ANALISIS JEJAK DIGITAL (OSINT) PADA DOMAIN PEMERINTAH DAN SIMULASI PEMINDAIAN JARINGAN (ACTIVE SCANNING)

Studi Kasus: Pemerintah Provinsi Jawa Barat & Simulasi Laboratorium

Ririn Yulandari

105841117923

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

1. Pendahuluan

a. Latar Belakang

Dalam era digital, keamanan infrastruktur teknologi informasi menjadi krusial. Tugas besar ini mensimulasikan proses *Security Assessment* yang terdiri dari tahapan *Passive Reconnaissance* (Pengumpulan informasi tanpa interaksi) dan *Active Reconnaissance* (Pemindaian jaringan secara aktif) untuk mengidentifikasi potensi celah keamanan.

b. Tujuan

1) Melakukan pemetaan aset digital (footprinting) pada target nyata menggunakan metode OSINT.
2) Mengidentifikasi port, layanan, dan sistem operasi pada target laboratorium menggunakan teknik pemindaian aktif.
3) Mendokumentasikan temuan teknis sebagai bahan evaluasi keamanan.

c. Ruang Lingkup (Scope)

1) **Passive Recon**

Target Passive: Pemerintah Provinsi Jawa Barat (**jabarprov.go.id**)

Batasan: Hanya sebatas pengumpulan informasi publik (OSINT) menggunakan Google Dorks, dan pencarian repositori eksternal tanpa melakukan pemindaian intrusif ke server pemerintah.

2) **Active Recon**

Target Active: Lingkungan Laboratorium Lokal (**IP: 192.168.131.39**)

Batasan: Pemindaian port (*Port Scanning*) dan analisis trafik jaringan (*Network Protocol Analysis*) dilakukan terhadap infrastruktur milik sendiri (*Localhost/Loopback*) untuk mensimulasikan interaksi antara penyerang dan target dalam lingkungan yang aman dan legal.

2. Metodologi & Alat

a. Skenario

Penulis bertindak sebagai Konsultan Keamanan Siber independen. Tahap pertama dilakukan untuk memetakan "permukaan serangan" (*attack surface*) dari target korporasi besar. Tahap kedua dilakukan dalam lingkungan terkontrol untuk mensimulasikan bagaimana penyerang mencari celah teknis pada server yang rentan.

b. Alat yang Digunakan

1) Passive Recon: Browser (Chrome), Wappalyzer, crt.sh, Google Dorks, Github.
2) Active Recon: Kali Linux, Nmap, Wireshark.

   Target Lab: Metasploitable 3 (IP Target: 192.168.131.39).

3. Passive Reconnaissance

a. Pencarian Domain & Sub-domain

Target: Pemerintah Provinsi Jawa Barat (jabarprov.go.id)

Untuk memetakan infrastruktur digital target tanpa melakukan interaksi langsung, penulis menggunakan metode OSINT dengan alat pencarian Certificate Transparency, yaitu crt.sh. Berikut adalah bukti temuan subdomain yang berhasil diidentifikasi:

Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
1688760495	2019-07-20	2019-07-20	2019-10-18	tanjab.bapenda.jabarprov.go.id	tanjab.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688792604	2019-07-20	2019-07-20	2019-10-18	portal.bapenda.jabarprov.go.id	portal.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688756946	2019-07-20	2019-07-20	2019-10-18	persediaanbarang.bapenda.jabarprov.go.id	persediaanbarang.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688755790	2019-07-20	2019-07-20	2019-10-18	e-surat.bapenda.jabarprov.go.id	e-surat.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688754165	2019-07-20	2019-07-20	2019-10-18	e-sim.bapenda.jabarprov.go.id	e-sim.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688753531	2019-07-20	2019-07-20	2019-10-18	e-perpustakaan.bapenda.jabarprov.go.id	e-perpustakaan.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688752850	2019-07-20	2019-07-20	2019-10-18	plopd.bapenda.jabarprov.go.id	plopd.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688751992	2019-07-20	2019-07-20	2019-10-18	p3d-tasikmalaya.bapenda.jabarprov.go.id	p3d-tasikmalaya.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688752210	2019-07-20	2019-07-20	2019-10-18	p3d-sumber.bapenda.jabarprov.go.id	p3d-sumber.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688752874	2019-07-20	2019-07-20	2019-10-18	p3d-sumedang.bapenda.jabarprov.go.id	p3d-sumedang.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688751926	2019-07-20	2019-07-20	2019-10-18	e-guestbook.bapenda.jabarprov.go.id	e-guestbook.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688751772	2019-07-20	2019-07-20	2019-10-18	p3d-sukabumi.bapenda.jabarprov.go.id	p3d-sukabumi.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688751871	2019-07-20	2019-07-20	2019-10-18	p3d-subang.bapenda.jabarprov.go.id	p3d-subang.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688769993	2019-07-20	2019-07-20	2019-10-18	p3d-sukaraja.bapenda.jabarprov.go.id	p3d-sukaraja.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688936065	2019-07-20	2019-07-20	2019-10-18	p3d-pelabuhanratu.bapenda.jabarprov.go.id	p3d-pelabuhanratu.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688752878	2019-07-20	2019-07-20	2019-10-18	p3d-soekarnohatta.bapenda.jabarprov.go.id	p3d-soekarnohatta.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X3
1688751945	2019-07-20	2019-07-20	2019-10-18	p3d-soreang.bapenda.jabarprov.go.id	p3d-soreang.bapenda.jabarprov.go.id	C=US, O=Let's Encrypt, CN=Let's Encrypt

Dalam tahap *Passive Reconnaissance* ini, ditemukan bahwa target memiliki permukaan serangan (*attack surface*) yang luas pada sektor pendapatan daerah. Screenshot di atas memperlihatkan adanya subdomain krusial seperti **portal.bapenda.jabarprov.go.id** dan **e-surat.bapenda.jabarprov.go.id**. Keberadaan subdomain **e-surat** dan **persediaanbarang** yang terekspos ke publik mengindikasikan bahwa aplikasi operasional internal dapat diakses dari jaringan internet umum. Hal ini meningkatkan risiko keamanan karena penyerang tidak perlu berada di dalam jaringan lokal kantor untuk mencoba mengeksploitasi sistem administrasi internal tersebut. Selain itu, banyaknya subdomain **p3d-*** (Pusat Pengelolaan Pendapatan Daerah) menunjukkan bahwa sistem ini terdesentralisasi ke berbagai wilayah cabang, yang mungkin memiliki standar keamanan yang tidak seragam di setiap titiknya.

