut.
`nmap -sU 10.161.202.185`	Host up, seluruh 1000 port UDP awal dilaporkan sebagai `open	filtered` tanpa respon yang jelas, sehingga tidak ada port UDP spesifik yang dapat dipastikan open.
`nmap -sU -p 53,67,68,69,123,161 10.161.202.185`	Beberapa port UDP penting menunjukkan status `open	filtered` dengan mapping layanan: 53/udp domain (DNS), 67/udp dhcps, 68/udp dhcpc, 69/udp tftp, 123/udp ntp, 161/udp snmp. Tidak ada versi software yang terdeteksi.
Wireshark (capture di eth0 saat scan)	Capture menunjukkan berbagai protokol: TCP SYN dari 10.161.202.208 (Kali) ke 10.161.202.185 (target), UDP (termasuk TFTP/NTP), ARP ("Who has 10.161.202.185 / 10.161.202.208?"), DHCP	Dari sisi analisis, paket TCP SYN dan UDP mengkonfirmasi aktivitas pemindaian port oleh Nmap; ARP menunjukkan proses resolusi alamat IP ke MAC sebelum pengiriman paket; DHCP dan DNS/MDNS/LLMNR menegaskan bahwa host bergantung pada layanan infrastruktur jaringan. Jika

	antara 10.161.202.208 dan 10.161.202.212 (gateway), serta DNS/MDNS/LLMNR query lokal.	protokol-protokol ini tidak diamankan (misalnya LLMNR/MDNS dibiarkan aktif di jaringan yang tidak dipercaya), penyerang dapat memanfaatkannya untuk serangan man-in-the-middle atau poisoning.