LAPORAN PENGUJIAN PENETRASI KOMPREHENSIF: ANALISIS PASSIVE (OSINT) DAN ACTIVE RECONNAISSANCE PADA INFRASTRUKTUR TARGET

UMMUL MU'MININ

105841117323

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

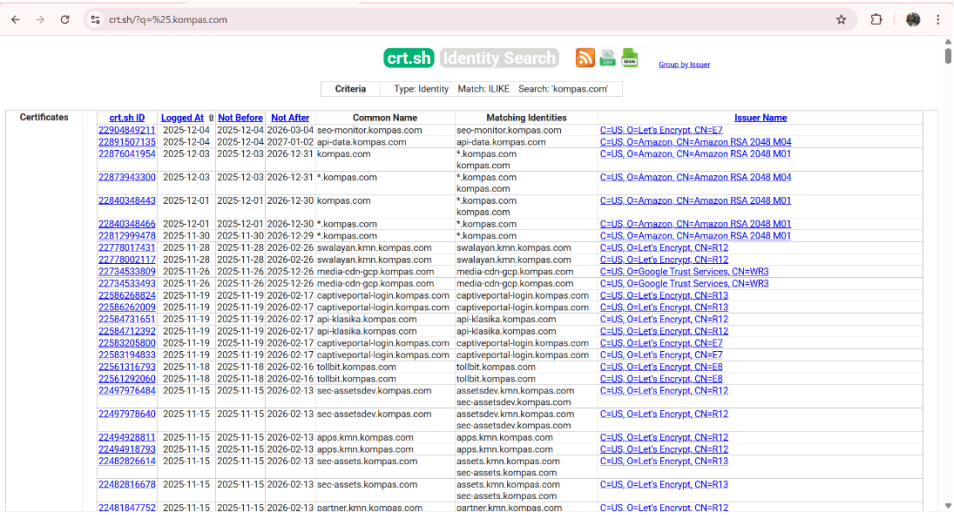
1. **Passive Reconnaissance**

   a. Mencari Domain

   Domain kompas.com telah dipilih sebagai target utama untuk pelaksanaan pengumpulan informasi publik (*Passive Reconnaissance*). Pemilihan ini didasarkan pada kebutuhan untuk mendemonstrasikan penerapan teknik *Open Source Intelligence* (OSINT) yang efektif pada sebuah entitas digital yang besar dan aktif.

   b. Pencarian Sub-domain

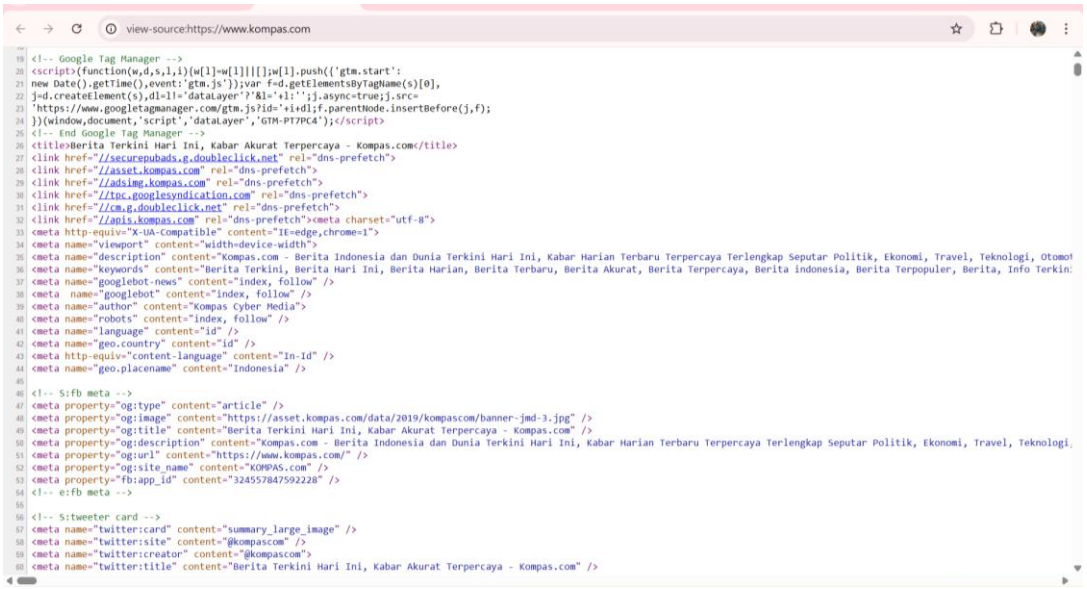
   Langkah awal dalam *Passive Reconnaissance* adalah mengidentifikasi aset digital tersembunyi target. Untuk tujuan ini, kami membuka *website* crt.sh. crt.sh berfungsi sebagai *Certificate Transparency Log*, sebuah *database* publik yang mencatat setiap sertifikat SSL/TLS yang diterbitkan untuk domain kompas.com. Tujuannya adalah untuk mencari sub-domain aktif yang mungkin tidak terdaftar secara publik di DNS. Berdasarkan hasil analisis, ditemukan beberapa sub-domain yang aktif dan relevan, di antaranya adalah seo-monitor.kompas.com, api-data.kompas.com, captiveportal-login.kompas.com, tolbit.kompas.com, dan sec-assetsdev.kompas.com.



