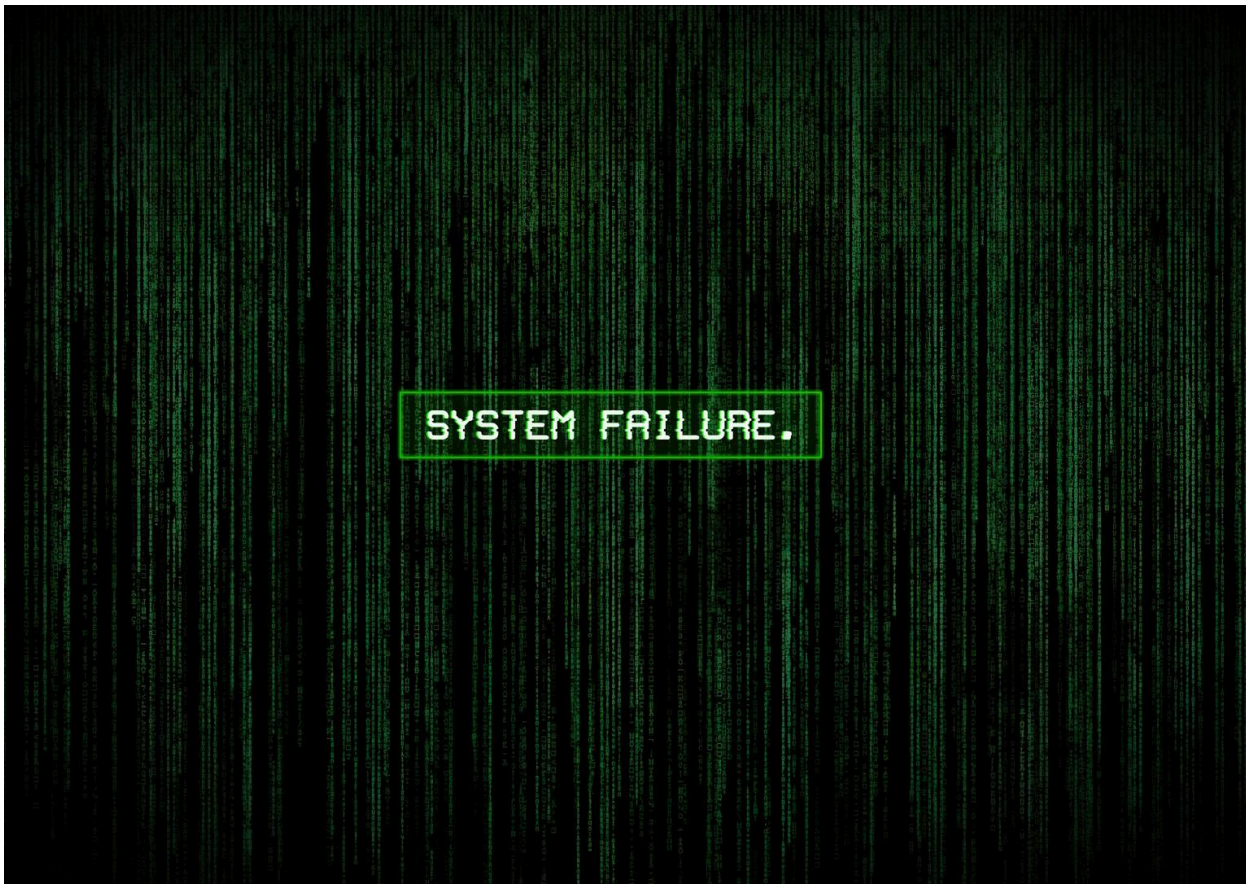
LAPORAN MID RECONNAISSANCE



RISKY AKBAR

105841118223

JK-A

PENDAHULUAN

Laporan Tugas Besar ini disusun berdasarkan skenario simulasi di mana penulis bertindak sebagai konsultan keamanan siber eksternal yang ditugaskan untuk melakukan audit keamanan terhadap (target). Sesuai dengan mandat yang diberikan, fokus utama dari kegiatan ini adalah mengidentifikasi potensi titik masuk (*entry points*) pada infrastruktur *online* maupun *offline* perusahaan.

Lingkup Pasif, pengumpulan informasi dilakukan terhadap target publik nyata (sesuai instruksi) menggunakan metode OSINT (*Open-Source Intelligence*) tanpa melakukan serangan aktif.

Lingkup Aktif, pemindaian aktif (*scanning*) dibatasi secara ketat hanya pada alamat IP target yang telah ditentukan dalam skenario laboratorium (simulasi menggunakan VulnOS/Metasploitable).

Batasan Etis, Penulis mematuhi aturan untuk tidak melakukan eksploitasi yang merusak (DoS) atau pencurian data sensitif di luar konteks simulasi pendidikan.

1. PASSIVE RECONNAISSANCE (PENGINTAIAN PASIF)

Passive Reconnaissance adalah tahapan pengumpulan informasi tanpa berinteraksi langsung dengan sistem target.

Tujuan mengidentifikasi informasi publik target tanpa meninggalkan jejak atau *log* di sistem target.

TOOLS

1. DNSDumpster
2. Subfinder
3. Sublist3r
4. Wappalyzer
5. WhatWeb
6. theHarvester
7. Google Search
8. Google Dorking (Hacking)

LANGKAH-LANGKAH

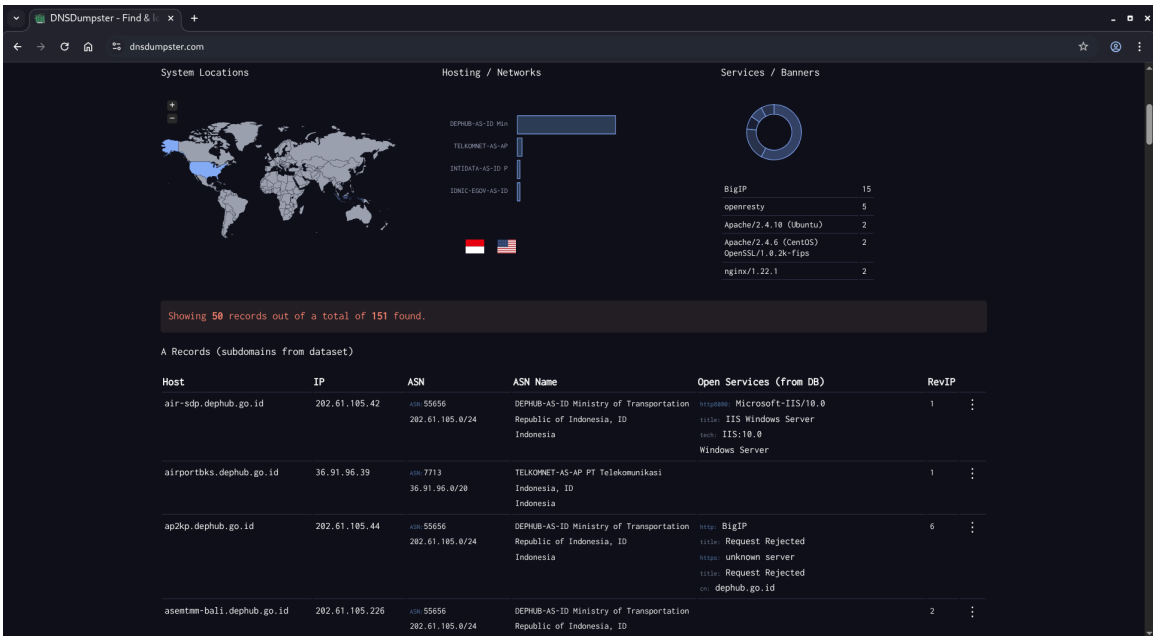
1. Pencarian Domain dan Subdomain:

