LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

NAMA : NUR SYAFITRI ANA

NIM : 105841102523

KELAS : JK-5B ETHICAL HACKING

SKENARIO

Pada Tanggal 7 Desember 2025, saya melaksanakan asesmen keamanan untuk membandingkan postur keamanan antara infrastruktur dunia nyata dan lingkungan laboratorium. Target pertama adalah website publik PT Djarum (djarum.com), di mana saya menerapkan metode *Passive Reconnaissance* secara ketat guna mematuhi etika keamanan siber tanpa mengganggu layanan kritikal. Pengumpulan informasi dilakukan tanpa interaksi langsung dengan server, melainkan memanfaatkan sumber data terbuka (OSINT) seperti inspeksi header HTTP via peramban, penggunaan ekstensi Wappalyzer untuk mendeteksi teknologi web, serta layanan Whois Lookup untuk memetakan arsitektur sistem dari sisi eksternal.

Sebaliknya, terhadap target kedua yaitu mesin rentan VulnOS yang berjalan di lingkungan virtual tertutup (*sandbox*), saya menerapkan pendekatan *Active Reconnaissance* secara menyeluruh. Proses ini melibatkan penggunaan alat teknis secara langsung, dimulai dengan *Netdiscover* untuk menemukan IP target, dilanjutkan dengan *Nmap* untuk memindai port TCP/UDP serta mendeteksi versi layanan dan sistem operasi, hingga penggunaan *Wireshark* untuk menganalisis paket jaringan seperti *Three-Way Handshake*. Hasil dari pendekatan aktif ini memberikan gambaran teknis mendalam mengenai kerentanan sistem yang siap dieksploitasi, melengkapi profil risiko yang telah disusun dari target sebelumnya.

1. PENDAHULUAN

Dalam era transformasi digital saat ini, keamanan infrastruktur teknologi informasi menjadi aspek krusial bagi keberlangsungan operasional organisasi, baik di sektor publik maupun privat. Ancaman siber yang terus berevolusi menuntut praktisi keamanan untuk tidak hanya memahami cara bertahan, tetapi juga memahami perspektif penyerang (*attacker's perspective*). Salah satu tahapan paling fundamental dalam siklus serangan siber (*Cyber Kill Chain*) adalah *Reconnaissance* atau pengumpulan informasi. Tahap ini menentukan seberapa efektif serangan lanjutan dapat dilakukan berdasarkan pemetaan permukaan serangan (*attack surface*) yang akurat.

2. TUJUAN KEGIATAN

Adapun tujuan spesifik dari pelaksanaan tugas besar ini adalah sebagai berikut:

a. Menerapkan Metodologi Information Gathering secara Komprehensif Mempraktikkan teknik pengumpulan informasi dengan dua pendekatan berbeda: Passive Reconnaissance (OSINT) untuk target infrastruktur publik dan Active Reconnaissance

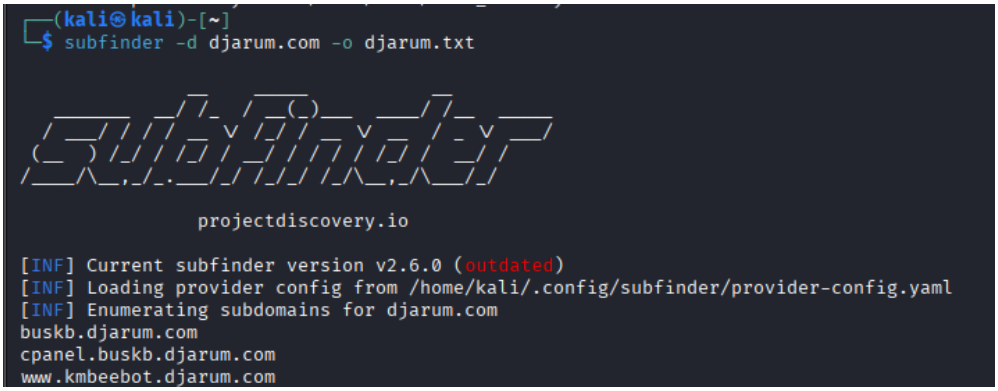
untuk target laboratorium, guna memahami perbedaan karakteristik dan risiko keduanya.

