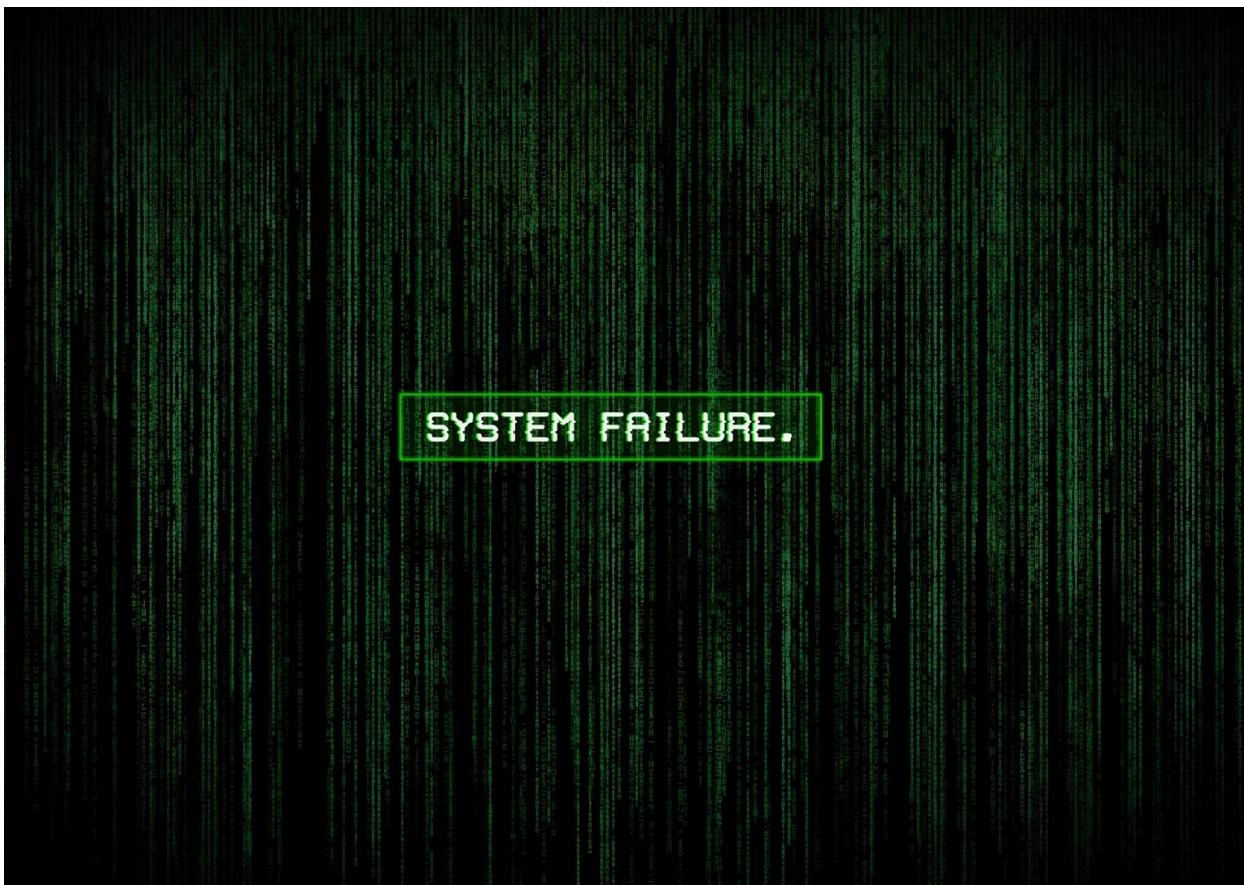


# LAPORAN MID RECONNAISSANCE



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 eksplorasi 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

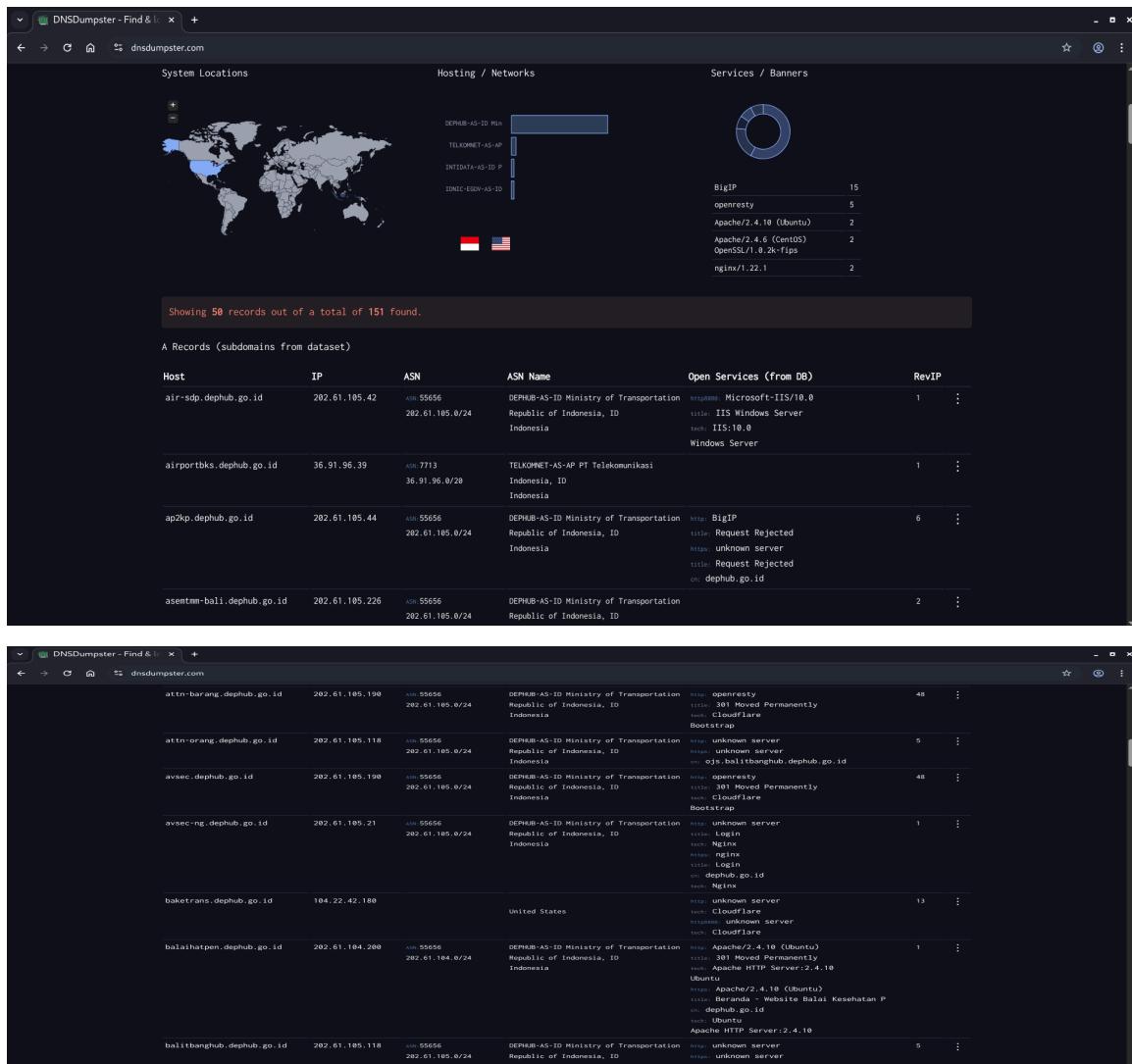
## 1. Pencarian Domain dan Subdomain:

### • Domain Utama

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

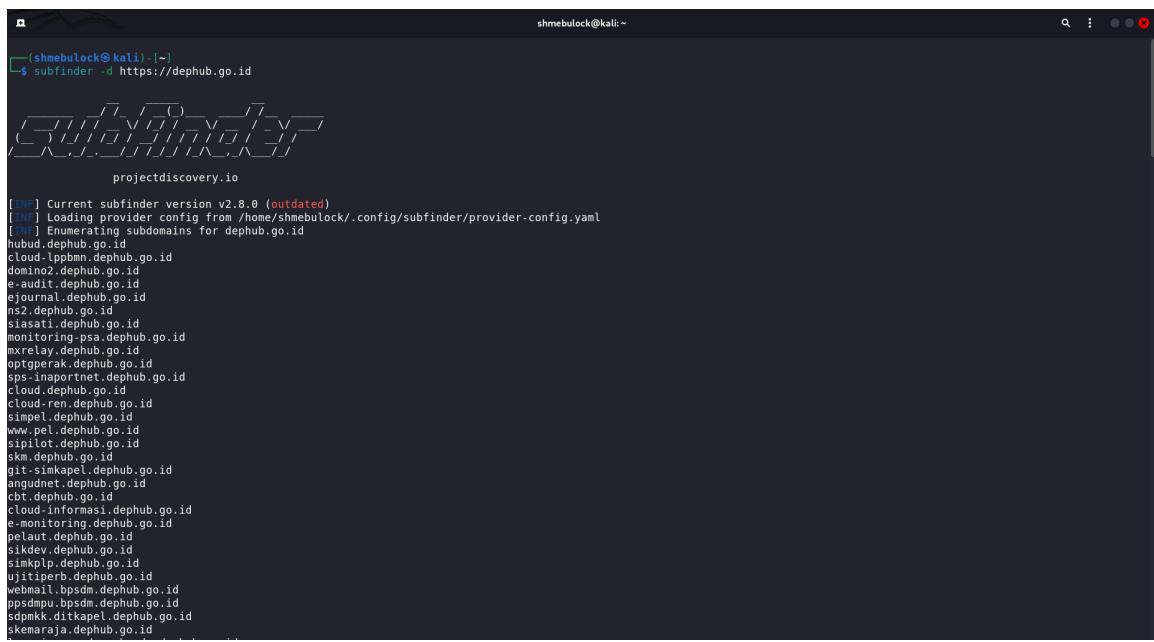
### • DNSDumpster (<https://dnsdumpster.com/>)

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



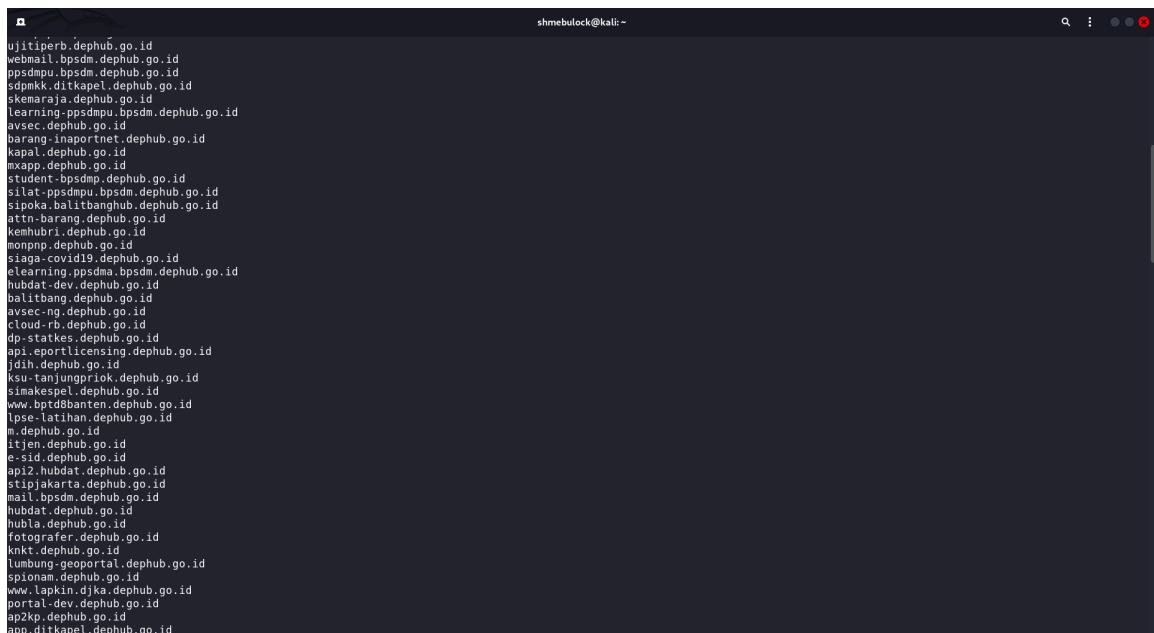
- **Subfinder**

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



```
shmebulock㉿kali:~$ subfinder -d https://dephub.go.id
projectdiscovery.io

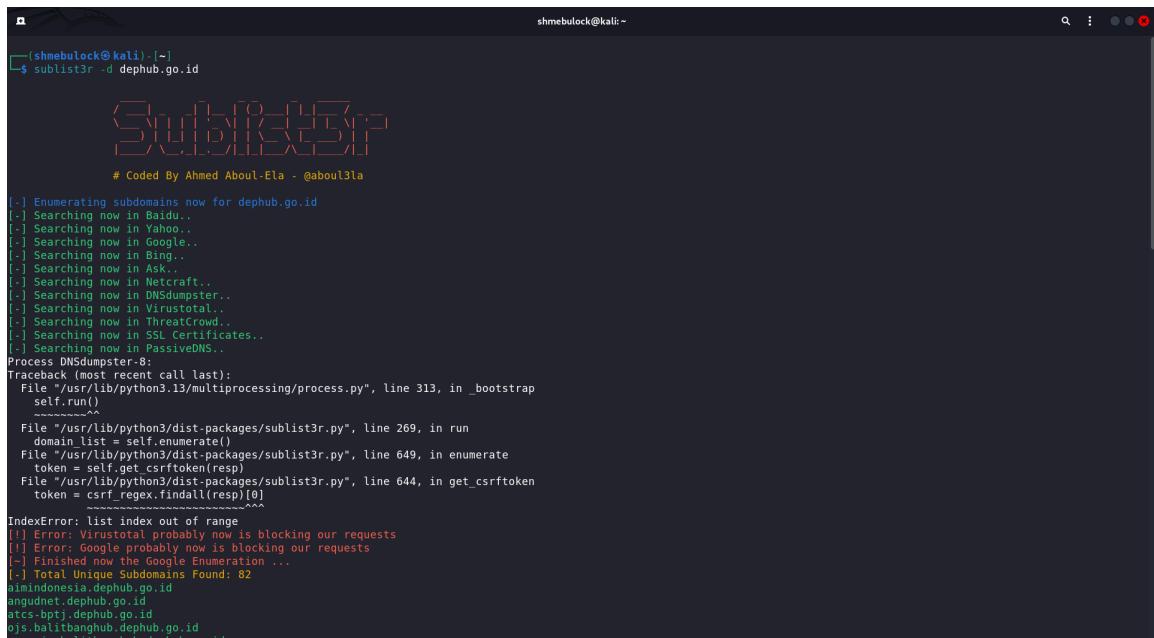
[INFO] Current subfinder version v2.8.0 (outdated)
[INFO] Loading provider config from /home/shmebulock/.config/subfinder/provider-config.yaml