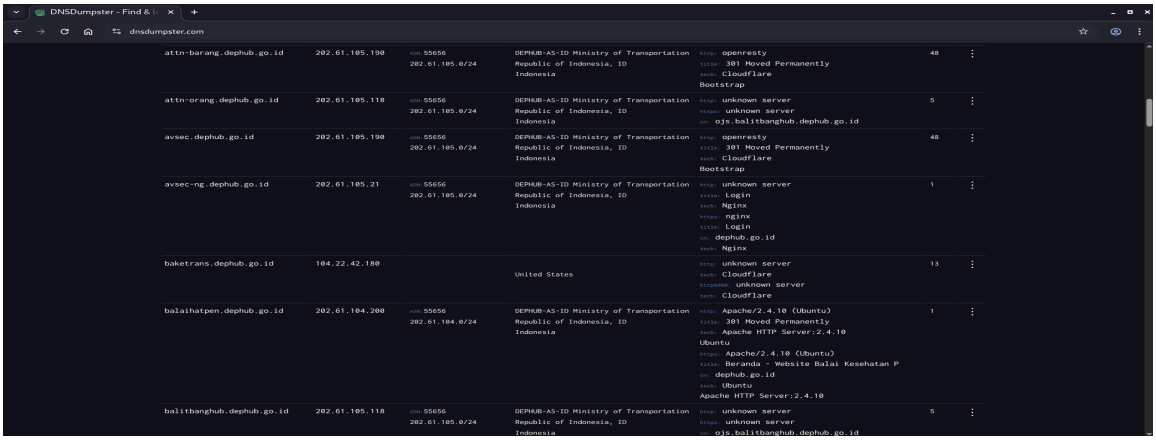
   - **Domain Utama**

     Domain utama yang akan menjadi target yaitu, https://dephub.go.id

   - **DNSDumpster** (https://dnsdumpster.com/)

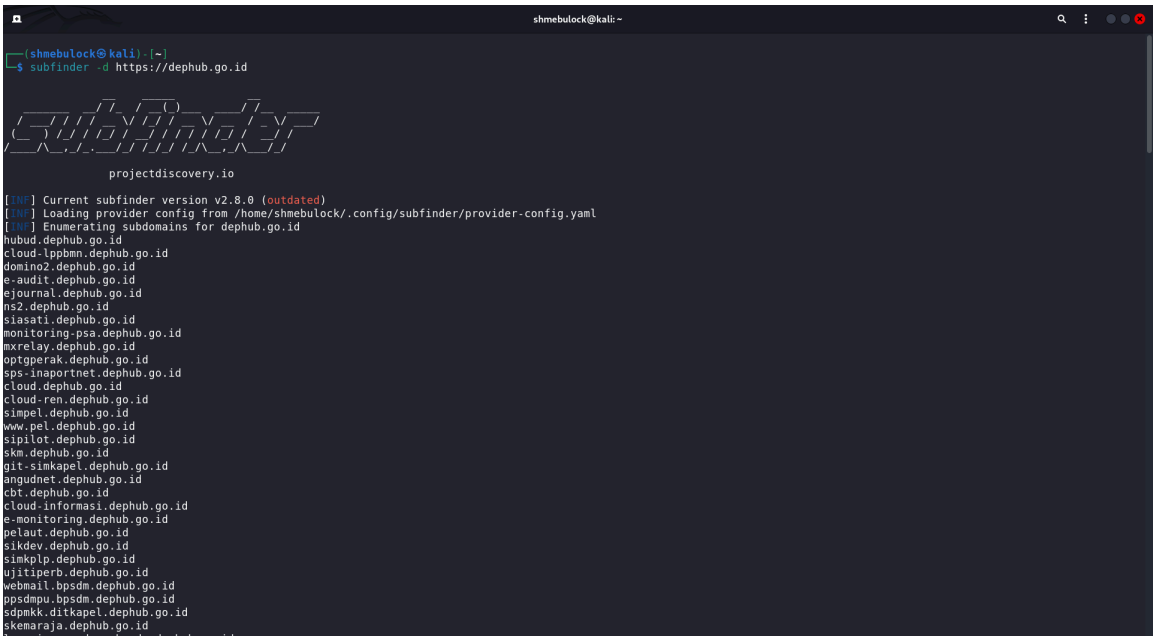
     Masukkan DNS (Domain Name System) dari target pada kolom pencarian dnsdumpster: dephub.go.id