b. Memetakan Permukaan Serangan (Attack Surface Analysis) Mengidentifikasi titik-titik potensial yang dapat dieksploitasi pada target VulnOSv2 melalui penemuan alamat IP, pemindaian port terbuka (TCP/UDP), deteksi versi layanan (Service Versioning), serta identifikasi sistem operasi (OS Fingerprinting).

c. Menganalisis Protokol Komunikasi Jaringan Melakukan analisis paket data (packet capture) menggunakan Wireshark untuk memahami mekanisme teknis di balik proses pemindaian, termasuk identifikasi protokol ARP dan proses Three-Way Handshake pada protokol TCP.

a. Bukti/Dokumentasi

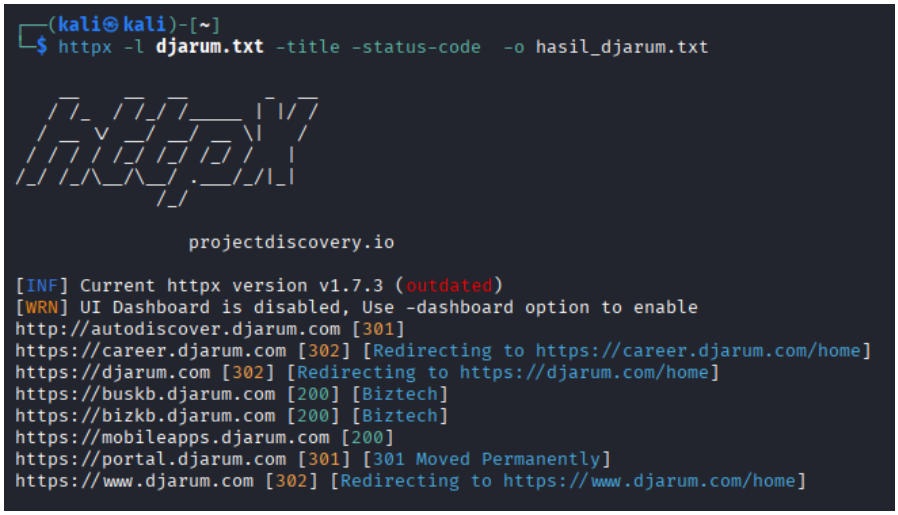
1. Mencari Sub Domain



Gambar 1.1 hasil pencarian di Subfinder

Melakukan Pencarian Sub domain Dari Kai.id menggunakan Tools Subfinder.

2. Mencari Domain Yang Aktif



Gambar 1.2

Melakukan Pencarian Subdomain Yang aktif menggunkan Tools HTTPX

3. DNS Record Public

- A RECORD (IP ADDREST)

```
┌──(kali㉿kali)-[~]
└─$ dig djarum.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> djarum.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 47235
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;djarum.com.                    IN      A

;; ANSWER SECTION:
djarum.com.             13005   IN      A       103.29.149.144

;; Query time: 96 msec
;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
;; WHEN: Tue Dec 09 09:37:24 EST 2025
;; MSG SIZE  rcvd: 55
```

Gambar 1.3

- MX RECORD (MAIL EXCHANGE)

```
┌──(kali㉿kali)-[~]
└─$ dig djarum.com mx

; <<>> DiG 9.20.11-4+b1-Debian <<>> djarum.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22520
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;djarum.com.                    IN      MX

;; ANSWER SECTION:
djarum.com.             28800   IN      MX      0 djarum-com.mail.protection.outlook.com.

;; Query time: 120 msec
;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
;; WHEN: Tue Dec 09 09:37:55 EST 2025
;; MSG SIZE  rcvd: 90
```