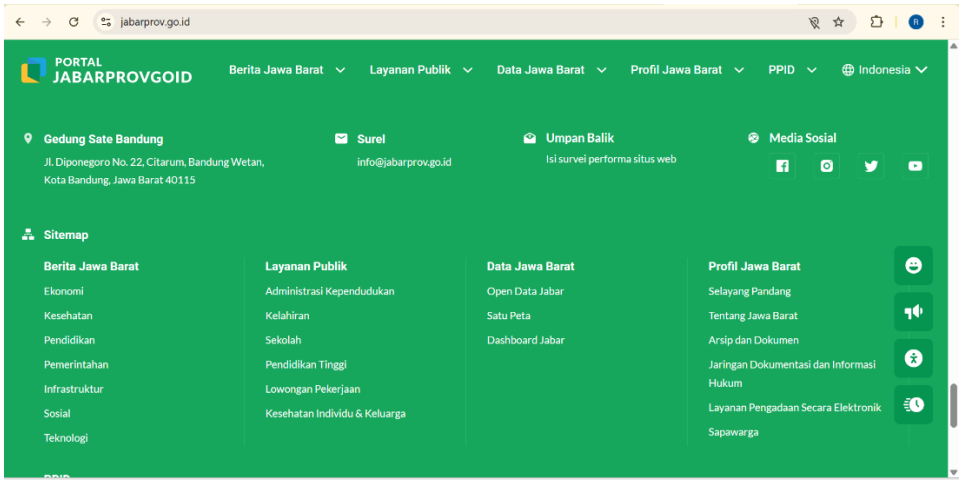
b. Informasi Email dan Karyawan:

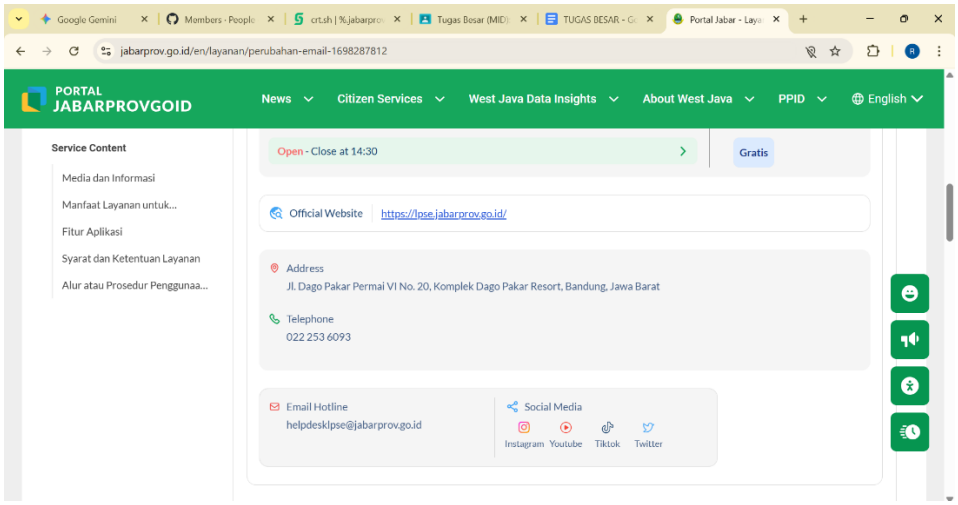
Bagian ini mendokumentasikan hasil pengumpulan informasi terkait struktur komunikasi dan personil teknis target.

1) **Identifikasi Format Email**

Tujuan: Menentukan pola alamat email standar perusahaan untuk keperluan serangan *Phishing* atau *Brute Force*.

Metode: *Google Dorking* dengan query site:jabarprov.go.id "email" "@jabarprov.go.id".





Berdasarkan hasil pencarian pada sumber terbuka (Open Source Intelligence), ditemukan bahwa organisasi menggunakan domain utama @jabarprov.go.id untuk komunikasi resmi.

Email Fungsional: Ditemukan alamat seperti info@jabarprov.go.id dan helpdesklpse@jabarprov.go.id.

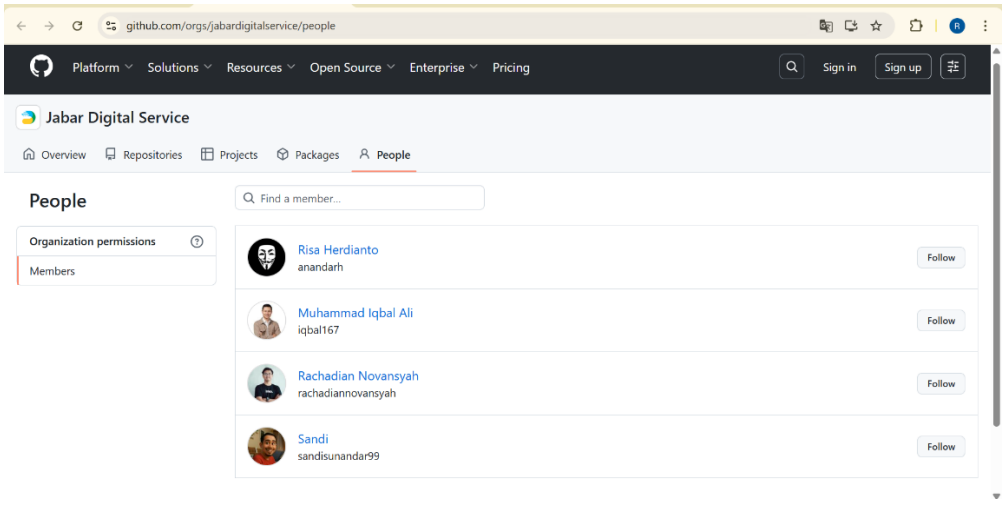
Pola Email Personal: Berdasarkan standar instansi pemerintahan dan pola nama pengguna yang ditemukan, format email karyawan diestimasikan mengikuti pola:

- **Format:**[nama.lengkap]@jabarprov.go.id atau [nama.depan]@jabarprov.go.id.