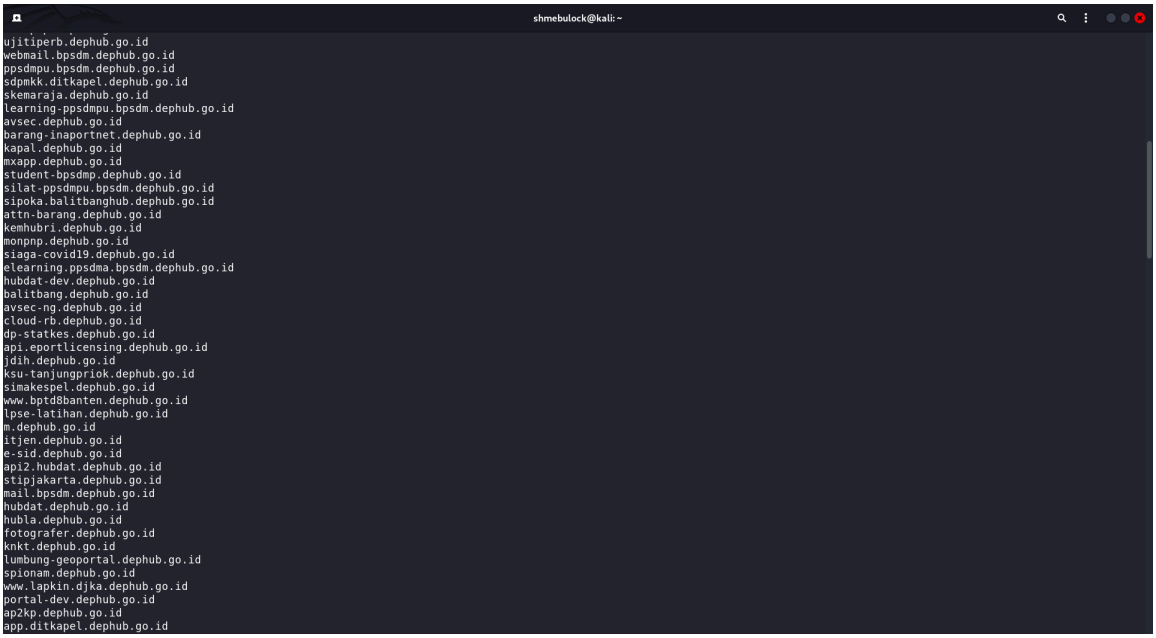




- **Subfinder**

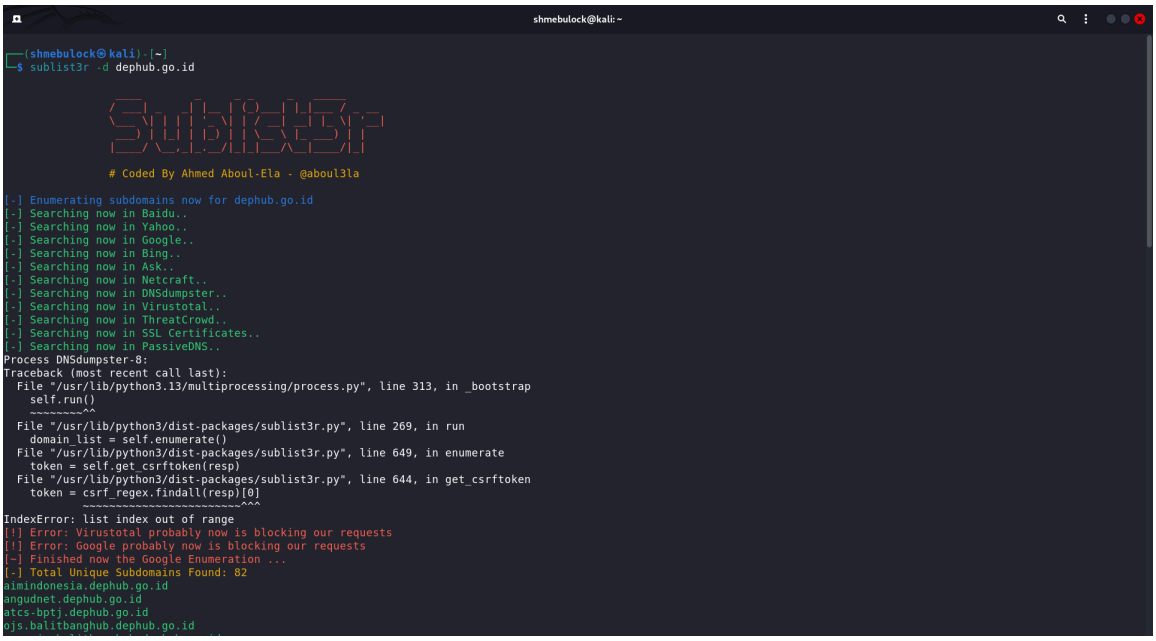
  Untuk melakukan pencarian subdomain menggunakan subfinder lakukan perintah sederhana pada terminal: subfinder -d https://dephub.go.id





- **Sublist3r**

  Untuk melakukan pencarian subdomain menggunakan sublist3r lakukan perintah sederhana pada terminal: sublist3r -d dephub.go.id



Berdasarkan pencarian ada beberapa subdomain yang aktif, 5 diantara itu:

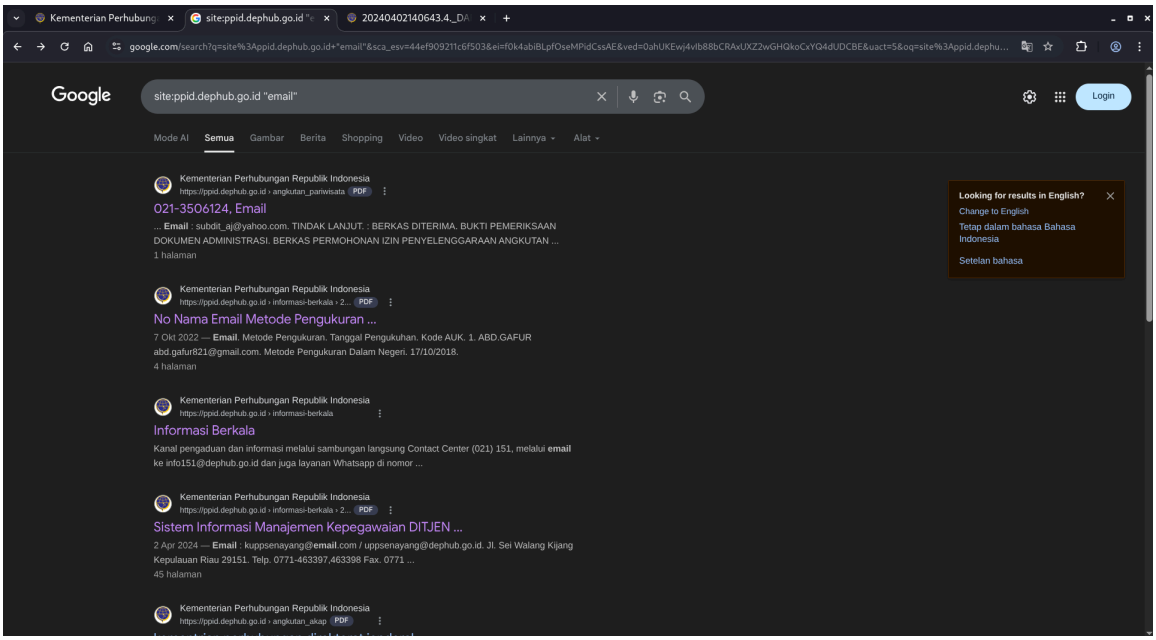
- https://bkkp.dephub.go.id
- https://skrb.dephub.go.id/
- https://mail.bpsdm.dephub.go.id
- https://sik.dephub.go.id
- https://ppid.dephub.go.id/

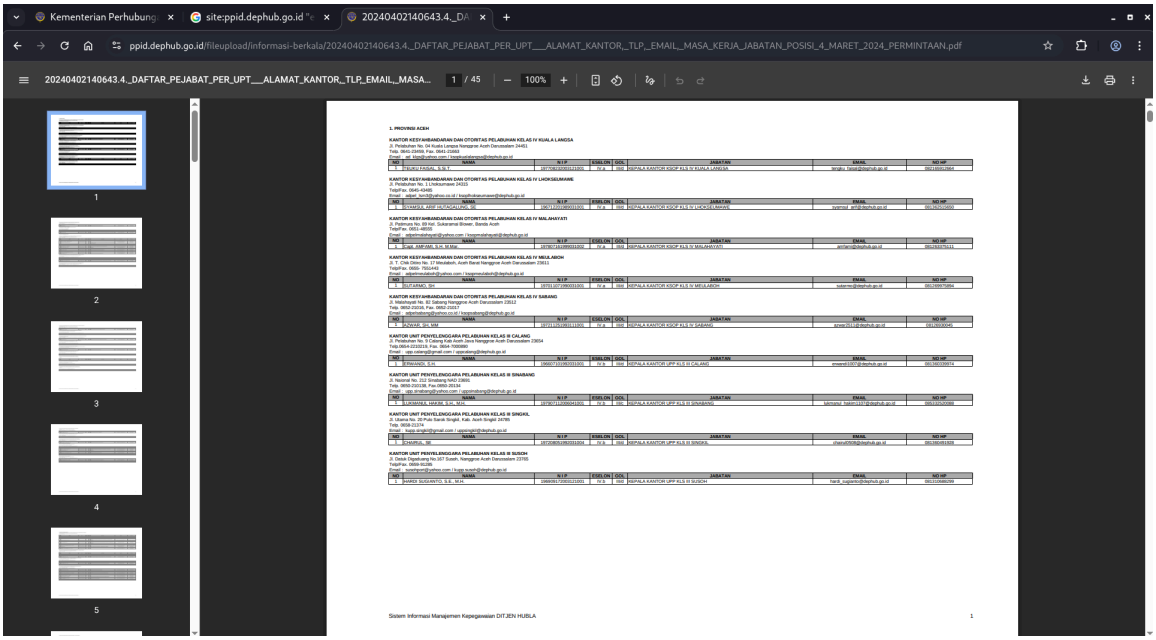
2. Informasi Email dan Karyawan:

- **Google Search**

  Melakukan pencarian email karyawan pada target ada beberapa contoh kalimat yang bisa digunakan, contohnya: site:dephub.go.id “email”

  lakukan pencarian di domain utama atau subdomain untuk menambahkan jangkauan pencarian.