Gambar 1.4

- NS RECORD (NAMESERVER)

```
┌──(kali㉿kali)-[~]
└─$ dig djarum.com mx

; <<>> DiG 9.20.11-4+b1-Debian <<>> djarum.com mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 22520
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
;; QUESTION SECTION:
;djarum.com.                    IN      MX

;; ANSWER SECTION:
djarum.com.             28800   IN      MX      0 djarum-com.mail.protection.outlook.com.

;; Query time: 120 msec
;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
;; WHEN: Tue Dec 09 09:37:55 EST 2025
;; MSG SIZE  rcvd: 90
```

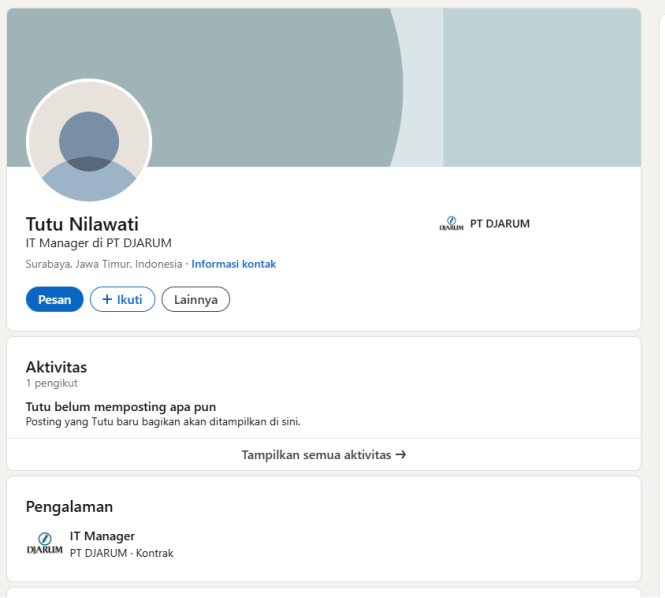
Gambar 1.5

- TXT RECORD

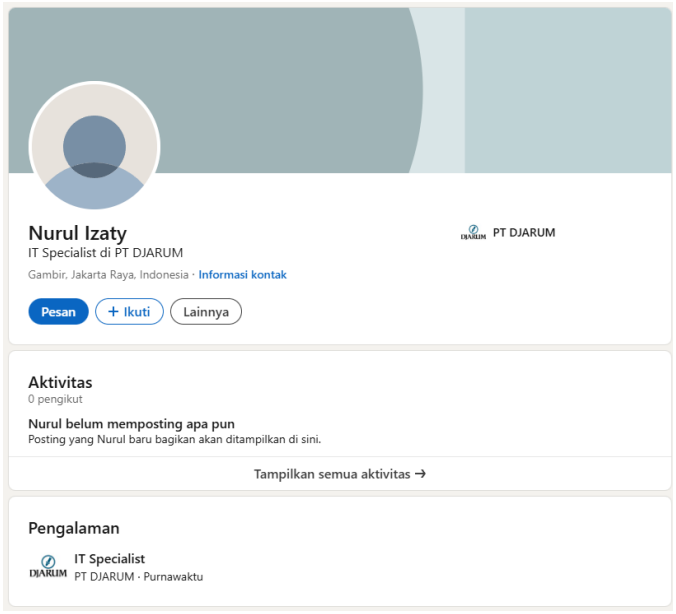
```
┌──(kali㉿kali)-[~]
└─$ dig djarum.com txt
;; communications error to 192.168.43.1#53: timed out
;; communications error to 192.168.43.1#53: timed out
;; communications error to 192.168.43.1#53: timed out

; <<>> DiG 9.20.11-4+b1-Debian <<>> djarum.com txt
;; global options: +cmd
;; no servers could be reached
```