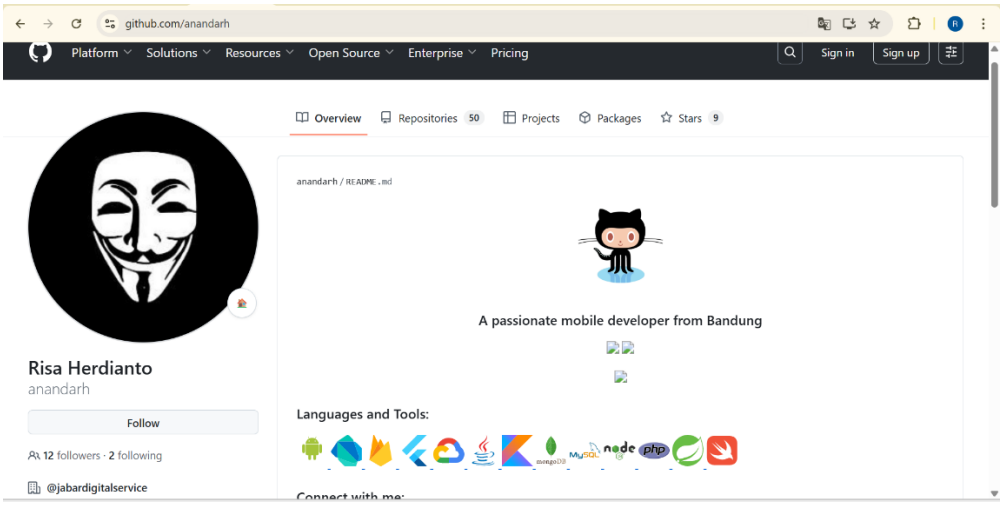
Relevansi Keamanan: Mengetahui format email memungkinkan penyerang membuat daftar target (wordlist) berisi ribuan kemungkinan alamat email pegawai untuk dikirimi malware atau tautan berbahaya.

2) **Profiling Karyawan (Employee Profiling)**

Mengidentifikasi individu kunci dalam organisasi (Teknis & Manajemen) sebagai target serangan *Social Engineering*. Menggunakan metode analisis profil publik pada organisasi GitHub resmi Jabar Digital Service.