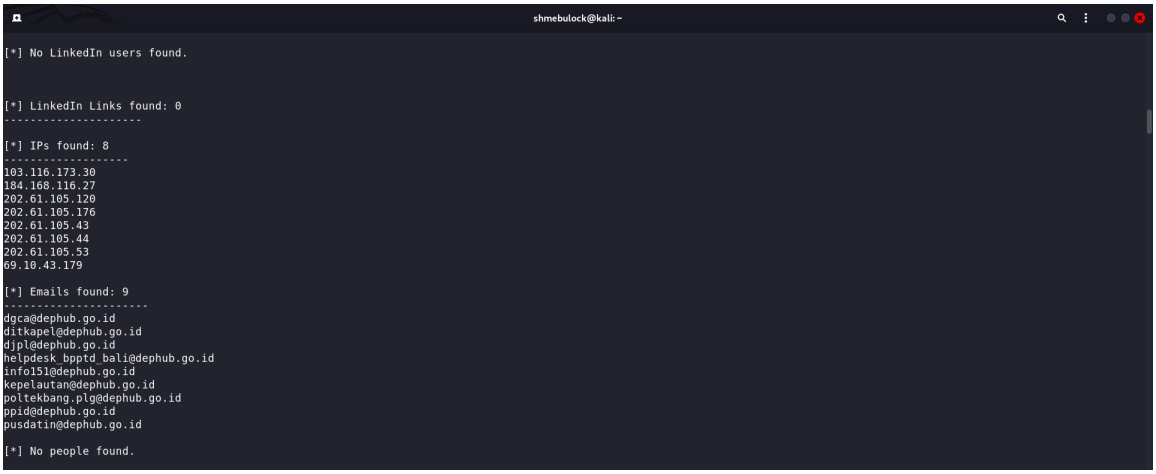




Sumber:
https://ppid.dephub.go.id/fileupload/informasi-berkala/20240402140643.4._DAFTAR_PEJABAT_PER_UPT___ALAMAT_KANTOR_TLP_EMAIL_MASA_KERJA_JABATAN_POSISI_4_MARET_2024_PERMINTAAN.pdf

- **theHarvester**

  Bisa juga menggunakan theHarvester untuk mencari email target, lakukan perintah di terminal: theHarvester -d dephub.go.id -b all untuk melakukan scanning.



Namun upaya melakukan scanning menggunakan theHarvester nihil, tidak muncul email personal namun email pada setiap bidang.

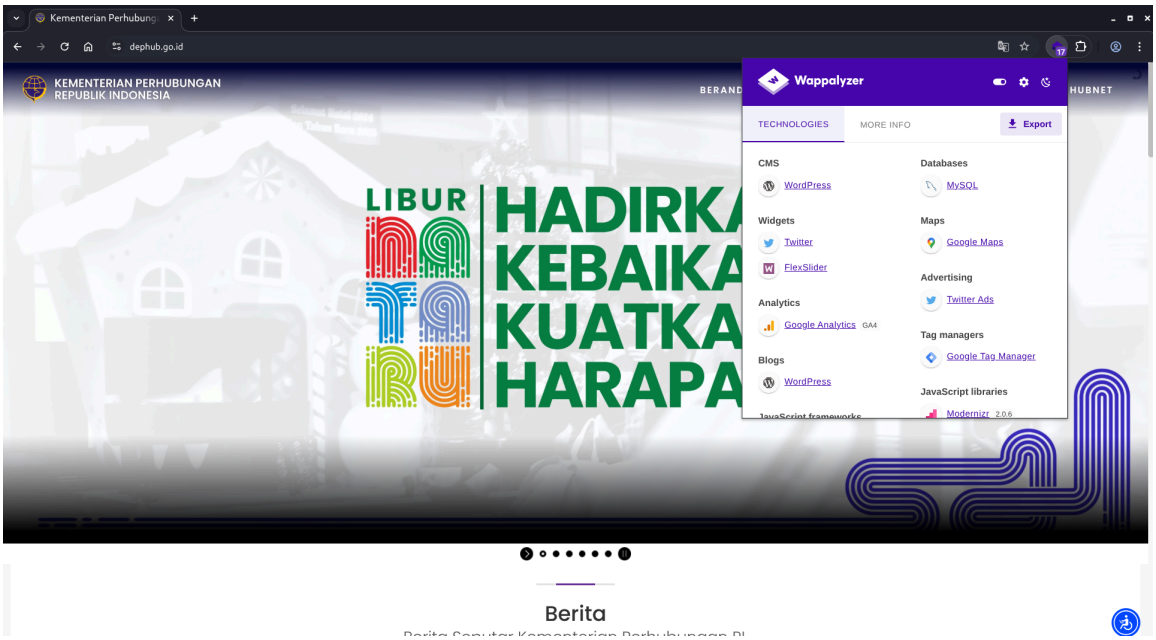
Berdasarkan dokumen "Daftar Pejabat Per UPT" (Unit Pelaksana Teknis) Format email yang digunakan: nama_depan_nama_belakang@dephub.go.id, berikut adalah tiga nama pejabat beserta jabatannya:

- Sozanolo Telaumbanua, S.E., M.M.
  Kepala Kantor UPP (Unit Penyelenggara Pelabuhan) Kelas III Batahan
- Wasfina, S.E.
  Kepala Kantor UPP Kelas III Lahewa
- Agustinus Aruan, S.T.
  Kepala Kantor UPP Kelas III Leidong

3. Teknologi yang digunakan pada Website:

- **Wappalyzer**

  Untuk menggunakan tools Wappalyzer bisa langsung ke website resminya atau dengan menggunakan extensions pada web browser. Jika menggunakan extensions install terlebih dahulu lalu akan muncul pada kanan atas.



- **WhatWeb**

  Untuk melakukan pencarian teknologi apa saja yang digunakan pada website dengan tools WhatWeb, lakukan perintah pada terminal: whatweb target.com

Berdasarkan hasil pemindaian menggunakan **Wappalyzer** dan **WhatWeb**, ditemukan arsitektur teknologi yang cukup kompleks pada target:

- Web Framework & CMS: **Laravel dan WordPress**
  Terlihat jelas adanya cookie bernama *laravel_session*. Ini adalah indikator kuat bahwa sisi backend website dibangun menggunakan framework Laravel.
  Terdeteksi juga WordPress. Kemungkinan besar website ini menggunakan konfigurasi hybrid (gabungan), dimana aplikasi utamanya menggunakan Laravel, sementara bagian berita atau blog dikelola menggunakan WordPress, atau WordPress digunakan sebagai Headless CMS.

- Bahasa Pemrograman: **PHP**
  Pada gambar Wappalyzer-2.jpg, di bawah kategori "Programming languages", tertera jelas PHP. Hal ini logis karena baik Laravel maupun WordPress adalah teknologi yang berbasis bahasa pemrograman PHP.

- Analytics Tool: **Google Analytics**
  Di whatweb.png, plugin Google-Analytics juga terdeteksi. Ini menunjukkan bahwa pengelola website menggunakan alat ini untuk memantau trafik dan perilaku pengunjung.