Gambar 1.6

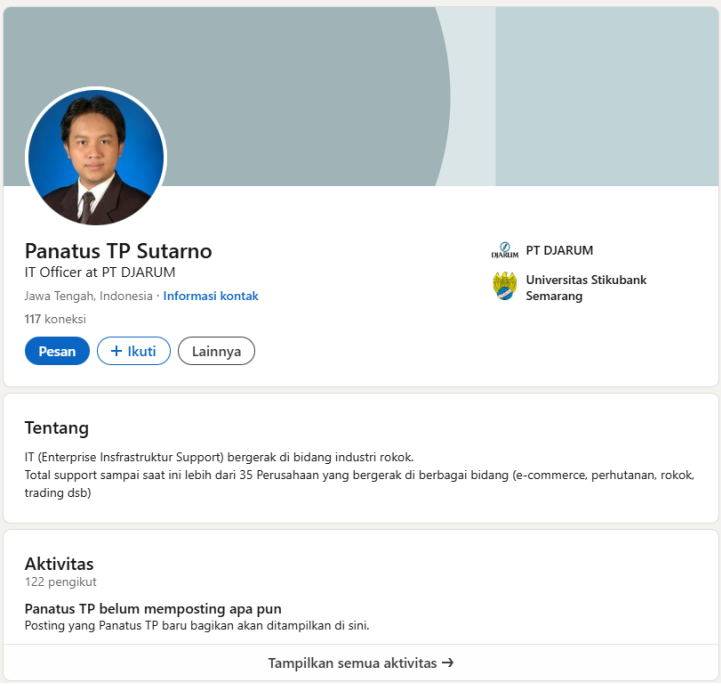
4. Profil Karyawan IT Di Linkedin



Gambar 1.7

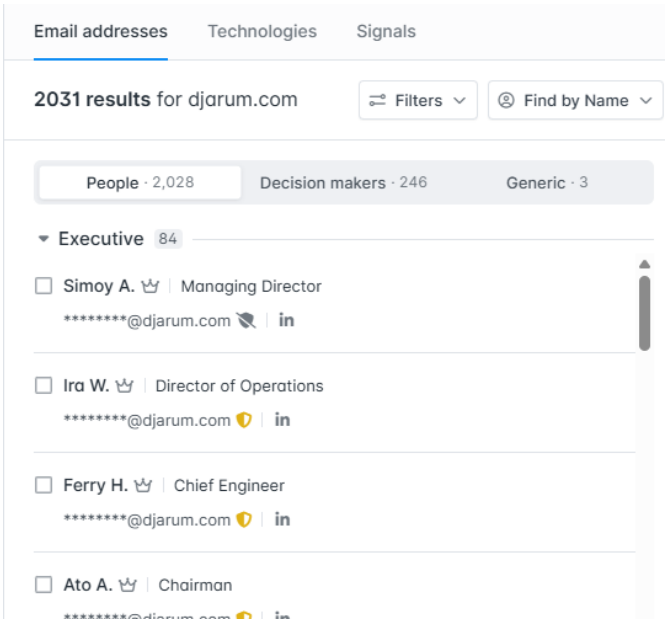


Gambar 1.8



Gambar 1.9

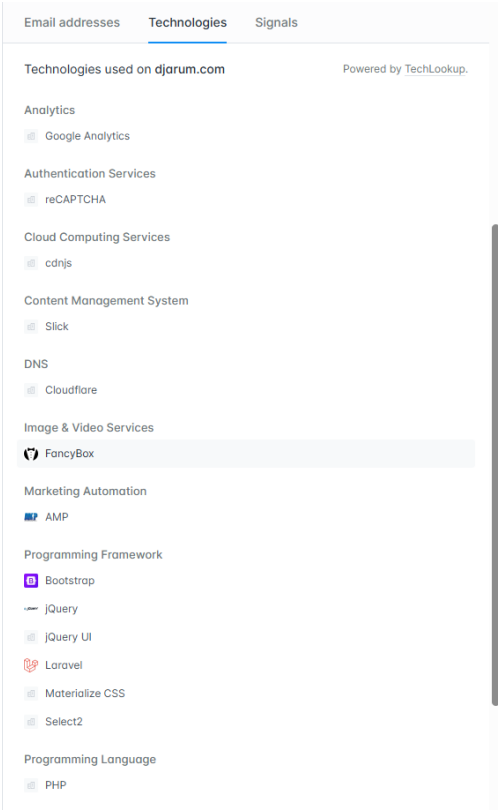
5. Domain/Format Email Perusahaan



Gambar 1.10

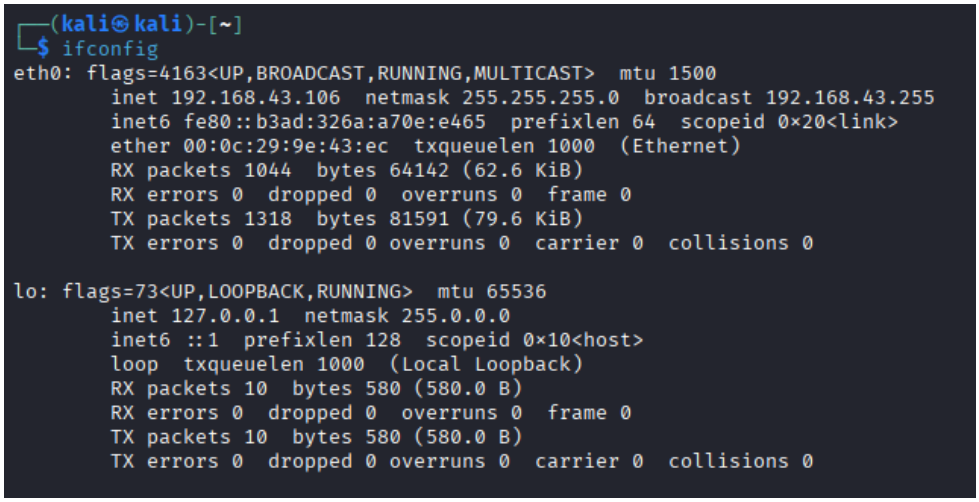
Mencari Format Email yang di gunakan Yaitu @djarum.com, Pencarian Menggunakan Hunter.iO

6. Teknologi yang di Gunakan



Gambar 1.11

4. ACTIVE RECONNAISSANCE

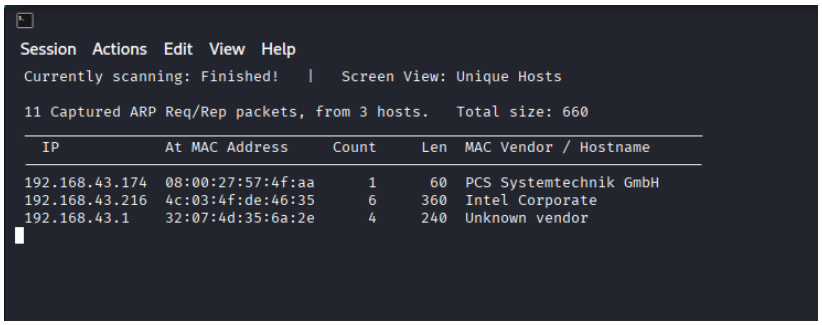


gambar 4.1

Sebelum melakukan pemindaian aktif, verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah ifconfig, di mana interface eth0 teridentifikasi memiliki alamat IP 172.20.10.2 dengan netmask 255.255.255.240 (Gambar [Nomor]). Konfigurasi ini mengonfirmasi bahwa penyerang berada dalam satu segmen jaringan (subnet) yang sama dengan target 172.20.10.3, memvalidasi skenario Internal Network Attack melalui konektivitas Layer 2 (Data Link) yang memungkinkan efektivitas teknik ARP Scanning serta memastikan paket probe Nmap dapat mencapai target tanpa terhalang oleh Network Firewall atau router eksternal."

