LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

NAMA : RIZKY ADHITYA

NIM : 105841114123

KELAS : JK-5A 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 Kereta Api Indonesia (kai.id), 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.

Proyek ini dilaksanakan untuk mensimulasikan peran seorang Konsultan Keamanan Siber yang ditugaskan melakukan asesmen awal terhadap dua jenis target yang memiliki karakteristik bertolak belakang. Target pertama adalah infrastruktur publik milik PT Kereta Api Indonesia (kai.id) yang merepresentasikan sistem nyata dengan lapisan keamanan aktif. Target kedua adalah mesin VulnOSv2, sebuah sistem operasi yang sengaja dirancang rentan untuk keperluan simulasi eksploitasi di lingkungan laboratorium.

Melalui perbandingan dua objek ini, proyek ini bertujuan untuk mendemonstrasikan penerapan metodologi pengumpulan informasi yang tepat, mulai dari teknik *Passive Reconnaissance* yang bersifat non-invasif untuk target publik, hingga *Active Reconnaissance* yang agresif untuk target simulasi. Pemahaman mendalam mengenai kedua teknik ini sangat penting untuk memastikan proses audit keamanan berjalan efektif tanpa melanggar etika maupun hukum yang berlaku.

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.
d. Menguji Validitas Keamanan Infrastruktur Mengevaluasi postur keamanan awal dari mesin target VulnOSv2 dengan menemukan layanan-layanan usang (outdated services) atau konfigurasi yang tidak aman yang berpotensi menjadi celah masuk bagi penyerang.
e. Memahami Etika dan Batasan Hukum Keamanan Siber Mendemonstrasikan pemahaman mengenai Rules of Engagement (RoE) dengan membedakan tindakan yang legal dilakukan pada target publik (PT KAI) dan tindakan yang hanya boleh dilakukan pada lingkungan terkontrol (sandbox).

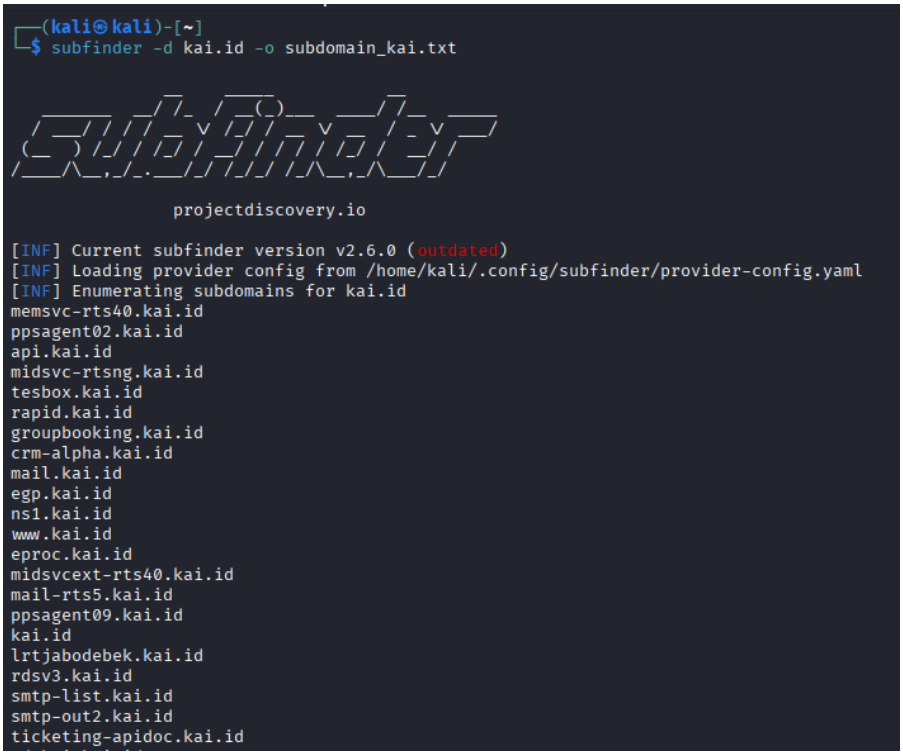
3. TABEL TEMUAN INFORMASI: Passive Reconnaissance (Target: kai.id)