[INFO] Enumerating subdomains for dephub.go.id
hubud.dephub.go.id
cloud-lppmn.dephub.go.id
domino2.dephub.go.id
e-audit.dephub.go.id
ejournal.dephub.go.id
ns2.dephub.go.id
slasati.dephub.go.id
monitoring-psa.dephub.go.id
mxrelay.dephub.go.id
optperak.dephub.go.id
sps-inaportnet.dephub.go.id
cloud.dephub.go.id
cloud-ren.dephub.go.id
simpel.dephub.go.id
www.pel.dephub.go.id
simpot.dephub.go.id
skm.dephub.go.id
git-sikapeli.dephub.go.id
angudnet.dephub.go.id
cbt.dephub.go.id
cloud-informasi.dephub.go.id
e-monitoring.dephub.go.id
pelaut.dephub.go.id
sikdev.dephub.go.id
simkpl.dephub.go.id
ujitiperb.dephub.go.id
webmail.bpsdm.dephub.go.id
bpsdmpu.bpsdm.dephub.go.id
sdpmk.ditkapel.dephub.go.id
skemaraja.dephub.go.id
sikapeli.dephub.go.id
learning.ppsdmpu.bpsdm.dephub.go.id
avsec.dephub.go.id
barang-inaportnet.dephub.go.id
kapal.dephub.go.id