1. Dokumentasi

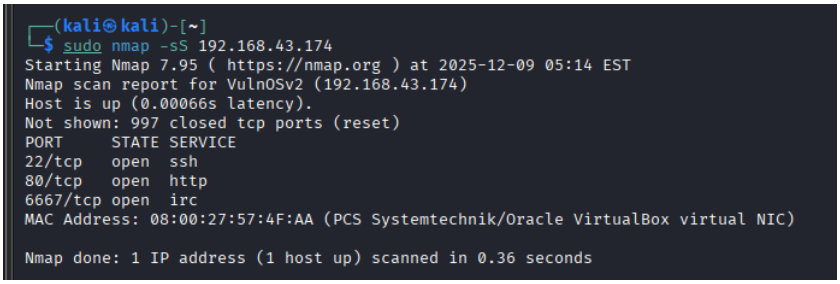
- NETDISCOVER



Gambar 4.2

Memindai ip dari VulnOS atau Target Kita, Yaitu 192.168.43.174 dan mac nya PCS Systemtechnik GmbH

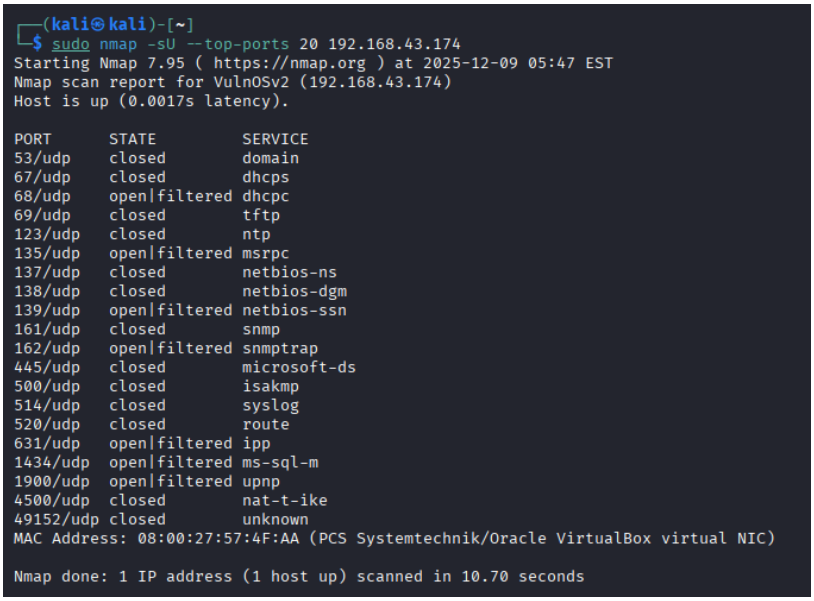
- SCAN PORT TCP



Gambar 4.3

Menemukan port TCP terbuka (22, 80, 6667) tanpa menyelesaikan 3-way handshake

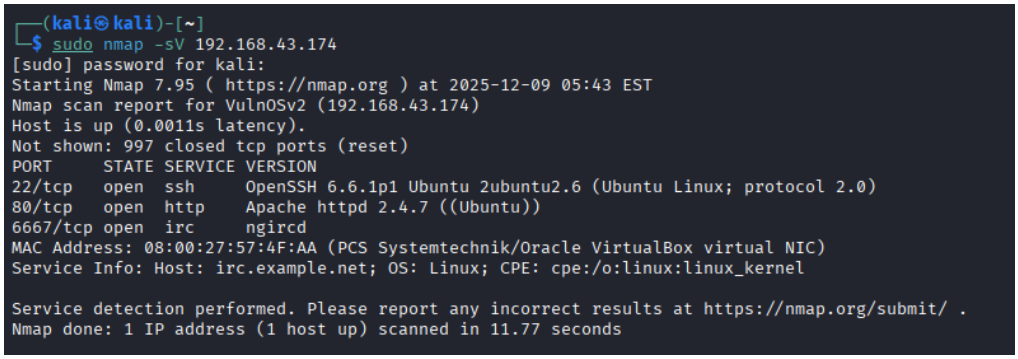
- SCAN PORT UDP



Gambar 4.4

Identifikasi layanan berbasis UDP seperti DNS (53) dan DHCP (67) yang berstatus open/filtered