   c. Identifikasi Teknologi dan Metadata (View Source Code)

   Pengumpulan informasi dilanjutkan dengan analisis kode sumber (View Source Code) dari halaman utama kompas.com. Analisis ini bertujuan untuk mengidentifikasi teknologi *front-end* yang digunakan. Hasilnya, ditemukan implementasi Google Tag Manager (GTM) dan berbagai *tag* <meta>. Penggunaan GTM ini mengindikasikan target bergantung pada *third-party scripts*, yang dapat membuka vektor Supply Chain Attack jika sistem pihak ketiga tersebut disusupi. Selain itu, metadata yang terekspos,

termasuk ID Aplikasi Facebook (fb:app_id), dapat digunakan untuk membuat serangan *social engineering* yang lebih kredibel.



d. Analisis Otomatis Menggunakan Wappalyzer

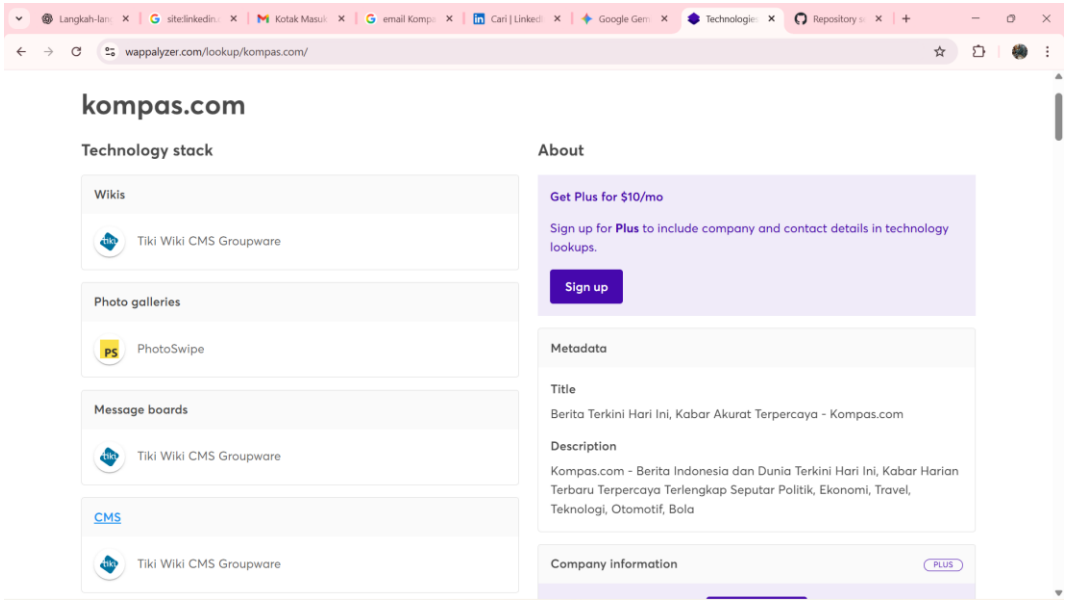
Untuk mengkonfirmasi dan memperluas temuan yang diperoleh secara manual, kami menggunakan alat otomatis Wappalyzer. Analisis ini memberikan gambaran lengkap mengenai tumpukan teknologi target. Di sisi infrastruktur, diidentifikasi penggunaan layanan *Platform as a Service* (PaaS) Amazon Web Services (AWS) dan Nginx yang berfungsi ganda sebagai *Reverse Proxy* dan *Web Server*. Untuk pengiriman konten, Wappalyzer mendeteksi penggunaan *Content Delivery Network* (CDN) Amazon CloudFront dan Cloudflare. Lebih lanjut, di sisi *front-end*, terdeteksi penggunaan bahasa pemrograman seperti Node.js dan PHP, serta *framework* Bootstrap dan *library* JQuery.