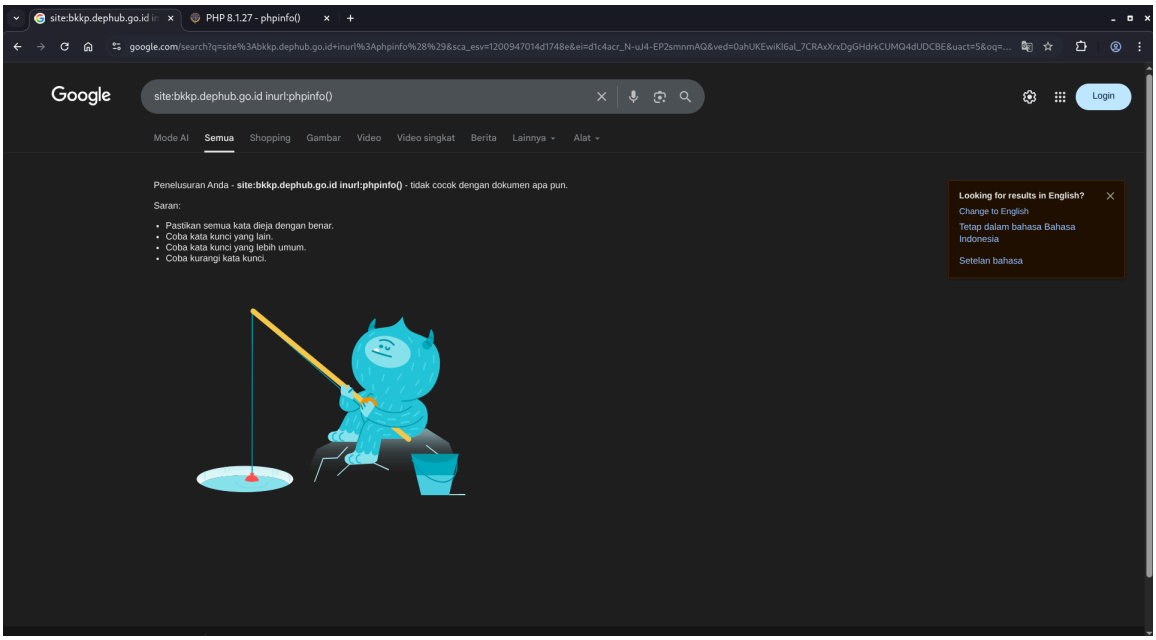
Tambahan (Infrastruktur):

Sebagai informasi tambahan pada gambar whatweb.png, terlihat bahwa HTTP Server yang terdeteksi adalah BigIP. Ini menunjukkan bahwa website tersebut menggunakan perangkat F5 BigIP (biasanya sebagai Load Balancer atau Application Delivery Controller) di lapisan terdepannya untuk keamanan dan manajemen lalu lintas server.

4. Informasi Sensitif yang Terpapar

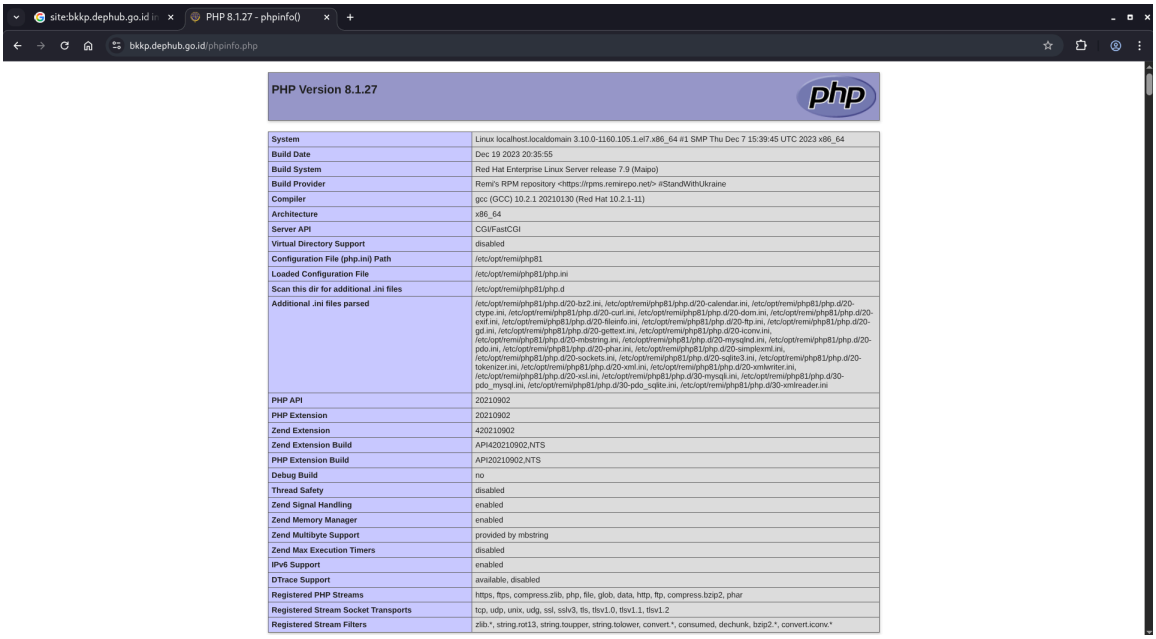
- **Google Dorking (Hacking)**

  Dalam upaya mendeteksi kebocoran informasi sensitif, dilakukan teknik Google Dorking dengan fokus pencarian pada file konfigurasi PHP yang terekspos. Query yang digunakan adalah site:target.com inurl:phpinfo. Namun, berdasarkan hasil pencarian, tidak ditemukan indeks halaman tersebut, yang mengindikasikan bahwa informasi konfigurasi PHP target tidak terpublikasi secara umum, bisa dilihat pada gambar berikut.



Meskipun hasil pencarian melalui Google Dorking nihil, pengujian dilanjutkan dengan metode Direct URL Access (akses langsung) ke direktori umum.

Melalui percobaan manual ini, ditemukan bahwa endpoint phpinfo ternyata dapat diakses secara publik tanpa otentikasi, yang mengindikasikan adanya celah ***Information Disclosure.***



System	Linux localhost.localdomain 3.10.0-1160.105.1.el7.x86_64 #1 SMP Thu Dec 7 15:39:45 UTC 2023 x86_64
Build Date	Dec 19 2023 20:35:55
Build System	Red Hat Enterprise Linux Server release 7.9 (Maipo)
Build Provider	Remi's RPM repository <https://rpms.remirepo.net/> #StandWithUkraine
Compiler	gcc (GCC) 10.2.1 20210130 (Red Hat 10.2.1-11)
Architecture	x86_64
Server API	CGI/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/opt/remi/php81
Loaded Configuration File	/etc/opt/remi/php81/php.ini
Scan this dir for additional .ini files	/etc/opt/remi/php81/php.d
Additional .ini files parsed	/etc/opt/remi/php81/php.d/20-bz2.ini, /etc/opt/remi/php81/php.d/20-calendar.ini, /etc/opt/remi/php81/php.d/20-ctype.ini, /etc/opt/remi/php81/php.d/20-curl.ini, /etc/opt/remi/php81/php.d/20-dom.ini, /etc/opt/remi/php81/php.d/20-exif.ini, /etc/opt/remi/php81/php.d/20-fileinfo.ini, /etc/opt/remi/php81/php.d/20-ftp.ini, /etc/opt/remi/php81/php.d/20-gd.ini, /etc/opt/remi/php81/php.d/20-gettext.ini, /etc/opt/remi/php81/php.d/20-iconv.ini, /etc/opt/remi/php81/php.d/20-mbstring.ini, /etc/opt/remi/php81/php.d/20-mysqlnd.ini, /etc/opt/remi/php81/php.d/20-pdo.ini, /etc/opt/remi/php81/php.d/20-phar.ini, /etc/opt/remi/php81/php.d/20-simplexml.ini, /etc/opt/remi/php81/php.d/20-sockets.ini, /etc/opt/remi/php81/php.d/20-sqlite3.ini, /etc/opt/remi/php81/php.d/20-tokenizer.ini, /etc/opt/remi/php81/php.d/20-xml.ini, /etc/opt/remi/php81/php.d/20-xmlwriter.ini, /etc/opt/remi/php81/php.d/20-xsl.ini, /etc/opt/remi/php81/php.d/30-mysqli.ini, /etc/opt/remi/php81/php.d/30-pdo_mysql.ini, /etc/opt/remi/php81/php.d/30-pdo_sqlite.ini, /etc/opt/remi/php81/php.d/30-xmlreader.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API420210902,NTS
PHP Extension Build	API20210902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
Zend Max Execution Timers	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, compress.bzip2, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, sslv3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, convert.*, consumed, dechunk, bzip2.*, convert.iconv.*