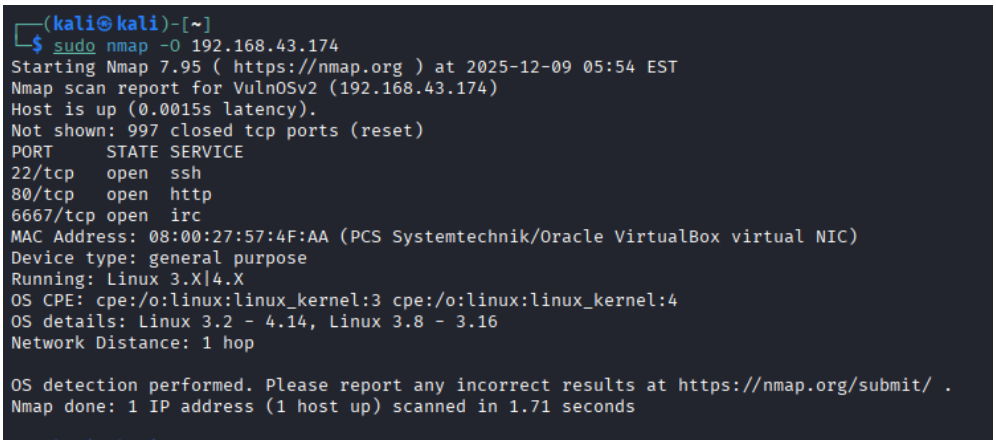
2. Service and Version Detection



Gambar 4.5

Gambar tersebut menampilkan hasil eksekusi perintah `nmap` dengan parameter `-sV` yang ditujukan ke alamat IP 192.168.43.174 untuk melakukan enumerasi versi layanan pada target yang teridentifikasi sebagai VulnOSv2. Hasil pemindaian menunjukkan bahwa host target dalam keadaan aktif dan memiliki tiga port TCP yang terbuka, yaitu port 22 untuk layanan SSH dengan versi OpenSSH 6.6.1p1, port 80 untuk layanan web (HTTP) yang menggunakan Apache 2.4.7, serta port 6667 untuk layanan IRC menggunakan ngircd. Informasi detail mengenai versi perangkat lunak ini sangat krusial dalam tahap *Information Gathering* karena memberikan data spesifik yang diperlukan untuk mencari kerentanan (CVE) yang mungkin ada pada versi aplikasi tersebut, sekaligus memvalidasi bahwa target berjalan di atas platform virtualisasi Oracle VirtualBox berdasarkan identifikasi alamat MAC-nya.