- Infrastruktur dan Layanan Back-End

  Pencarian otomatis menggunakan Wappalyzer mengkonfirmasi tumpukan teknologi inti target. Di sisi infrastruktur, diidentifikasi penggunaan layanan *Platform as a Service* (PaaS) dari Amazon Web Services (AWS). Selain itu, Nginx digunakan sebagai *Reverse Proxy* dan *Web Server*. Untuk pengiriman konten dan optimasi kecepatan, Wappalyzer mendeteksi penggunaan *Content Delivery Network* (CDN) Amazon CloudFront dan Cloudflare. Temuan ini penting karena mengidentifikasi komponen yang mungkin rentan terhadap *misconfiguration* atau eksploitasi pada layanan server.

- Bahasa Pemrograman dan Framework Front-End

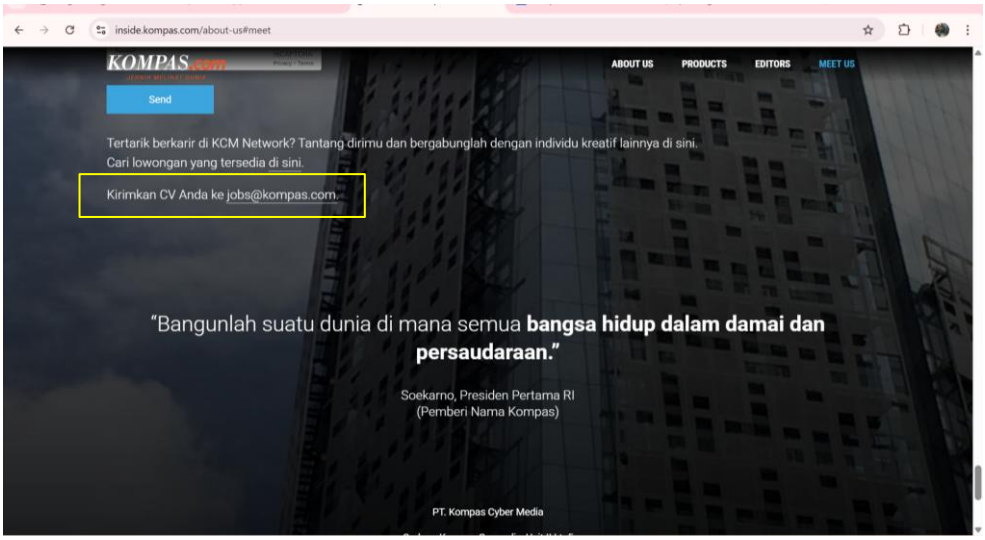
  Analisis Wappalyzer juga memberikan gambaran mengenai teknologi yang digunakan di sisi *front-end* dan pendukung. Ditemukan penggunaan bahasa pemrograman Node.js dan PHP sebagai dasar *scripting*. Selain itu, Wappalyzer mendeteksi penggunaan *framework* Bootstrap dan *library* JQuery. Informasi ini sangat berguna untuk fase pengujian kerentanan (*Vulnerability Assessment*), di mana *penetration tester* dapat mencari kerentanan yang spesifik pada versi *framework* dan bahasa pemrograman tersebut.