mxapp.dephub.go.id
student-bpsdmp.dephub.go.id
silat-psdmpu.bpsdm.dephub.go.id
sipoka.balitbanghub.dephub.go.id
attn-barang.dephub.go.id
kemhubri.dephub.go.id
monpnp.dephub.go.id
siaga-covid19.dephub.go.id
elearning.ppsdma.bpsdm.dephub.go.id
hubdat-dev.dephub.go.id
balitbang.dephub.go.id
avsec.dephub.go.id
Cloud-rs.dephub.go.id
dp.states.dephub.go.id
api.eportlicensing.dephub.go.id
jidih.dephub.go.id
ksu-tanjungpriok.dephub.go.id
simakespel.dephub.go.id
www.bptdbanten.dephub.go.id
lpse-latihan.dephub.go.id
m.dephub.go.id
itjen.dephub.go.id
e-sid.dephub.go.id
api2.hubdat.dephub.go.id
stipjarkarta.dephub.go.id
mail.bpsdm.dephub.go.id
hubdat.dephub.go.id
hubla.dephub.go.id
fotografer.dephub.go.id
knkt.dephub.go.id
lumbung-deportal.dephub.go.id
spionage.dephub.go.id
www.lapkin.dika.dephub.go.id
portal-dev.dephub.go.id
ap2kp.dephub.go.id
app.ditkapel.dephub.go.id