Informasi yang di temukan	Sumber Tools/Website	Alasan Relevansi (pentingnya Serangan)
Daftar Subdomain Mentah	Subfinder	Memperluas Permukaan Serangan (Attack Surface).
Subdomain Aktif (Live Hosts)	httpx	Efisiensi Waktu & Fokus Serangan.
DNS Records (MX, TXT, SPF records)	Dig	MX record menunjukkan penyedia email (untuk target phishing). TXT record kadang membocorkan informasi verifikasi layanan pihak ketiga yang dipakai perusahaan.
Email Karyawan & Username	Hunter.io,GoogleDorks	Data ini digunakan untuk serangan Social Engineering

		(Phishing) atau serangan Credential Stuffing (mencoba password yang bocor dari data lain).
Teknologi Web & Versi	Hunter.io	Mengetahui *tech stack* memungkinkan penyerang mencari CVE (Common Vulnerabilities and Exposures) spesifik yang diketahui untuk versi tersebut (misal: plugin WordPress yang usang).
Logika Parameter Login API	GitHub Search	Memudahkan penyerang melakukan serangan Brute Force karena mereka tahu persis nama variabel yang diminta server. Tanpa ini, penyerang harus menebak-nebak apakah server meminta username, phone, atau email.

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

```
┌──(kali㉿kali)-[~]
└─$ httpx -l subdomain_kai.txt -title -status-code -o subdomain_kai_hidup.txt

                     __     _
   ____  ____  ____/ /_   | |/ /
  / __ \/ __ \/ __  / __ \|   /
 / / / / /_/ / /_/ / /_/ /   |
/_/ /_/\__,_/\__,_/ .___/_/|_|
                 /_/

                projectdiscovery.io

[INF] Current httpx version v1.7.3 (latest)
[WRN] UI Dashboard is disabled, Use -dashboard option to enable
https://e-recruitment.kai.id [200] [e-Recruitment PT. Kereta Api Indonesia]
https://memsvcs-rts40.kai.id [404]
https://midkci.kai.id [200]
https://booking.kai.id [200] [PT Kereta Api Indonesia -      Reservasi Tiket]
https://midsvc-rts40.kai.id [404] [404 Not Found]
https://memsvcdev.kai.id [404]
https://api.kai.id [404]
https://media.kai.id [302]
https://mail.kai.id [200] [Zimbra Web Client Sign In]
https://middev.kai.id [200] [Kereta Api Indonesia]
https://cargo.kai.id [200] [Web Portal Angkutan Barang]
https://groupbooking.kai.id [200] [KAI - Group Booking]
https://ppid.kai.id [200] [E-PPID PT Kereta Api Indonesia (Persero)]
https://pso.kai.id [200] [PSO Online]
https://rapid.kai.id [301] [301 Moved Permanently]
https://rdsv3-rw.kai.id [200] [Rail Document System - PT Kereta Api Indonesia]
https://rdsv3-ro.kai.id [200] [Rail Document System - PT Kereta Api Indonesia]
https://recruitment.kai.id [301] [301 Moved Permanently]
https://subsidiary-rts40.kai.id [404] [404 Not Found]
https://www.kai.id [200] [Situs Resmi PT Kereta Api Indonesia (Persero)]
https://b2b-apidoc.kai.id [200] [B2B KAI]
```