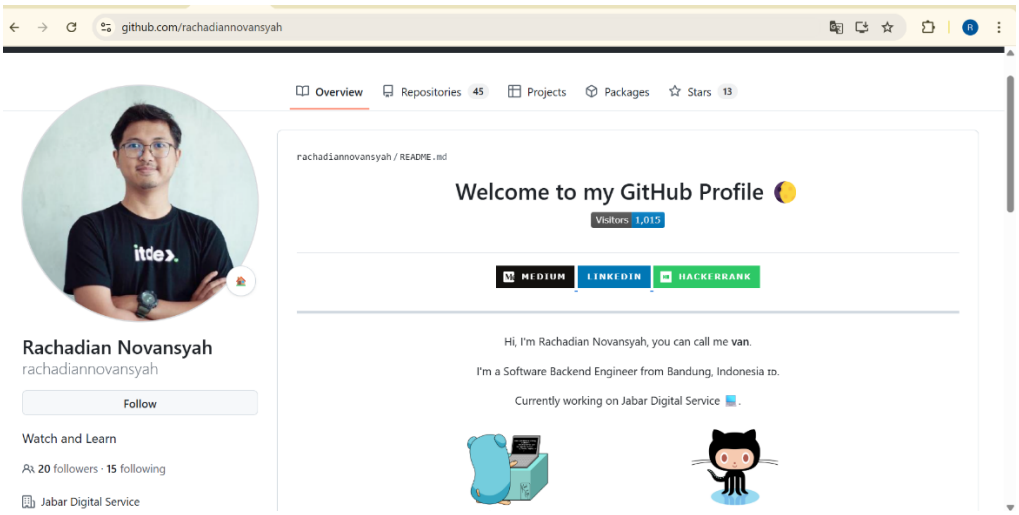


- Karyawan: Risa Herdianto,
  Jabatan: Mobile Developer



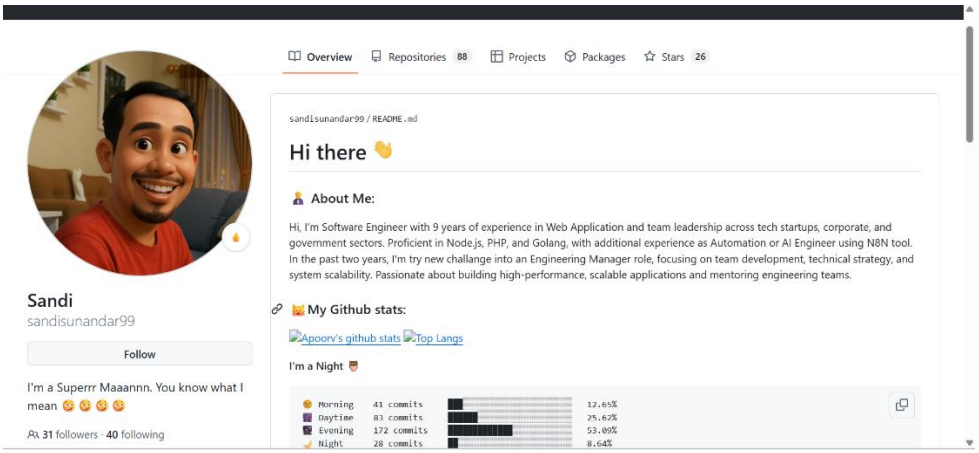
- Karyawan: Rachadian Novansyah

  Jabatan: Software Backend Engineer



- Karyawan: Sandi

  Jabatan: Engineering Manager & Software Engineer



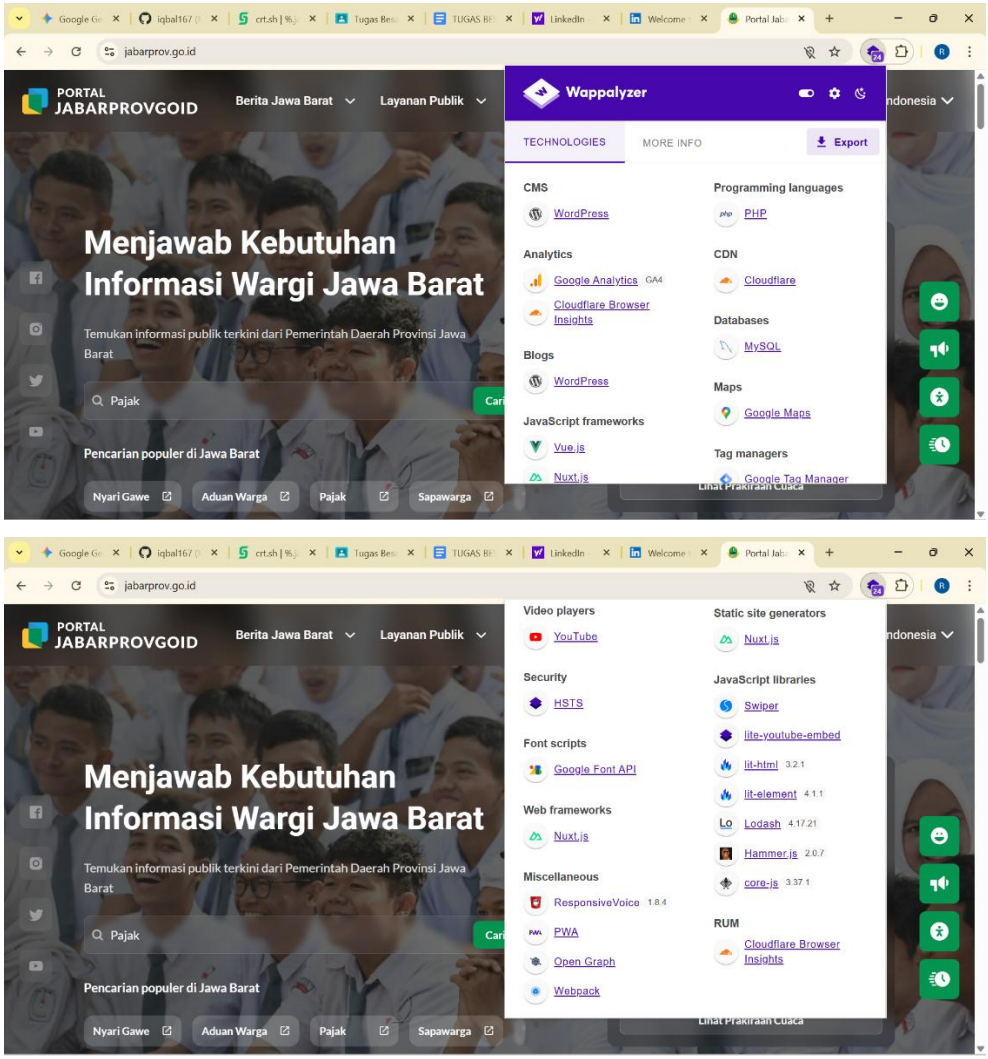
  Analisis & Relevansi Keamanan:

  Target Bernilai Tinggi (High Value Target) ditemukannya akun *Engineering Manager* (Sandi) sangat kritis. Jika akun ini berhasil diretas, penyerang bisa mendapatkan akses manajerial ke seluruh infrastruktur pengembangan. Serangan Spesifik (*Spear Phishing*), penyerang dapat mengirim email palsu kepada Rachadian (*Backend Engineer*) yang berisi "Update Server Penting" palsu, karena perannya berkaitan langsung dengan *server*. Mengetahui jabatan spesifik membuat skenario penipuan terlihat jauh lebih meyakinkan.

c. Identifikasi Teknologi

Metode: Identifikasi stack teknologi menggunakan ekstensi browser **Wappalyzer**.

Target URL: https://jabarprov.go.id



1) Target menggunakan layanan *Cloudflare*. Hal ini menyulitkan proses *Active Reconnaissance* karena Cloudflare menyembunyikan alamat IP asli (*Origin IP*) server. Penyerang harus mencari celah *misconfiguration* atau *bypass* untuk menemukan IP asli agar bisa menyerang server secara langsung.
2) Terdeteksi penggunaan framework *Vue.js* (atau Nuxt.js). Ini menandakan arsitektur aplikasi bersifat *Single Page Application* (SPA). Fokus kerentanan pada teknologi ini biasanya berada di sisi klien (*Client-Side Vulnerabilities*) seperti *Cross-Site Scripting* (XSS), bukan di sisi server tradisional.
3) Penggunaan *Google Analytics* memungkinkan pihak pengelola memantau trafik pengguna. Bagi penyerang, ID pelacak (*Tracking ID*) yang terekspos terkadang

dapat digunakan untuk melacak jejak digital aset website lain yang dimiliki oleh organisasi yang sama (teknik *Reverse Analytics*).