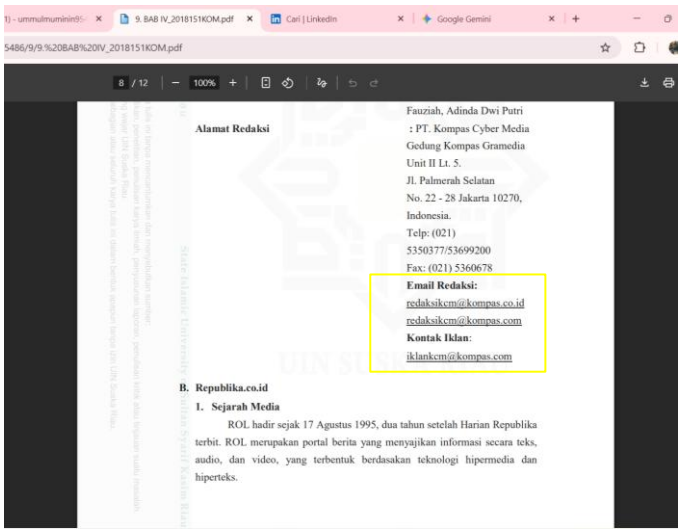


e. Informasi Email dan Karyawan

- Informasi Email

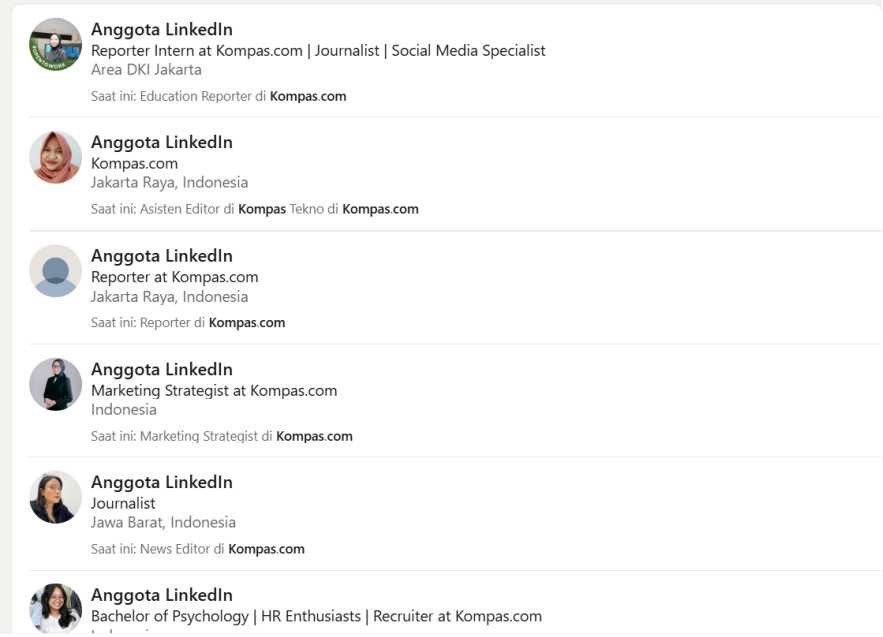
  Pengumpulan informasi dilanjutkan dengan mengidentifikasi alamat kontak penting. Dari halaman *About Us* kompas.com, ditemukan alamat kontak rekrutmen yaitu jobs@kompas.com. Selain itu, melalui penelusuran di repositori publik (laporan penelitian), ditemukan alamat email redaksi dan iklan, yaitu redaksikcm@kompas.com dan iklankcm@kompas.com. Temuan ini mengindikasikan bahwa format email standar perusahaan kemungkinan besar adalah [fungsi/posisi]@kompas.com atau [nama]@kompas.com. Informasi ini sangat penting karena format email yang tervalidasi dapat digunakan untuk melakukan serangan *phishing* yang ditargetkan (*spear-phishing*) atau *brute-force* kredensial *login*.