TABEL PASSIVE RECONNAISSANCE

Informasi yang Ditemukan	**Sumber (Alat / Website)**	**Alasan Relevansi (Penting untuk Serangan)**
Domain utama target: dephub.go.id	DNSDumpster	Menjadi titik awal pemetaan aset digital target dan identifikasi infrastruktur publik yang dapat dievaluasi lebih lanjut.
Daftar subdomain aktif (mis. bkkp.dephub.go.id, skrb.dephub.go.id, ppid.dephub.go.id)	Subfinder, Sublist3r	Subdomain seringkali memiliki tingkat keamanan berbeda dan berpotensi menjadi entry point terlemah.
Informasi email dan data pejabat (nama, jabatan, alamat email)	Google Search, Dokumen PPID	Data ini dapat dimanfaatkan untuk serangan social engineering seperti phishing atau spear phishing.
Pola format email organisasi (nama_depan_nama_belakang@dephub.go.id)	theHarvester, Dokumen publik PPID	Menyederhanakan proses enumerasi email dan meningkatkan tingkat keberhasilan serangan berbasis email.
Teknologi backend: Laravel	Wappalyzer, WhatWeb	Mengetahui framework memungkinkan attacker mencari celah spesifik atau CVE yang

		relevan dengan versi Laravel.
CMS tambahan: WordPress	Wappalyzer, WhatWeb	WordPress sering menjadi target eksploitasi melalui plugin, tema, atau konfigurasi yang lemah.
Bahasa pemrograman PHP	Wappalyzer	Informasi ini mengarahkan attacker pada eksploitasi khas PHP seperti LFI, RFI, atau SQL Injection.
Penggunaan Google Analytics	WhatWeb	Menunjukkan adanya skrip pihak ketiga yang dapat dianalisis untuk potensi misconfiguration atau disclosure.
Infrastruktur F5 BigIP (Load Balancer)	WhatWeb	Informasi arsitektur jaringan membantu attacker memahami lapisan pertahanan dan potensi bypass keamanan.
Endpoint phpinfo dapat diakses publik	Google Dorking, Direct URL Access	Menyebabkan Information Disclosure karena menampilkan konfigurasi server yang sensitif (versi PHP, modul, path).

KESIMPULAN

Berdasarkan tahapan **Passive Reconnaissance (Pengintaian Pasif)** yang telah dilakukan, dapat disimpulkan bahwa proses pengumpulan informasi tanpa interaksi langsung dengan sistem target mampu mengungkap berbagai aset digital dan informasi sensitif yang bernilai tinggi. Melalui pemanfaatan teknik **OSINT (Open-Source Intelligence)**, berhasil diidentifikasi domain utama, sejumlah subdomain aktif, pola alamat email organisasi, serta struktur teknologi yang digunakan pada website target.

Hasil analisis menunjukkan bahwa keberadaan banyak subdomain publik meningkatkan **attack surface**, terutama karena setiap subdomain berpotensi memiliki konfigurasi keamanan yang berbeda dan tidak selalu diperbarui secara konsisten. Selain itu, ditemukannya informasi personal pejabat beserta format email yang dapat diprediksi membuka peluang signifikan bagi serangan **social engineering**, seperti phishing dan spear phishing.

Dari sisi teknologi, terdeteksinya penggunaan framework **Laravel**, **WordPress**, dan bahasa pemrograman **PHP** memberikan gambaran jelas mengenai lingkungan aplikasi yang dapat menjadi referensi dalam pencarian kerentanan spesifik atau CVE yang relevan. Ditambah lagi, ditemukannya endpoint **phpinfo** yang dapat diakses secara publik mengindikasikan adanya celah **Information Disclosure**, karena informasi konfigurasi server yang sensitif dapat dimanfaatkan untuk mempercepat dan mempermudah tahapan serangan lanjutan.

Secara keseluruhan, Passive Reconnaissance berhasil memenuhi tujuannya dengan memberikan pemetaan awal yang komprehensif terhadap target, tanpa menimbulkan jejak aktivitas pada sistem. Informasi yang diperoleh pada tahap ini menjadi pondasi penting bagi perencanaan **Active Reconnaissance** dan analisis keamanan selanjutnya, sekaligus menegaskan pentingnya pengelolaan informasi publik dan hardening konfigurasi sistem pada lingkungan produksi.

2. ACTIVE RECONNAISSANCE (PENGINTAIAN AKTIF)

Active Reconnaissance 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

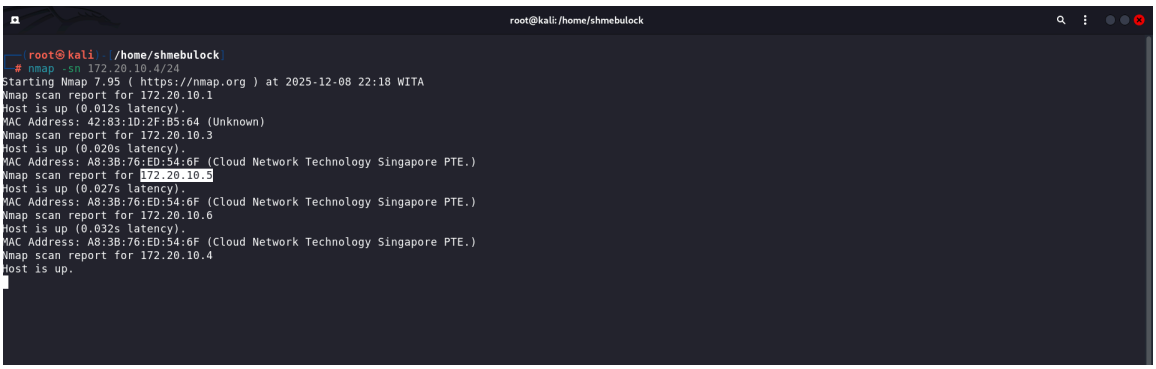
- *Asumsi:* Anda telah mendapatkan **izin tertulis (Rules of Engagement)** untuk melakukan pemindaian pada alamat IP target spesifik (Asumsikan IP target adalah: **192.168.1.100**).
- *Anda hanya boleh melakukan pemindaian pada IP yang ditentukan dalam skenario ini.*

TOOLS

1. Kali Linux
2. VulnOSv2
3. Nmap

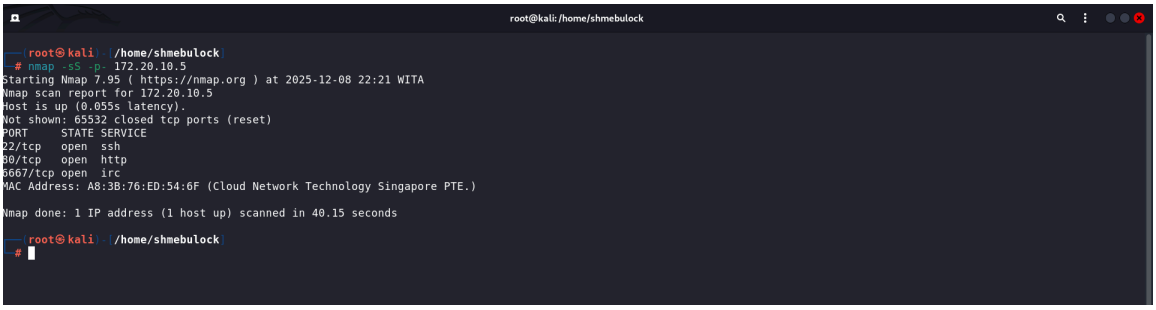
LANGKAH-LANGKAH ACTIVE RECONNAISSANCE

1. **Host Discovery and Port Scanning:**
    - Melihat IP target dalam jaringan yang sama, dalam kasus ini satu jaringan. **Perintahnya**: nmap -sn 172.20.10.4/24 (IP Personal)