d. Informasi Sensitif yang Terpapar (Information Disclosure)

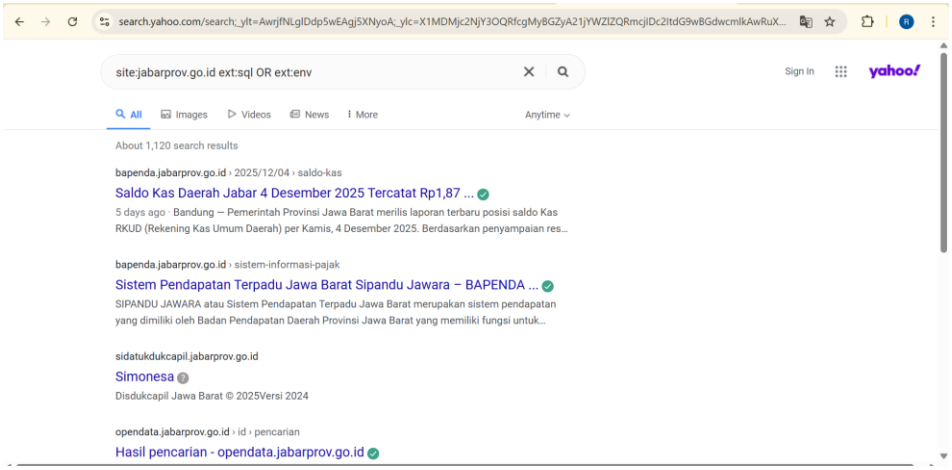
Mengidentifikasi kebocoran informasi sensitif (kredensial, backup database, atau dokumen internal) yang terindeks secara publik di mesin pencari dan repositori kode, tanpa melakukan interaksi langsung dengan server target. Dilakukan teknik *Passive Reconnaissance* menggunakan Google Dorks dan GitHub Search terhadap domain jabarprov.go.id.

Hasil Temuan:

- **Pencarian Google Dorks:**

  Query: site:jabarprov.go.id ext:sql OR ext:env

  Status: Aman / Tidak Ditemukan.

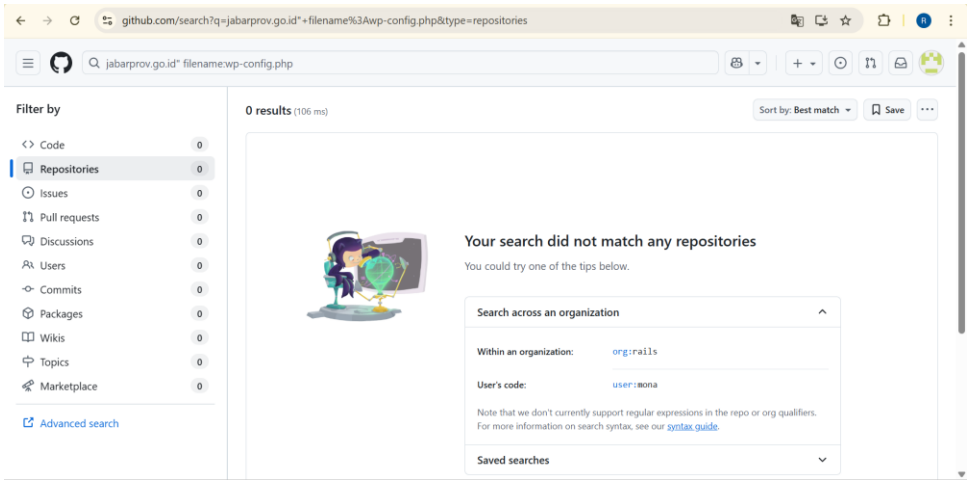


Validasi menggunakan query *site:jabarprov.go.id ext:sql OR ext:env* tidak menemukan file database atau konfigurasi server yang terekspos. Hasil pencarian hanya menampilkan halaman web publik (HTML) biasa, menandakan tidak adanya kebocoran file sensitif.

- **Pencarian Repository Kode(Github):**

  Query: jabarprov.go.id" filename:wp-config.php

  Status: Aman / Tidak Ditemukan.



Tidak ditemukan *hardcoded credentials* (API Key, Database Password) atau kode sumber internal yang bocor pada repositori publik GitHub.

- **Analisis Keamanan**

  Organisasi target menunjukkan tingkat kematangan keamanan yang baik dalam aspek pengelolaan aset digital publik (*Digital Footprint*). Mekanisme robots.txt dan konfigurasi server tampaknya telah diterapkan dengan benar untuk mencegah pengindeksan file sensitif.

e. Tabel Hasil Analisis Passive Reconnaissance (Target: jabarprov.go.id)

Informasi yang Ditemukan	Sumber (Alat/Website)	Alasan Relevansi
Potensi File Sensitif (Hasil Analisis: Aman/False Positive) *(Mencari file .sql & .env, namun hasil yang muncul hanya halaman web publik).*	Google Dorks (ext:sql, ext:env)	Informasi ini sangat kritikal karena file .sql atau .env seringkali memuat kredensial database, *password*, dan *API Key*. Jika ditemukan, penyerang bisa mengambil alih sistem tanpa perlu melakukan eksploitasi rumit.
Daftar Subdomain (Ditemukan daftar domain turunan dari log transparansi SSL).	crt.sh (Certificate Logs)	enting untuk memetakan "Permukaan Serangan" (*Attack Surface*). Penyerang sering menargetkan

		subdomain lama (seperti dev.jabarprov...) yang keamanannya sering terlupakan dibandingkan domain utama.
Profil Teknologi (Web Server/CMS)	Wappalyzer (Browser Extension)	Mengetahui jenis teknologi (misal: PHP, Apache, WordPress) dan versinya memungkinkan penyerang mencari kerentanan spesifik (*CVE*) yang sudah diketahui publik untuk versi tersebut.
Kebocoran Kode Sumber(Tidak ditemukan kredensial atau API Key pada repositori publik).	GitHub Search (Repository)	Penyerang mencari repositori ini untuk menemukan *password* atau *API Key* yang tidak sengaja tertulis (*hardcoded*) oleh developer di dalam kode program.
Pola Alamat Email & Identitas Karyawan (Ditemukan nama pejabat/pegawai dan format email instansi).	Search Engine / LinkedIn (Pattern Harvesting)	Informasi nama karyawan dan format email korporat (misal: nama.depan@instansi.go.id) adalah bahan baku utama untuk melancarkan serangan *Phishing* atau *Social Engineering*.