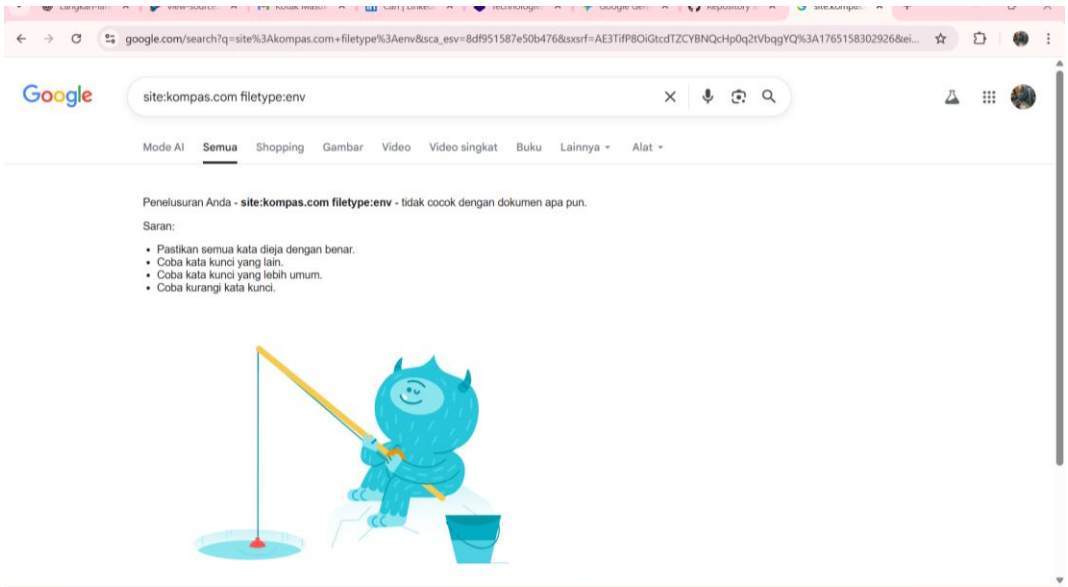
- Informasi Karyawan

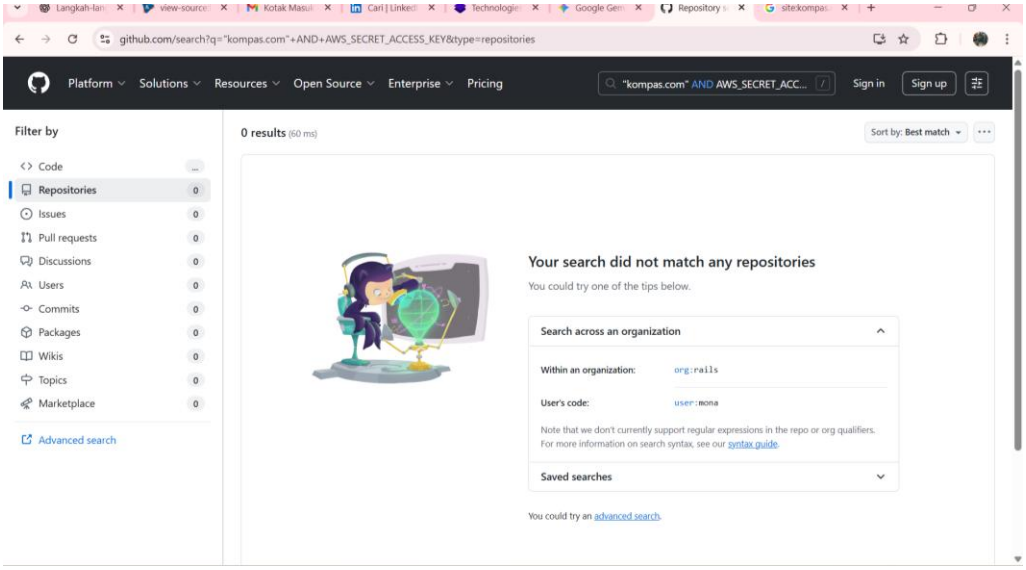
  Informasi yang dikumpulkan dari platform profesional (LinkedIn) juga mengkonfirmasi keberadaan dan posisi beberapa karyawan target. Karyawan yang teridentifikasi memiliki beragam peran, termasuk Reporter Intern, Asisten Editor di Kompas Tekno, dan Marketing Strategist. Penemuan nama dan jabatan karyawan ini sangat bernilai dalam *penetration test* karena memungkinkan penyerang untuk memilih target dengan *privilege* tertentu atau yang bekerja di divisi sensitif. Informasi ini akan digunakan untuk merancang pesan *phishing* yang kredibel dan sangat meyakinkan untuk mendapatkan akses awal ke dalam jaringan internal.