Gambar 1.2

Melakukan Pencarian Subdomain Yang aktif menggunkan Tools HTTPX

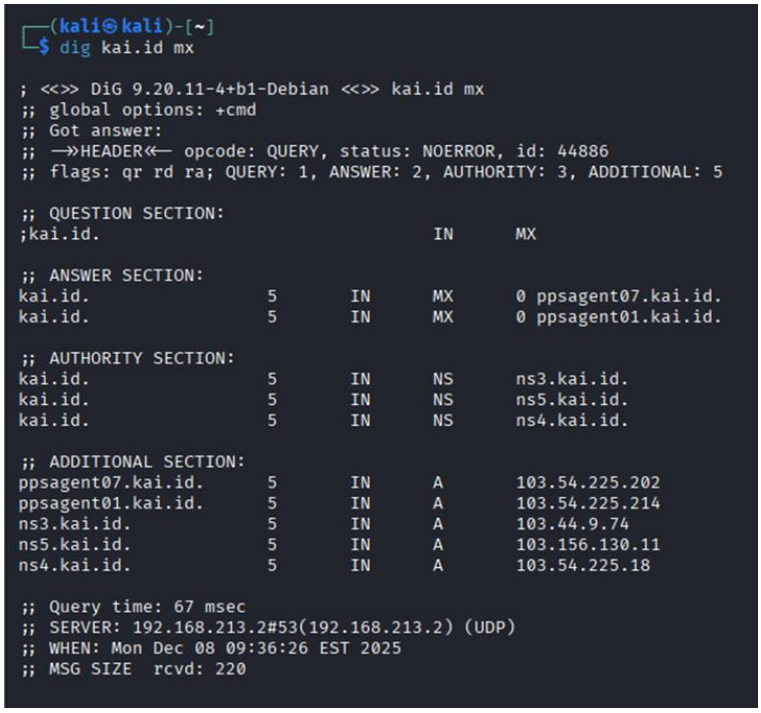
3. DNS Record Public

- A RECORD (IP ADDREST)

```
┌──(kali㉿kali)-[~]
└─$ dig kai.id

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30095
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; MBZ: 0x0005, udp: 4096
;; QUESTION SECTION:
;kai.id.                                IN      A

;; ANSWER SECTION:
kai.id.                 5       IN      A       103.54.225.47

;; Query time: 2035 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:35:55 EST 2025
;; MSG SIZE  rcvd: 51
```

Gambar 1.3

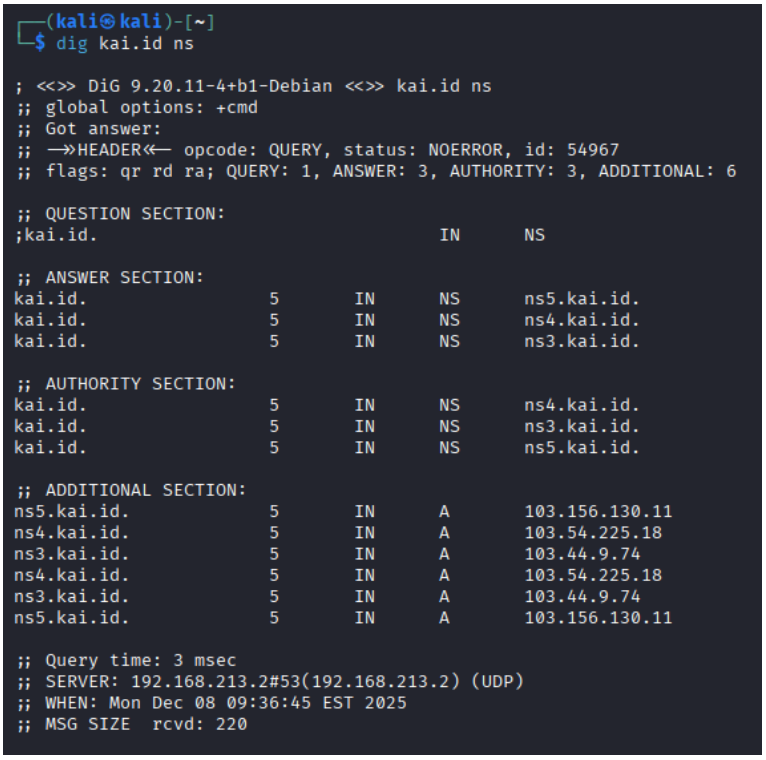
- MX RECORD (MAIL EXCHANGE)



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

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id mx
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44886
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 3, ADDITIONAL: 5

;; QUESTION SECTION:
;kai.id.                                IN      MX

;; ANSWER SECTION:
kai.id.                 5       IN      MX      0 ppsagent07.kai.id.
kai.id.                 5       IN      MX      0 ppsagent01.kai.id.