4. ACTIVE RECONNAISSANCE

Sebelum mengetik perintah Nmap, pastikan Laboratorium Virtual sudah siap:

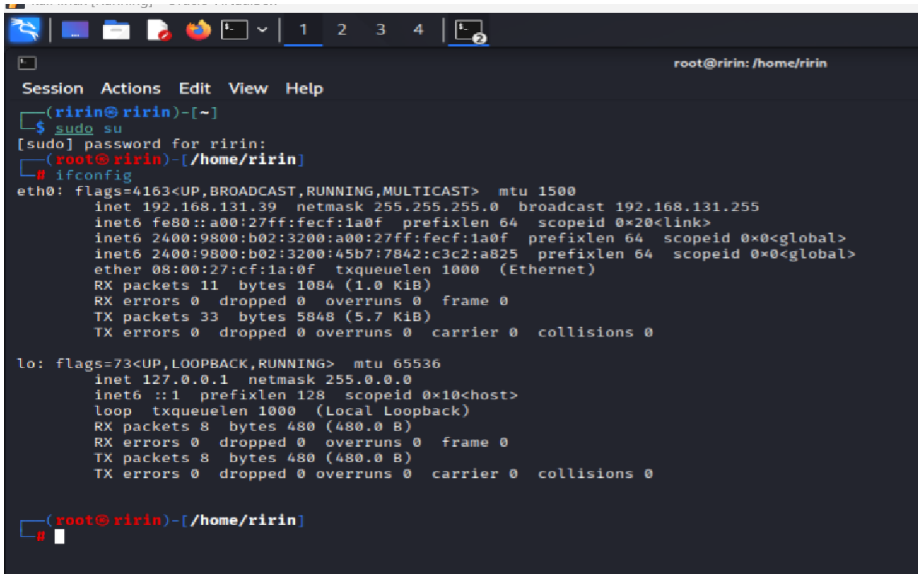
- Nyalakan Metasploitable 3 (atau VulnOS) di VirtualBox/VMware.
- Nyalakan Kali Linux.

a. Cek IP Target

Masuk ke Metasploitable, login, ketik ifconfig. Catat IP-nya

Target: Mesin Lab Metasploitable 3

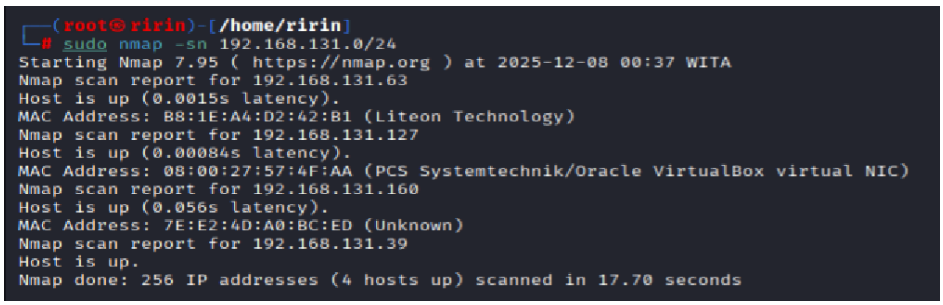
IP Target: 192.168.131.39



b. Host Discovery & SYN Scan

Tujuan: Menemukan IP target dalam jaringan

Command: sudo nmap -sn 192.168.131.0/24



Temuan: Target teridentifikasi pada IP 192.168.131.127 (Vendor: VirtualBox).Port 21 (FTP)

c. Port Scanning (TCP SYN Scan)

Tujuan: Mengidentifikasi pintu masuk (port) TCP yang terbuka.

Command: sudo nmap -sS 192.168.131.127

```
┌──(root㉿ririn)-[/home/ririn]
└─# sudo nmap -sS 192.168.131.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:39 WITA
Nmap scan report for 192.168.131.127
Host is up (0.00065s 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)

Nmap done: 1 IP address (1 host up) scanned in 7.14 seconds
```

Ditemukan 3 port terbuka yaitu SSH (22), HTTP (80), dan IRC (6667).

d. Service & Version Detection

Tujuan: Mengetahui versi aplikasi untuk mencari celah spesifik.

Command: nmap -sV 192.168.131.127

```
┌──(root㉿ririn)-[/home/ririn]
└─# nmap -sV 192.168.131.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:41 WITA
Nmap scan report for 192.168.131.127
Host is up (0.00049s 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 19.03 seconds
```

Analisis Kerentanan:

- Apache 2.4.7: Versi usang, rentan terhadap berbagai CVE.
- ngircd: Layanan IRC yang tidak lazim di jaringan korporat, berpotensi sebagai backdoor atau saluran C2 (Command & Control).

e. OS Fingerprinting

Tujuan: Mengidentifikasi Sistem Operasi.

Command: sudo nmap -O 192.168.131.127

```
┌──(root㉿ririn)-[/home/ririn]
└─# sudo nmap -O 192.168.131.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:44 WITA
Nmap scan report for 192.168.131.127
Host is up (0.0021s 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 8.52 seconds
```

Temuan: Target menggunakan OS Linux (Kernel 3.2 - 4.14)

f. UDP Scanning

Tujuan: Memeriksa layanan berbasis UDP.