```



```
ujitiperb.dephub.go.id
webmail.bpsdm.dephub.go.id
bpsdmpu.bpsdm.dephub.go.id
sdpmk.ditkapel.dephub.go.id
skemaraja.dephub.go.id
learning.ppsdmpu.bpsdm.dephub.go.id
avsec.dephub.go.id
barang-inaportnet.dephub.go.id
kapal.dephub.go.id
mxapp.dephub.go.id
student-bpsdmp.dephub.go.id
silat-psdmpu.bpsdm.dephub.go.id
sipoka.balitbanghub.dephub.go.id
attn-barang.dephub.go.id
kemhubri.dephub.go.id
monpnp.dephub.go.id
siaga-covid19.dephub.go.id
elearning.ppsdma.bpsdm.dephub.go.id
hubdat-dev.dephub.go.id
balitbang.dephub.go.id
avsec.dephub.go.id
Cloud-rs.dephub.go.id
dp.states.dephub.go.id
api.eportlicensing.dephub.go.id
jidih.dephub.go.id
ksu-tanjungpriok.dephub.go.id
simakespel.dephub.go.id
www.bptdbanten.dephub.go.id
lpse-latihan.dephub.go.id
m.dephub.go.id
itjen.dephub.go.id
e-sid.dephub.go.id
api2.hubdat.dephub.go.id
stipjarkarta.dephub.go.id