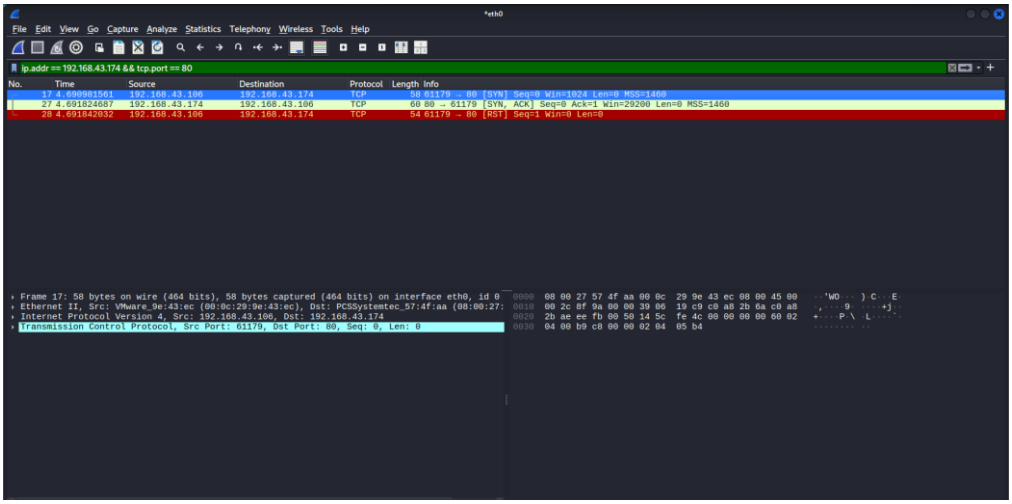
3. OS Fingerprinting



Gambar 3.1

hasil pemindaian jaringan menggunakan Nmap terhadap target dengan alamat IP 192.168.43.174 (teridentifikasi sebagai VulnOSv2), di mana perintah `sudo nmap -O` digunakan secara spesifik untuk mendeteksi sistem operasi yang berjalan pada target tersebut. Hasil pemindaian menunjukkan bahwa host tersebut dalam keadaan aktif dan memiliki tiga port terbuka, yaitu port 22 untuk layanan SSH, port 80 untuk web server (HTTP), dan port 6667 untuk IRC, sementara deteksi OS menyimpulkan bahwa target menggunakan sistem operasi Linux dengan kernel versi antara 3.2 hingga 4.14 dan berjalan di lingkungan virtualisasi VirtualBox.

4. WIRESHARK



Gambar 4.1

Tangkapan layar Wireshark tersebut memvisualisasikan mekanisme teknis dari teknik *TCP SYN Scan* (atau *half-open scanning*) yang dilakukan Nmap untuk mendeteksi bahwa port 80 terbuka tanpa membuat koneksi penuh. Prosesnya terlihat jelas dalam tiga baris log berurutan: pertama, komputer Anda (192.168.43.106) mengirimkan paket **SYN** sebagai permintaan koneksi, kemudian target (192.168.43.174) merespons dengan **SYN, ACK** yang mengonfirmasi bahwa layanan HTTP aktif, dan terakhir komputer Anda langsung memutus komunikasi dengan mengirimkan paket **RST** (Reset) alih-alih menyelesaikan *three-way handshake*. Tindakan memutus koneksi secara tiba-tiba inilah yang membuat metode ini efisien dan sering disebut "stealth" karena tidak sampai membentuk sesi koneksi utuh yang biasanya dicatat oleh log aplikasi server

5. KESIMPULAN

Berdasarkan aktivitas *reconnaissance* yang dilakukan, postur keamanan target kai.id dan IP 192.168.43.174 dinilai sangat kritis akibat kombinasi paparan informasi dan infrastruktur yang usang. Pada fase pasif, ditemukan kebocoran data sensitif melalui repositori GitHub publik dan eksposur struktur organisasi yang meningkatkan risiko serangan *Social Engineering*. Kondisi ini diperburuk oleh temuan fase aktif di mana target masih menjalankan layanan *outdated* (OpenSSH 6.6.1p1, Apache 2.4.7) serta sistem operasi berbasis kernel Linux lawas yang telah mencapai status *End-of-Life*, menjadikan sistem sangat rentan terhadap eksploitasi kerentanan keamanan (CVE) yang tersedia secara publik.

Selain kerentanan perangkat lunak, terdeteksi anomali berbahaya berupa aktifnya Port 6667 (layanan IRC) yang mengindikasikan keberadaan *backdoor* atau jalur komunikasi *Command and Control* (C2) botnet. Validasi teknis melalui analisis trafik Wireshark juga mengonfirmasi lemahnya pertahanan perimeter jaringan, di mana pola paket *Stealth Scan* (SYN Scan) dapat berjalan efektif tanpa terhalang. Hal ini membuktikan bahwa tidak ada konfigurasi *firewall* yang ketat untuk membatasi visibilitas penyerang terhadap topologi dan layanan internal target.