Command: sudo nmap -sU --top-ports 20 192.168.131.127

```
┌──(root㉿ririn)-[/home/ririn]
└─# sudo nmap -sU --top-ports 20 192.168.131.127
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 00:48 WITA
Nmap scan report for 192.168.131.127
Host is up (0.0021s 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   closed        msrpc
137/udp   closed        netbios-ns
138/udp   closed        netbios-dgm
139/udp   closed        netbios-ssn
161/udp   closed        snmp
162/udp   closed        snmptrap
445/udp   closed        microsoft-ds
500/udp   closed        isakmp
514/udp   closed        syslog
520/udp   closed        route
631/udp   closed        ipp
1434/udp  closed        ms-sql-m
1900/udp  closed        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 23.91 seconds
```

Temuan: Port 68/udp (DHCP) terdeteksi open|filtered.

g. Network Protocol Analysis

Melakukan analisis trafik jaringan menggunakan Wireshark selama proses *Active Reconnaissance* (Nmap Scanning) untuk memahami perbedaan perilaku protokol TCP saat berinteraksi dengan *port* yang terbuka dan tertutup pada antarmuka *loopback* (localhost).

Target: Localhost (IP: 192.168.131.39).

Interface: Loopback (lo).

Metode Scan: TCP Connect Scan (-sT).

a. Pemindaian pada Port Tertutup (Closed Port)

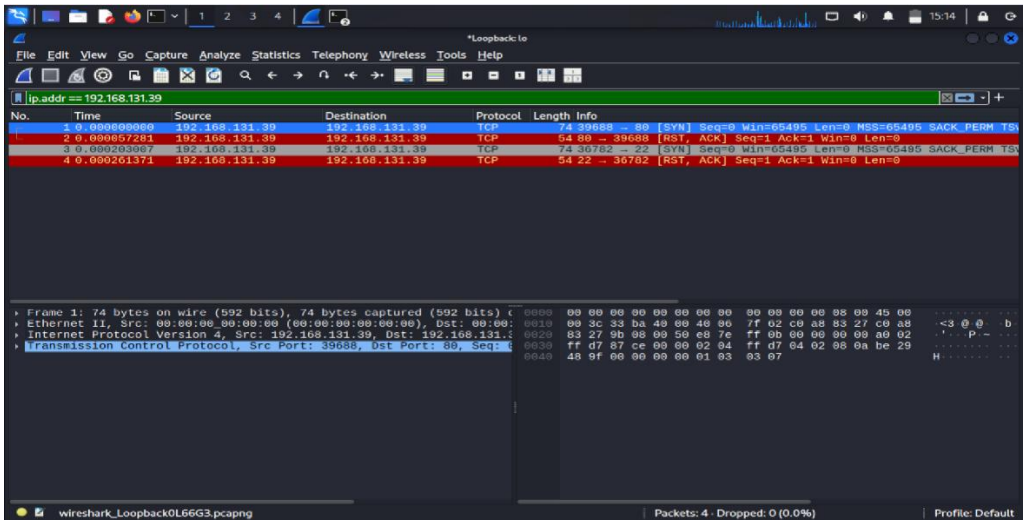
Pada percobaan pertama, layanan SSH dan Apache Web Server dinonaktifkan (*stopped*). Pemindaian dilakukan untuk melihat respons jaringan ketika koneksi ditolak.

```
┌──(root㉿ ririn)-[/home/ririn]
└─# nmap -sT -p 22,80 192.168.131.39
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 15:13 WITA
Nmap scan report for 192.168.131.39
Host is up (0.00049s latency).

PORT   STATE  SERVICE
22/tcp closed ssh
80/tcp closed http

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds

┌──(root㉿ ririn)-[/home/ririn]
```



Berdasarkan tangkapan layar di atas, Nmap melaporkan status port 22 dan 80 sebagai *closed.* Analisis paket pada Wireshark menunjukkan perilaku berikut:

- Inisiasi (SYN): Klien (Nmap) mengirimkan paket SYN ke target untuk memulai koneksi.
- Penolakan (RST, ACK): Karena tidak ada layanan yang aktif, sistem operasi target segera membalas dengan paket [RST, ACK] (Reset).
- Indikator Warna: Wireshark menandai paket ini dengan warna merah, yang mengindikasikan terjadinya *error* atau pemutusan koneksi secara paksa oleh server. Tidak terjadi proses *handshake* yang lengkap.

b. Pemindaian pada Port Terbuka (Open Port)

Pada percobaan kedua, layanan apache2 dan ssh diaktifkan menggunakan perintah systemctl start. Pemindaian ulang dilakukan untuk mengamati proses koneksi yang sukses.