;; AUTHORITY SECTION:
kai.id.                 5       IN      NS      ns3.kai.id.
kai.id.                 5       IN      NS      ns5.kai.id.
kai.id.                 5       IN      NS      ns4.kai.id.

;; ADDITIONAL SECTION:
ppsagent07.kai.id.      5       IN      A       103.54.225.202
ppsagent01.kai.id.      5       IN      A       103.54.225.214
ns3.kai.id.             5       IN      A       103.44.9.74
ns5.kai.id.             5       IN      A       103.156.130.11
ns4.kai.id.             5       IN      A       103.54.225.18

;; Query time: 67 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:36:26 EST 2025
;; MSG SIZE  rcvd: 220
```

Gambar 1.4

- NS RECORD (NAMESERVER)



```
┌──(kali㉿kali)-[~]
└─$ dig kai.id ns

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54967
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 3, ADDITIONAL: 6

;; QUESTION SECTION:
;kai.id.                                IN      NS

;; ANSWER SECTION:
kai.id.                 5       IN      NS      ns5.kai.id.
kai.id.                 5       IN      NS      ns4.kai.id.
kai.id.                 5       IN      NS      ns3.kai.id.

;; AUTHORITY SECTION:
kai.id.                 5       IN      NS      ns4.kai.id.
kai.id.                 5       IN      NS      ns3.kai.id.
kai.id.                 5       IN      NS      ns5.kai.id.

;; ADDITIONAL SECTION:
ns5.kai.id.             5       IN      A       103.156.130.11
ns4.kai.id.             5       IN      A       103.54.225.18
ns3.kai.id.             5       IN      A       103.44.9.74
ns4.kai.id.             5       IN      A       103.54.225.18
ns3.kai.id.             5       IN      A       103.44.9.74
ns5.kai.id.             5       IN      A       103.156.130.11