f. Informasi Sensitif yang Terpapar

Pencarian informasi sensitif yang terekspos dilakukan menggunakan teknik Google Dorking dan penelusuran platform repositori kode. Fokus utama pencarian diarahkan pada *file* konfigurasi yang terekspos seperti filetype:env, serta kredensial *hardcoded* seperti AWS_SECRET_ACCESS_KEY di GitHub. Setelah pencarian yang teliti, tidak ditemukan *file* atau *credential* internal yang langsung terekspos di domain publik. Hasil ini menunjukkan bahwa tim pengembangan target telah mengambil langkah yang tepat dalam mencegah paparan *file* konfigurasi kritikal ke mesin pencari dan repositori kode. Namun, upaya pencarian ini tetap krusial dalam fase *penetration testing* untuk memverifikasi integritas keamanan target.





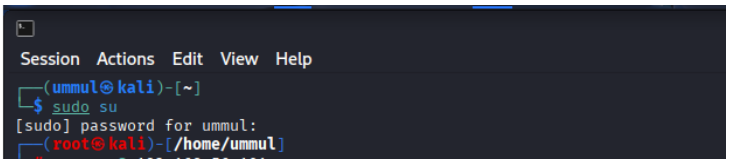
g. Tabel

Kategori	**Alat yang Digunakan**	**Temuan Kunci yang Teridentifikasi**
Aset Domain (Sub-domain)	crt.sh	Sub-domain yang mengindikasikan endpoint data: api-data.kompas.com. Sub-domain lingkungan development: sec-assetsdev.kompas.com.
Tumpukan Teknologi (CMS/Framework)	Wappalyzer	Penggunaan Tiki Wiki CMS Groupware untuk Wikis, Message Boards, dan CMS. Penggunaan PhotoSwipe untuk galeri fot.
Informasi Personalia	Pencarian Publik/Profesional	Format Email dan identifikasi peran karyawan (Asisten Editor, Reporter).
Eksposur Data Sensitif	Google Dorking	Tidak ditemukan file konfigurasi sensitif (.env, API keys) yang terekspos.

2. Active Reconnaissance

a. Persiapan Lingkungan dan Akses Root

Proses *Active Reconnaissance* dimulai dengan membuka terminal pada sistem operasi pengujian (Kali Linux atau sejenisnya). Untuk memastikan semua fungsi Nmap, terutama TCP SYN Scan (-sS), dapat berjalan dengan hak akses yang diperlukan, kami terlebih dahulu mengubah hak akses menjadi root. Akses *root* ini penting karena pemindaian *stealth* memerlukan manipulasi paket jaringan tingkat rendah yang hanya diizinkan oleh pengguna dengan hak administratif.

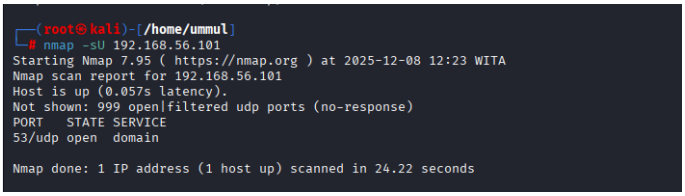


b. Pemindaian Port TCP dan Deteksi Perangkat (Menggunakan Nmap)

Setelah mendapatkan hak akses *root*, perintah Nmap dieksekusi pada target 192.168.56.101 (lingkungan VulnOS). TCP SYN Scan (-sS) dilakukan untuk mengidentifikasi layanan yang terbuka. Hasilnya menunjukkan bahwa 999 *port* TCP tertutup dan *host* dideteksi sebagai perangkat keamanan jaringan (*firewall/router*). Temuan ini mengindikasikan adanya filter jaringan yang sangat ketat pada target.