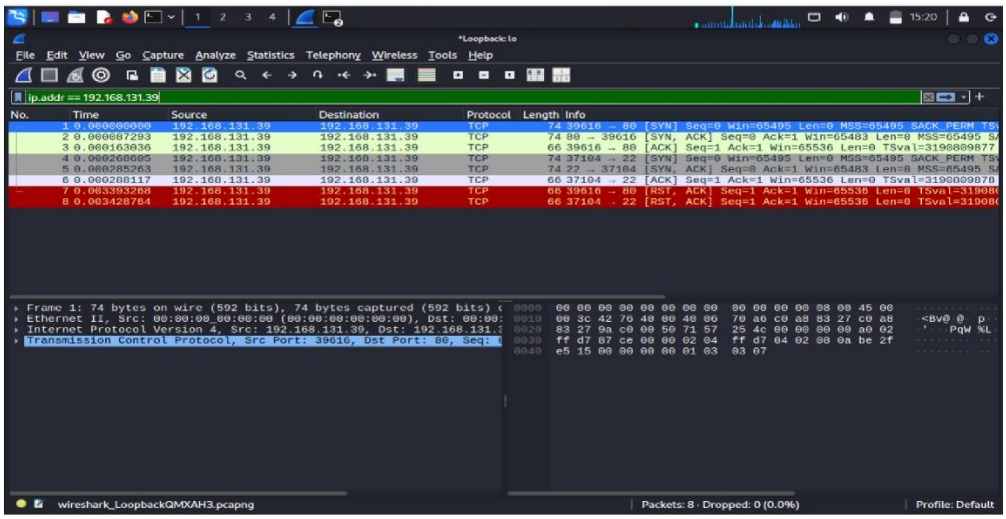
```
┌──(root㉿ririn)-[/home/ririn]
└─# systemctl start apache2

┌──(root㉿ririn)-[/home/ririn]
└─# systemctl start ssh

┌──(root㉿ririn)-[/home/ririn]
└─# nmap -sT -p 22,80 192.168.131.39
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 15:20 WITA
Nmap scan report for 192.168.131.39
Host is up (0.0035s latency).

PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```



Setelah layanan diaktifkan, Nmap melaporkan status port sebagai *open.* Wireshark berhasil menangkap proses *TCP 3-Way Handshake* yang lengkap dengan urutan sebagai berikut:

- (SYN): Klien mengirim permintaan koneksi (Baris 1).
- (SYN, ACK): Server merespons dan menyetujui koneksi (Baris 2 - *paket ini yang tidak muncul pada skenario A*).
- (ACK): Klien mengonfirmasi koneksi, sehingga status menjadi *Established* (Baris 3).

  Setelah Nmap memastikan port terbuka, koneksi kemudian ditutup kembali (RST/FIN) untuk menghemat sumber daya.

h. Analisis Risiko (Active Reconnaissance)

Berdasarkan serangkaian pemindaian aktif yang dilakukan terhadap target 192.168.131.127, dapat disimpulkan bahwa target memiliki tingkat keamanan yang sangat rendah (*Critical Vulnerability*). Berikut adalah rangkuman analisis risiko dari temuan tersebut:

1) Permukaan Serangan (*Attack Surface*): Target memiliki setidaknya tiga pintu masuk utama (Port 22, 80, 6667) yang terbuka tanpa filter firewall yang memadai. Keberadaan layanan IRC (*Internet Relay Chat*) pada port 6667 di dalam lingkungan jaringan perusahaan adalah indikator bahaya terbesar, karena layanan ini sering disalahgunakan sebagai saluran komunikasi *backdoor* atau *Command & Control (C2)* oleh penyerang.

2) Perangkat Lunak Usang *(Outdated Software):* Hasil *Service Version Detection* menunjukkan bahwa target menjalankan perangkat lunak yang sudah sangat tertinggal zaman, yaitu:
   - Apache httpd 2.4.7: Versi ini memiliki banyak kerentanan publik (CVE) yang dapat dieksploitasi untuk serangan *Remote Code Execution* (RCE) atau *Denial of Service* (DoS).
   - OpenSSH 6.6.1p1: Versi lama ini rentan terhadap enumerasi user, memudahkan penyerang melakukan serangan *Brute Force*.
3) Eksposur Sistem Operasi: Deteksi OS berhasil mengidentifikasi target sebagai Linux (Kernel 3.x - 4.x). Informasi spesifik ini memudahkan penyerang untuk mencari eksploitasi level kernel (*Kernel Exploits*) seperti "Dirty COW" untuk mendapatkan akses *root* jika sistem tidak di-*patch*.
4) Analisis Protokol Jaringan (Network Protocol Analysis)

   Analisis trafik menggunakan Wireshark memvalidasi status layanan target:
   - Konfirmasi Layanan Aktif: Terpantau adanya pola TCP 3-Way Handshake yang sukses (SYN–SYN-ACK-ACK) pada port 22, 80, dan 6667. Diterimanya paket [SYN, ACK] dari target membuktikan bahwa layanan tersebut siap menerima koneksi dan tidak dilindungi oleh *rule* firewall (DROP/REJECT).
   - Risiko Protokol: Adanya lalu lintas pada port HTTP (80) dan IRC (6667) mengindikasikan penggunaan protokol teks terang (*cleartext*). Hal ini meningkatkan risiko *sniffing* kredensial atau data sensitif jika terjadi komunikasi data.

5. Kesimpulan

Berdasarkan serangkaian simulasi *Security Assessment* yang terbagi menjadi tahapan *Passive Reconnaissance* dan *Active Reconnaissance*, dapat ditarik kesimpulan sebagai berikut:

1) Postur Keamanan Informasi (Passive Reconnaissance)

   Hasil audit jejak digital terhadap target jabarprov.go.id menunjukkan tingkat "Digital Hygiene" yang sangat baik. Melalui metode Google Dorking dan GitHub Recon, tidak ditemukan adanya kebocoran informasi kritikal seperti file backup database (.sql), konfigurasi server (.env, wp-config), maupun kredensial yang hardcoded di repositori

publik. Hal ini mengindikasikan bahwa instansi terkait telah menerapkan kebijakan keamanan konten publik (robots.txt) dan manajemen repositori kode yang efektif untuk meminimalisir risiko Information Disclosure.

2) Analisis Perilaku Protokol (Active Reconnaissance)
3) Praktikum pemindaian aktif pada lingkungan laboratorium (Localhost/192.168.131.39) berhasil memvalidasi teori dasar jaringan komputer secara empiris menggunakan Wireshark. Analisis paket data menunjukkan perbedaan perilaku yang signifikan antara status port:
    - Port Terbuka (Open): Dikonfirmasi melalui keberhasilan proses *Three-Way Handshake* (SYN-SYN-ACK - ACK).
    - Port Tertutup (Closed): Dikonfirmasi melalui penolakan koneksi secara aktif oleh server menggunakan paket [RST, ACK] (Reset).

Secara keseluruhan, praktikum ini memberikan pemahaman mendalam mengenai bagaimana celah keamanan dipetakan dari sisi eksternal (OSINT) dan bagaimana interaksi jaringan terjadi di level protokol saat pemindaian kerentanan dilakukan.