mail.bpsdm.dephub.go.id
hubdat.dephub.go.id
hubla.dephub.go.id
fotografer.dephub.go.id
knkt.dephub.go.id
lumbung-deportal.dephub.go.id
spionage.dephub.go.id
www.lapkin.dika.dephub.go.id
portal-dev.dephub.go.id
ap2kp.dephub.go.id
app.ditkapel.dephub.go.id
```

- **Sublist3r**

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



```
shmebulock@kali:~$ sublist3r -d dephub.go.id
[!] Error: VirusTotal probably now is blocking our requests
[!] Error: Google probably now is blocking our requests
[-] Finished now the Google Enumeration ...
[-] Total Unique Subdomains Found: 82
aimindonesia.dephub.go.id
angudnet.dephub.go.id
atcs-bptj.dephub.go.id
ojs.balitbanghub.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/>

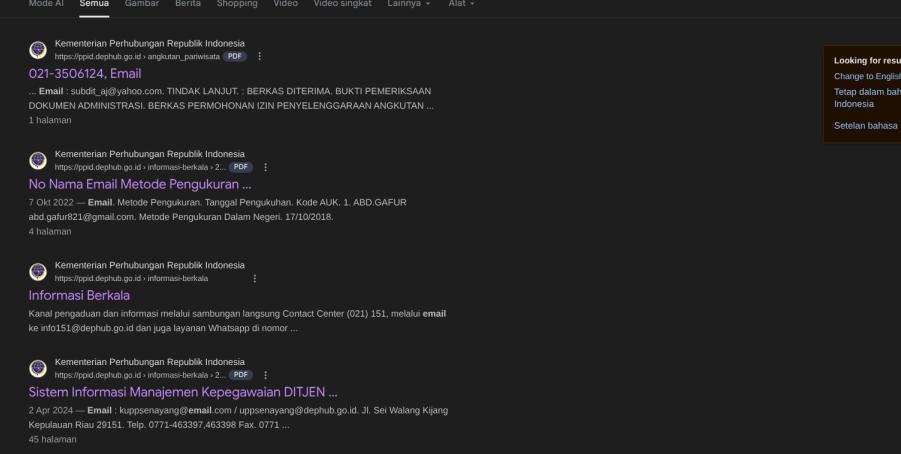
## 2. Informasi Email dan Karyawan:

- **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.