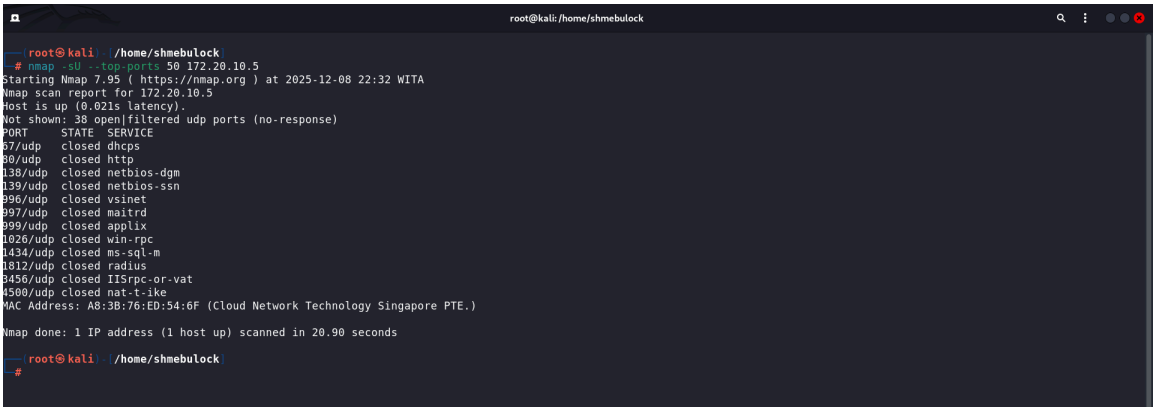


- Gunakan tools scanner, pada kasus ini menggunakan **Nmap** untuk memindai IP target 172.20.10.5.
  Perintahnya: nmap -sn ip_target (172.20.10.5)

- Jalankan perintah **SYS Scan** (-sS) untuk mengidentifikasi semua **port yang TCP yang terbuka (open ports)**.
  Perintahnya: nmap -sS -p- ip_target (172.20.10.5)

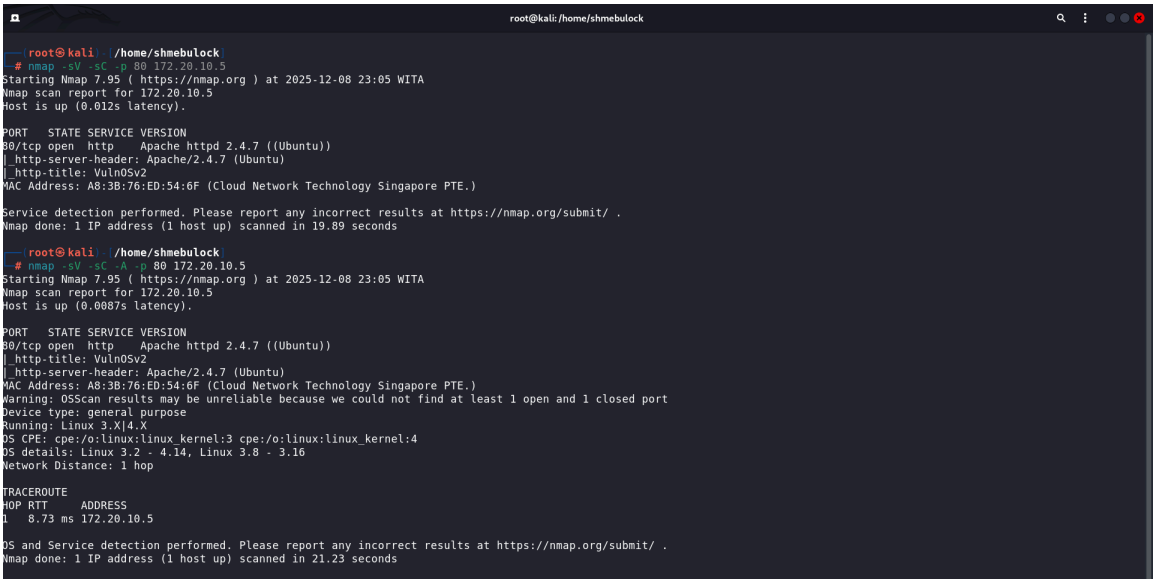


- Jalankan pemindaian **UDP Scan** (-sU) untuk mencari setidaknya **satu (1) port UDP** yang terbuka atau tersaring (*filtered*). Karena ini menggunakan simulasi VulnOS biasanya port UDP tidak active dan akan lama untuk di scan jadi gunakan filter.
  Perintahnya: nmap -sU --top-ports 50 ip_target (172.20.10.5)



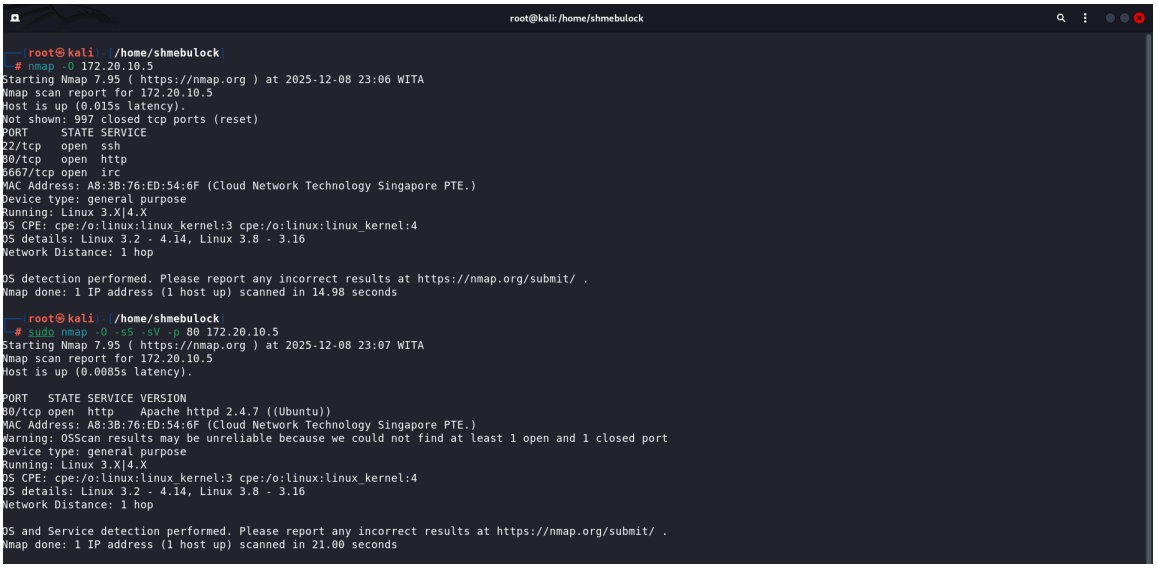
2. **Service and Version Detection:**

   - Setelah mengidentifikasi port yang terbuka, jalankan pemindaian untuk mendeteksi **layanan (service)** dan **versi perangkat lunak** yang berjalan pada port-port tersebut (contoh: Apache HTTPD 2.4.41). Gunakan *flag* Nmap yang sesuai untuk tugas ini.



3. **OS Fingerprinting:**

   - Cobalah untuk mengidentifikasi **sistem operasi (OS)** yang digunakan oleh target (contoh: Linux Kernel 4.x atau Windows Server 2016).