;; Query time: 3 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:36:45 EST 2025
;; MSG SIZE  rcvd: 220
```

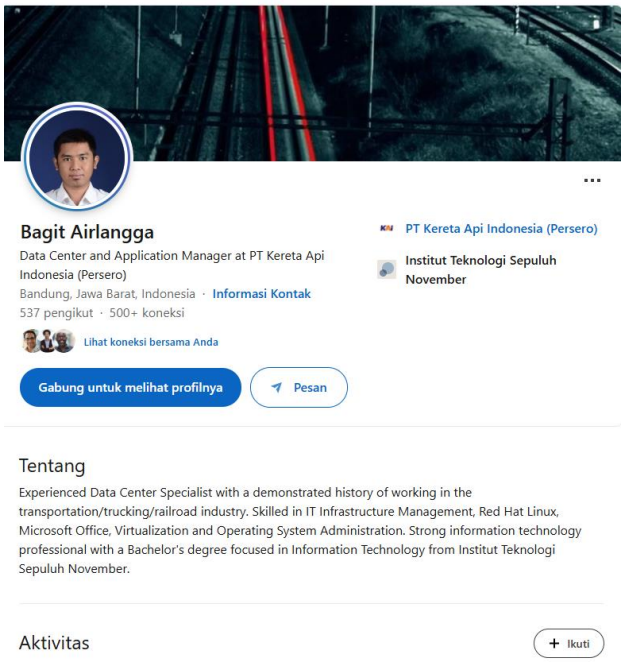
Gambar 1.5

- TXT RECORD

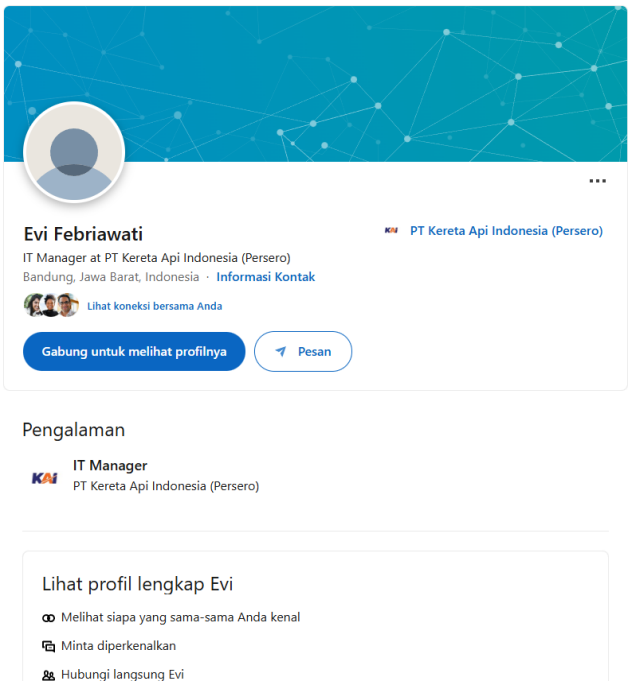
```
┌──(kali㉿kali)-[~]
└─$ dig kai.id txt

; <<>> DiG 9.20.11-4+b1-Debian <<>> kai.id txt
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38406
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;kai.id.                                IN      TXT

;; ANSWER SECTION:
kai.id.                 5       IN      TXT     "yahoo-verification-key=XmDRO9kroQ4cr1Bn8nfhYBHeVBqJPl+CoLiQ58hohwk="
kai.id.                 5       IN      TXT     "tq6qjsr420klo13la7jmsgbpds"
kai.id.                 5       IN      TXT     "MS=A952DF8E8223CF5DAFC3FF9B4CA749D462821B90"
kai.id.                 5       IN      TXT     "globalsign-domain-verification=5bfa44135cf14960b840f9993b814e8d"
kai.id.                 5       IN      TXT     "dtm-domain-verification=OMspuu1W4nNsvLgltL038pkwVmN3iUpW_c6ARL5bHBg"
kai.id.                 5       IN      TXT     "google-site-verification=DGOB3LAFcK2ZAL4spsT7XMQ8GkYFnwfkKVDsBgpeRM0"
kai.id.                 5       IN      TXT     "google-gws-recovery-domain-verification=4817228"