Kementerian Perhubungan x https://ppid.dephub.go.id/x 2024/04/21 14:06:43.4\_D+ +

google.com/search?q=site%3Appid.dephub.go.id+"email"&sa\_csevz=44fe90911c6f503&ei=0f4ab1lpf0seMPdCsAE&ved=0ahUKEwiv4vlb8BtCRAxUXZ2wGHQkoCxYQ4dUDCBE&uact=5&q=site%3Appid.dep... 

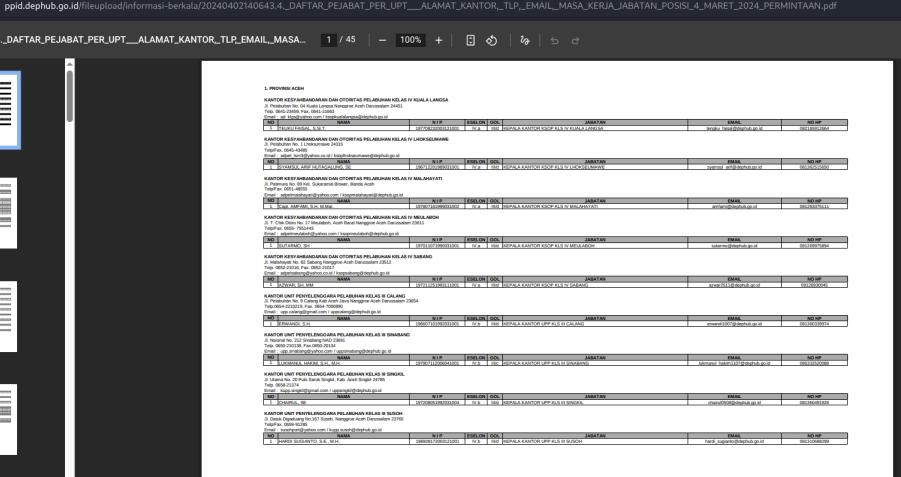
Looking for results in English? Change to English  
Tetap dalam bahasa Bahasa Indonesia Setelan bahasa

Kementerian Perhubungan Republik Indonesia [PDF](https://ppid.dephub.go.id/angkutan_pemintaan.pdf) : 021-3506124, Email ... Email - subdit\_aj@yahoo.com. TINDAK LANJUT : BERKAS DITERIMA. BUKTI PEMERIKSAAN DOKUMEN ADMINISTRASI. BERKAS PERMOHONAN IZIN PENYELENGGARAAN ANGGUTAN ... 1 halaman

Kementerian Perhubungan Republik Indonesia [PDF](https://ppid.dephub.go.id/informasi-berkala_2.pdf) : No Nama Email Metode Pengukuran ... 7 Okt 2022 — Email, Metode Pengukuran, Tanggal Pengukuran, Kode AUK, 1. ABD.GAFUR abd.gafur621@gmail.com. Metode Pengukuran Dalam Negeri, 17/10/2018, 4 halaman

Kementerian Perhubungan Republik Indonesia [PDF](https://ppid.dephub.go.id/informasi-berkala_2.pdf) : Informasi Berkala ... Kanal pengabdian dan informasi melalui sambungan langsung Contact Center (021) 151, melalui email ke info151@deprib.go.id dan juga layanan WhatsApp di nomor ...

Kementerian Perhubungan Republik Indonesia [PDF](https://ppid.dephub.go.id/informasi-berkala_2.pdf) : Sistem Informasi Manajemen Kepegawaian Ditjen ... 2 Apr 2024 — Email: kppusmayang@email.com / uppsmayang@deprib.go.id, Jl. Sei Walang Kijang Kepulauan Riau 29151, Telp. 0771-463397, 463398 Fax. 0771 ... 45 halaman

Kementerian Perhubungan Republik Indonesia [PDF](https://ppid.dephub.go.id/angkutan_akap.pdf) : 

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.