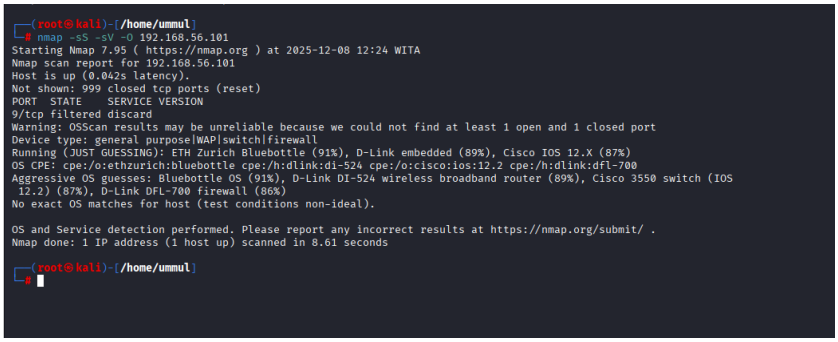
c. Pemindaian Port UDP (Menggunakan Nmap -sU)

Setelah menyelesaikan pemindaian TCP, kami melanjutkan pemindaian dengan fokus pada *port* UDP menggunakan perintah nmap -sU 192.168.56.101. Pemindaian UDP dilakukan karena layanan penting, seperti DNS, sering berjalan di protokol ini, dan pemindaian TCP tidak dapat mendeteksinya. Hasil pemindaian ini menunjukkan bahwa 999 *port* UDP tidak merespons, namun mengidentifikasi Port 53 (layanan domain) dalam status open|filtered. Temuan ini sangat penting karena Port 53 adalah satu-satunya titik interaksi yang terdeteksi, dan mengarahkan *penetration tester* untuk fokus pada potensi serangan *Zone Transfer* atau kerentanan lain pada layanan DNS tersebut.



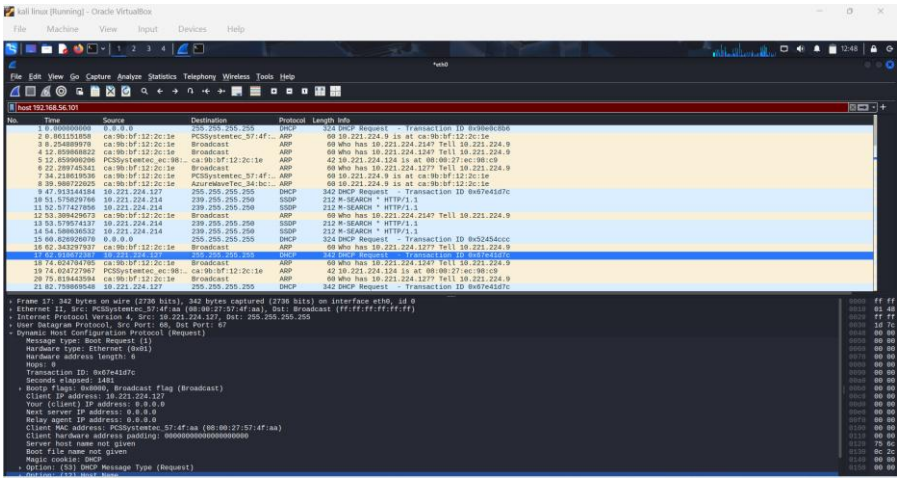
d. Pemindaian UDP dan Deteksi OS/Versi (Menggunakan Nmap Lanjutan)

Setelah pemindaian awal, pemindaian *stealth* TCP (disertai deteksi OS dan Versi) dieksekusi. Hasil pemindaian pada terminal menunjukkan bahwa *Host is up* (Host hidup), namun 999 closed tcp ports (reset) dilaporkan. Pada bagian deteksi OS, Nmap menebak bahwa *Device type* adalah general purpose | WAP | switch | firewall. Nmap melakukan *Aggressive OS guesses* dengan tingkat kepercayaan tinggi, yaitu ETH Zurich Bluebottle OS (91%), D-Link embedded (89%), dan Cisco IOS 12.x (87%).