;; Query time: 2043 msec
;; SERVER: 192.168.213.2#53(192.168.213.2) (UDP)
;; WHEN: Mon Dec 08 09:36:58 EST 2025
;; MSG SIZE  rcvd: 496
```

Gambar 1.6

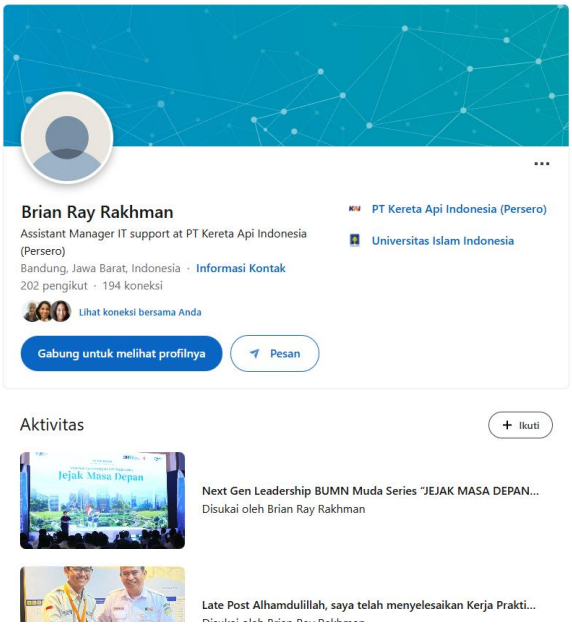
4. Profil Karyawan IT Di Linkedin



Gambar 1.7 Data Center And Application Manager PT KAI

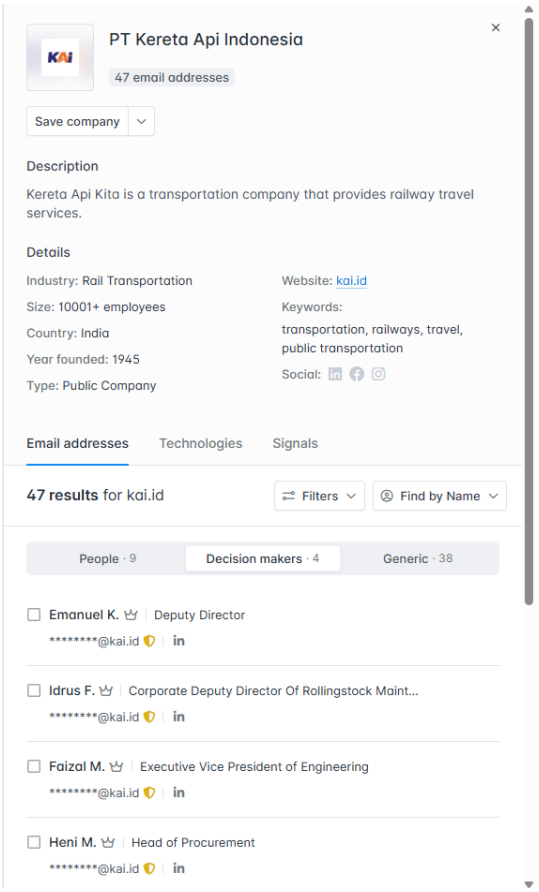


Gambar 1.8 IT Manager PT KAI



Gambar 1.9 IT ASSISTAN MANAGER / IT SUPPORT PT KAI

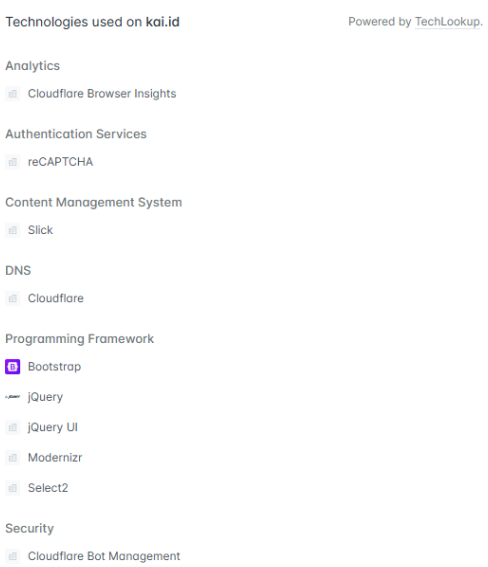
5. Domain/Format Email Perusahaan



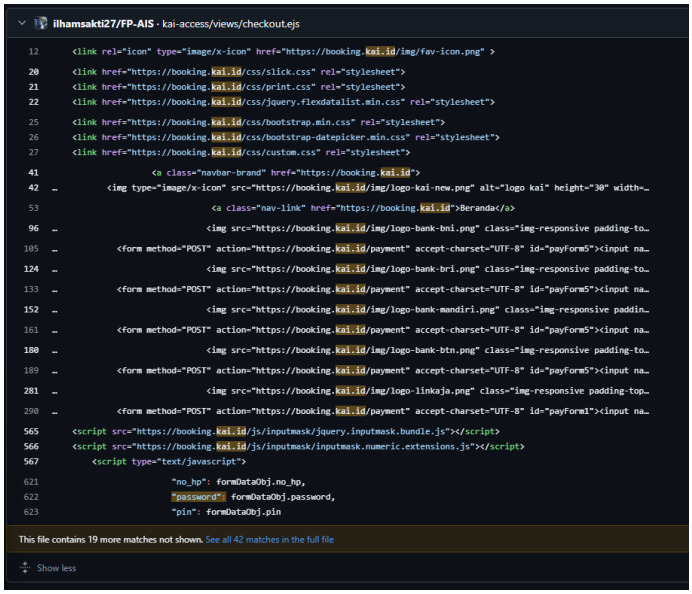
Gambar 1.10

Mencari Format Email yang di gunakan Yaitu @kai.id, Pencarian Menggunakan Hunter.io

6. Teknologi yang di Gunakan



7. Informasi Git PT Kai

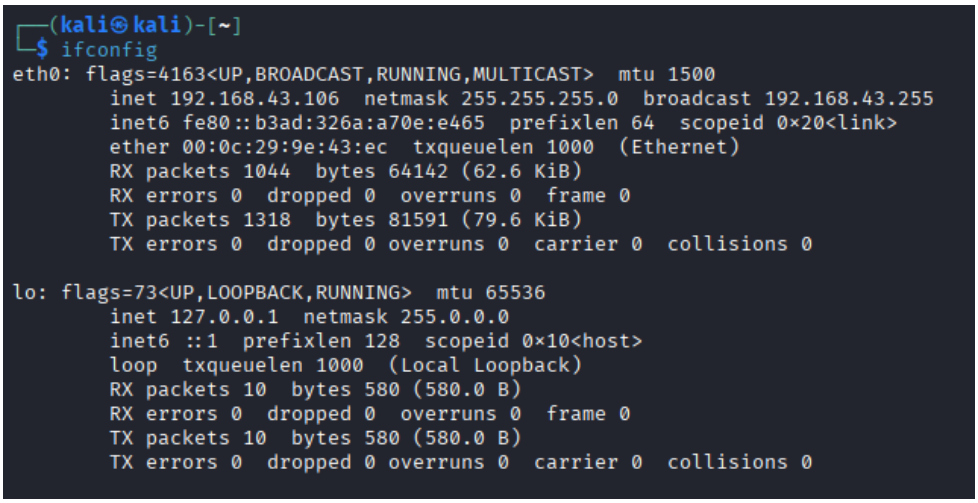


Gambar 1.12

Commit github yang di temukan adalah bagian dari kai access yang di dapatkan menggunakan Github dengan cara “PTKAI” “password”:

4. ACTIVE RECONNAISSANCE (HASIL DAN ANALASIS)

Ifconfig



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."

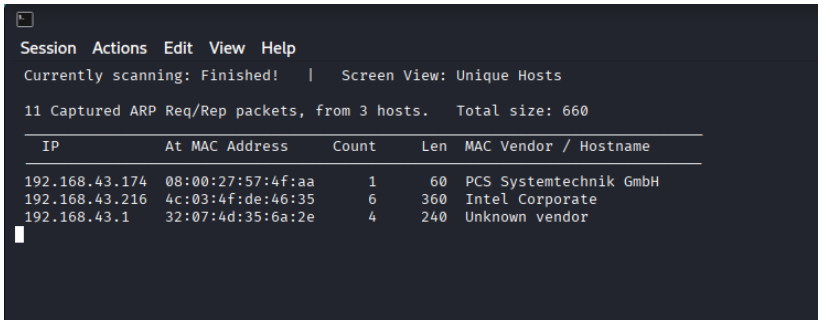
a. Host Discover and Port Scanning

Tabel 1.4 Hasil Pemindaian Host dan Port (Active Reconnaissance)

Tugas	Command	Hasil	Potensi dampak
Host Discovery	sudo netdiscover -r 172.20.10.0/24	Target ditemukan: 172.20.10.3	Memastikan host aktif di jaringan.