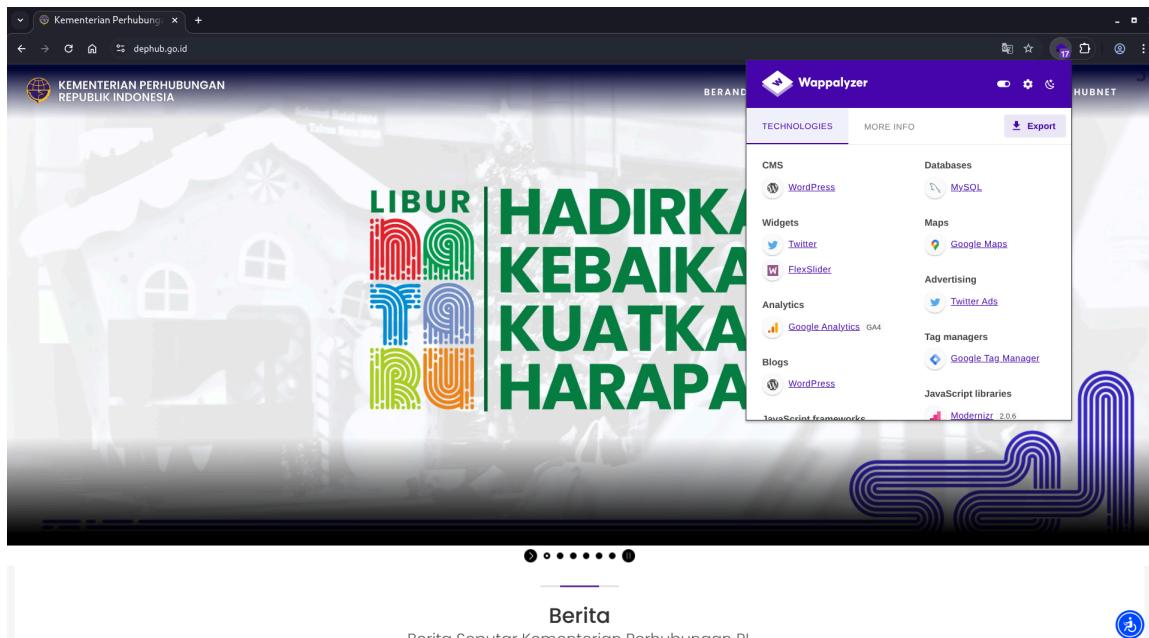
Berdasarkan dokumen "Daftar Pejabat Per UPT" (Unit Pelaksana Teknis) Format email yang digunakan: nama\_depan\_nama\_belakang@dephub.go.id, berikut adalah tiga nama pejabat beserta jabatannya:

- 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

```
shmebulock@kali:~$ whatweb dephub.go.id
http://dephub.go.id [302 Found] Country[INDONESIA][ID], HTTPServer[BigIP], IP[202.61.105.44], RedirectLocation[https://dephub.go.id/]
https://dephub.go.id [200 OK] Bootstrap, Cookies[T501fd17ea,XSRF-TOKEN,laravel_session], Country[INDONESIA][ID], Email[info15@dephub.go.id], Frame, Google-Analytics[Universal], HTML5, HttpOnly[laravel_session], IP[202.61.105.44], JQuery[3.6.0], Laravel, Modernizr, Script[text/javascript], Title[Kementerian Perhubungan Republik Indonesia], X-UA-Compatible[IE=edge]
https://dephub.go.id/ [200 OK] Bootstrap, Cookies[T501fd17ea,XSRF-TOKEN,laravel_session], Country[INDONESIA][ID], Email[info15@dephub.go.id], Frame, Google-Analytics[Universal], HTML5, HttpOnly[laravel_session], IP[202.61.105.44], JQuery[3.6.0], Laravel, Modernizr, Script[text/javascript], Title[Kementerian Perhubungan Republik Indonesia], X-UA-Compatible[IE=edge]
(shmebulock@kali:~$
```

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.