e. Analisis Lalu Lintas Jaringan (Menggunakan Wireshark)

Secara paralel dengan pemindaian Nmap, aplikasi Wireshark dibuka untuk melakukan *packet capture* dan menganalisis lalu lintas jaringan secara langsung. Analisis ini mengkonfirmasi bahwa *host* target merespons upaya pemindaian Nmap dengan paket TCP dan ICMP. Kehadiran paket ICMP memvalidasi bahwa *host* target berada dalam status *live* (*host discovery*), sedangkan paket TCP yang dikirimkan oleh Nmap (SYN) dan respons yang terpotong mengkonfirmasi bahwa target memproses permintaan koneksi, meskipun akhirnya dibatasi oleh *firewall* yang aktif. Dengan demikian, Wireshark berhasil memvalidasi bahwa temuan Nmap berasal dari perangkat yang berfungsi, bukan dari *host* yang mati.


kali linux [Running] - Oracle VirtualBox
File Machine View Input Devices Help
eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
host 192.168.56.101
No. Time Source Destination Protocol Length Info
1 0.000000000 0.0.0.0 255.255.255.255 DHCP 324 DHCP Request - Transaction ID 0x90e0c8b6
2 0.861151858 ca:9b:bf:12:2c:1e PCSSystemtec_57:4f:.. ARP 60 10.221.224.9 is at ca:9b:bf:12:2c:1e
3 8.254889979 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.214? Tell 10.221.224.9
4 12.859068822 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.124? Tell 10.221.224.9
5 12.859900206 PCSSystemtec_ec:98:.. ca:9b:bf:12:2c:1e ARP 42 10.221.224.124 is at 08:00:27:ec:98:c9
6 22.289745341 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.127? Tell 10.221.224.9
7 34.218619536 ca:9b:bf:12:2c:1e PCSSystemtec_57:4f:.. ARP 60 10.221.224.9 is at ca:9b:bf:12:2c:1e
8 39.980722025 ca:9b:bf:12:2c:1e AzureWaveTec_34:bc:.. ARP 60 10.221.224.9 is at ca:9b:bf:12:2c:1e
9 47.913144184 10.221.224.127 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x67e41d7c
10 51.575829766 10.221.224.214 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
11 52.577427856 10.221.224.214 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
12 53.309429673 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.214? Tell 10.221.224.9
13 53.579574137 10.221.224.214 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
14 54.580635532 10.221.224.214 239.255.255.250 SSDP 212 M-SEARCH * HTTP/1.1
15 60.626926070 0.0.0.0 255.255.255.255 DHCP 324 DHCP Request - Transaction ID 0x52454ccc
16 62.343297937 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.127? Tell 10.221.224.9
17 62.910671261 10.221.224.127 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x67e41d7c
18 74.024704705 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.124? Tell 10.221.224.9
19 74.024727967 PCSSystemtec_ec:98:.. ca:9b:bf:12:2c:1e ARP 42 10.221.224.124 is at 08:00:27:ec:98:c9
20 75.819443594 ca:9b:bf:12:2c:1e Broadcast ARP 60 Who has 10.221.224.127? Tell 10.221.224.9
21 82.759869548 10.221.224.127 255.255.255.255 DHCP 342 DHCP Request - Transaction ID 0x67e41d7c
Frame 17: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface eth0, id 0
Ethernet II, Src: PCSSystemtec_57:4f:aa (08:00:27:57:4f:aa), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Internet Protocol Version 4, Src: 10.221.224.127, Dst: 255.255.255.255
User Datagram Protocol, Src Port: 68, Dst Port: 67
Dynamic Host Configuration Protocol (Request)
Message type: Boot Request (1)
Hardware type: Ethernet (0x01)
Hardware address length: 6
Hops: 0
Transaction ID: 0x67e41d7c
Seconds elapsed: 1481
Bootp flags: 0x0000, Broadcast flag (Broadcast)
Client IP address: 10.221.224.127
Your (client) IP address: 0.0.0.0
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: PCSSystemtec_57:4f:aa (08:00:27:57:4f:aa)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (Request)
Option: (12) Host Name