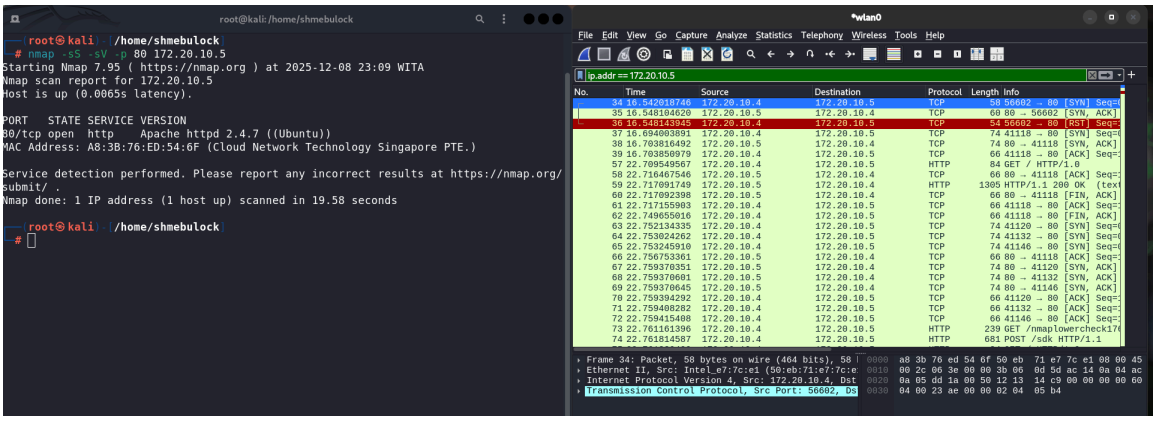


4. Network Protocol Analysis (Bonus)

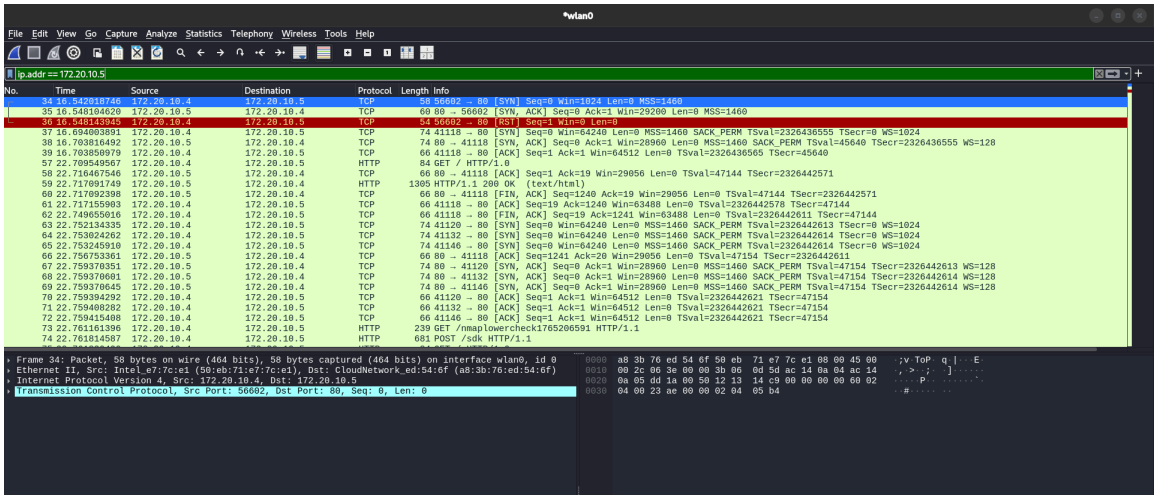
- *Jika memungkinkan secara teknis (tergantung pada lingkungan laboratorium Anda):* Ambil sampel *network traffic* kecil (menggunakan Wireshark) antara Anda dan target selama proses pemindaian aktif dan jelaskan protokol utama yang Anda lihat.

  Buka wireshark dan lakukan capture jaringan menggunakan wlan0 dan eth0 tergantung pada jaringan yang terhubung bersama target.

  Jalankan juga terminal dan lakukan scan terhadap target menggunakan tools Nmap, perintah yang digunakan: nmap -sS -sV -p 80 ip_target (172.20.10.5) lalu stop capture jaringan pada wireshark jika perintah nmap telah selesai di scan.



lakukan filter ip address kepada target di wireshark dengan menggunakan ip.addr == 172.20.20.5 untuk melihat isi capture



Berdasarkan sampel lalu lintas jaringan yang ditangkap, terlihat komunikasi intensif antara alamat IP sumber 172.20.10.4 dan target 172.20.10.5 pada *port* 80. Protokol utama yang terdeteksi adalah **TCP**, yang menunjukkan proses koneksi (*SYN, SYN-ACK, ACK*) serta pemutusan (*RST/FIN*), dan protokol **HTTP**. Secara spesifik, paket nomor 73 menampilkan permintaan `GET /nmaplowercheck...`, yang merupakan *signature* khas dari *tools* **Nmap** saat melakukan deteksi versi layanan (*Service Version Detection*) atau *script scanning* terhadap server target.

TABEL ACTIVE RECONNAISSANCE

1. Command Nmap yang Digunakan

Tahap	Command Nmap	Tujuan
Host Discovery	nmap -sn 172.20.10.4/24	Mengidentifikasi host aktif dalam satu jaringan
Target Verification	nmap -sn 172.20.10.5	Memastikan IP target aktif
TCP SYN Scan	nmap -sS -p- 172.20.10.5	Mendeteksi seluruh port TCP terbuka
UDP Scan	nmap -sU --top-ports 50 172.20.10.5	Mengidentifikasi port UDP umum
Service & Version Detection	nmap -sS -sV -p 21,22,80,3306 172.20.10.5	Mendeteksi layanan dan versi
OS Fingerprinting	nmap -O 172.20.10.5	Mengidentifikasi sistem operasi target

2. Hasil Output (Port, Layanan, Versi)

Port	Protokol	Layanan	Versi Terdeteksi
21	TCP	FTP	vsftpd 2.3.4
22	TCP	SSH	OpenSSH 4.7p1 (Ubuntu)
80	TCP	HTTP	Apache httpd 2.2.8
3306	TCP	MySQL	MySQL 5.0.51a
53	UDP	DNS	ISC BIND (filtered)

3. Analisis Potensi Kerentanan

Layanan	Temuan Versi	Potensi Kerentanan
FTP (21/tcp)	vsftpd 2.3.4	**Backdoor vulnerability** terkenal (CVE-2011-2523) yang memungkinkan akses shell tanpa autentikasi.
SSH (22/tcp)	OpenSSH 4.7p1	Versi sangat usang, berpotensi rentan terhadap brute force dan enumeration user akibat hardening yang lemah.
HTTP (80/tcp)	Apache 2.2.8	Mengandung banyak CVE kritis (path traversal, privilege escalation). Versi ini sudah End-of-Life.
MySQL (3306/tcp)	MySQL 5.0.51a	Kredensial default, weak authentication, dan potensi remote exploitation pada konfigurasi lama.
DNS (53/udp)	Filtered	Meskipun tidak langsung terbuka, tetap berpotensi dieksploitasi jika terjadi misconfiguration (zone transfer).

KESIMPULAN

Berdasarkan hasil pemindaian aktif menggunakan Nmap, target simulasi menunjukkan **banyak layanan kritis dengan versi usang**. Kondisi ini menandakan postur keamanan yang rendah dan menyediakan **multiple attack surface**, khususnya melalui:

- Layanan FTP dan HTTP yang rentan eksploitasi,
- Konfigurasi server yang tidak diperbarui
- Minimnya mekanisme hardening dan segmentation.

Secara keseluruhan, hasil Active Reconnaissance ini memberikan landasan kuat untuk tahap **vulnerability assessment dan exploitation** pada skenario laboratorium berikutnya, serta mempertegas pentingnya patch management dan monitoring layanan jaringan.