TCP SYN Scan	sudo nmap -sS 172.20.10.3	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	sudo nmap -sU --top ports 20 172.20.10.3	Open/Filtered: 53, 67	DNS dan DHCP berpotensi menjadi target analisis.

1. **Dokumentasi**

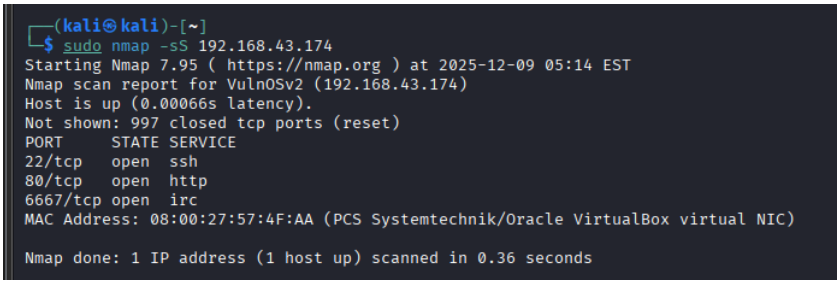
- NETDISCOVER



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

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sU --top-ports 20 192.168.43.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:47 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.0017s latency).

PORT      STATE         SERVICE
53/udp    closed        domain
67/udp    closed        dhcps
68/udp    open|filtered dhcpc
69/udp    closed        tftp
123/udp   closed        ntp
135/udp   open|filtered msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   open|filtered netbios-ssn
161/udp   closed        snmp
162/udp   open|filtered snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   open|filtered ipp
1434/udp  open|filtered ms-sql-m
1900/udp  open|filtered upnp
4500/udp  closed        nat-t-ike
49152/udp closed        unknown
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 10.70 seconds
```

Gambar 4.4

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

2. Service and Version Detection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 192.168.43.174
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:43 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.0011s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
6667/tcp open  irc     ngircd
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.77 seconds
```

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.

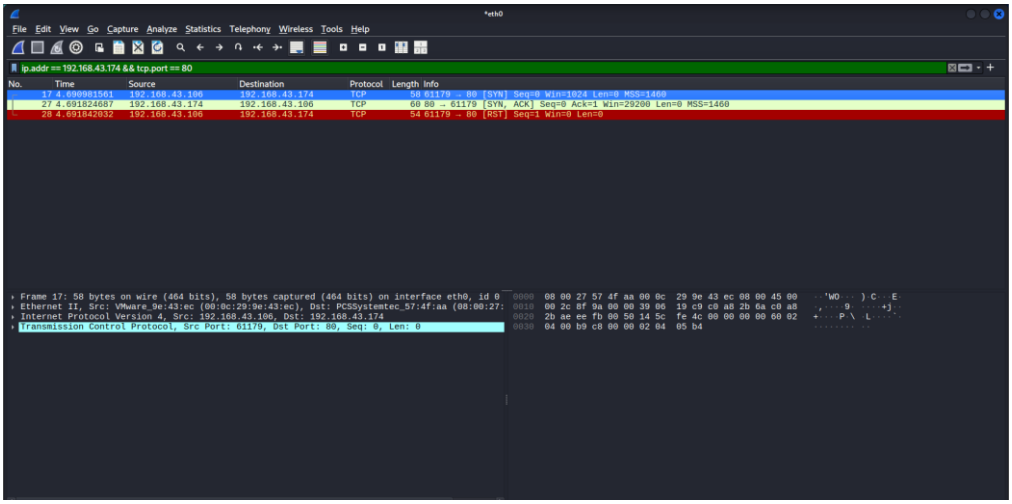
3. OS Fingerprinting

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.43.174
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:54 EST
Nmap scan report for VulnOSv2 (192.168.43.174)
Host is up (0.0015s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
6667/tcp open  irc
MAC Address: 08:00:27:57:4F:AA (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
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 1.71 seconds
```

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.