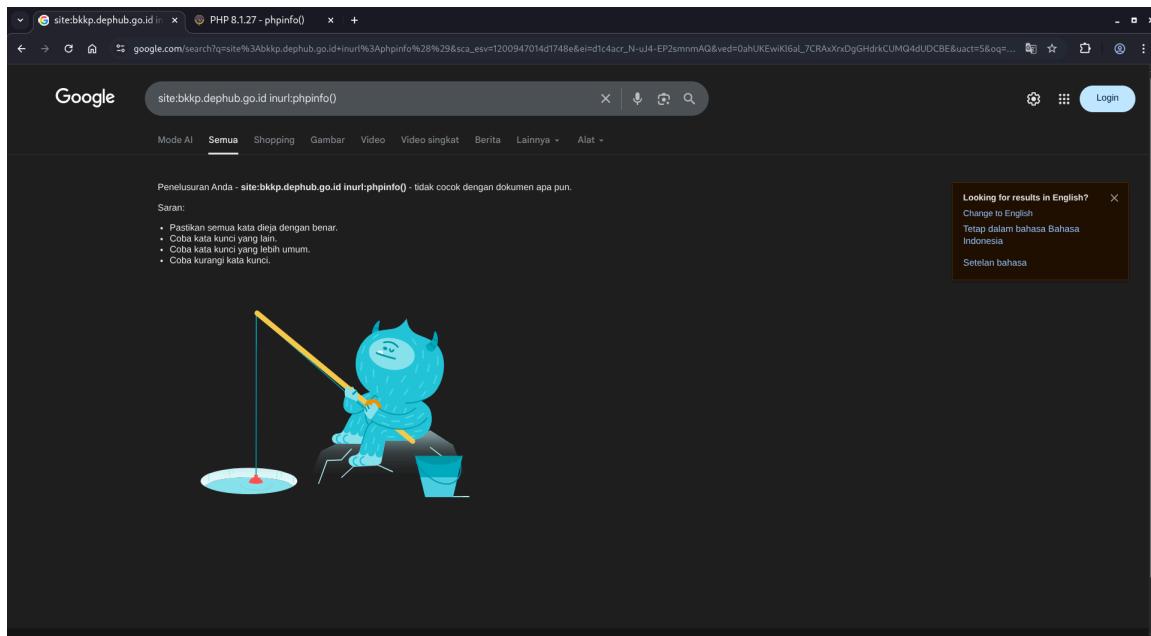
#### **Tambahan (Infrastruktur):**

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***.

The screenshot shows a browser window displaying the `phpinfo()` output for PHP Version 8.1.27. The title bar reads "PHP Version 8.1.27 - phpinfo()". The page content includes a "php" logo at the top right. The main body is a table with various PHP configuration details:

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	Renn's RPM repository <https://rpms.rennp.org/> #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/php
Loaded Configuration File	/etc/opt/remi/php81/php.ini
Scan this dir for additional .ini files	/etc/opt/remi/php81/php.d/20-apc.ini, /etc/opt/remi/php81/php.d/20-calendar.ini, /etc/opt/remi/php81/php.d/20-cgi-zts.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-ext.ini, /etc/opt/remi/php81/php.d/20-fileno.ini, /etc/opt/remi/php81/php.d/20-fp-ini, /etc/opt/remi/php81/php.d/20-gd.ini, /etc/opt/remi/php81/php.d/20-mbstring.ini, /etc/opt/remi/php81/php.d/20-mysqli.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-simplenxml.ini, /etc/opt/remi/php81/php.d/20-tokenizer.ini, /etc/opt/remi/php81/php.d/20-wddx.ini, /etc/opt/remi/php81/php.d/20-xmldiff.ini, /etc/opt/remi/php81/php.d/20-xmwriter.ini, /etc/opt/remi/php81/php.d/20-xmlini.ini, /etc/opt/remi/php81/php.d/20-xmlreader.ini
PHP API	20210902
PHP Extension	20210902
Zend Extension	420210902
Zend Extension Build	API/20210902.NTS
PHP Extension Build	API/20210902.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
DTTrace 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, ssh3, tls, tlsv1.0, tlsv1.1, tlsv1.2
Registered Stream Filters	zlib, string.rot13, string.toupper, string.tolower, convert, consumed, dechunk, bzp2, convert.iconv

## TABEL PASSIVE RECONNAISSANCE

<b>Informasi yang Ditemukan</b>	<b>Sumber (Alat / Website)</b>	<b>Alasan Relevansi (Penting untuk Serangan)</b>
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.*

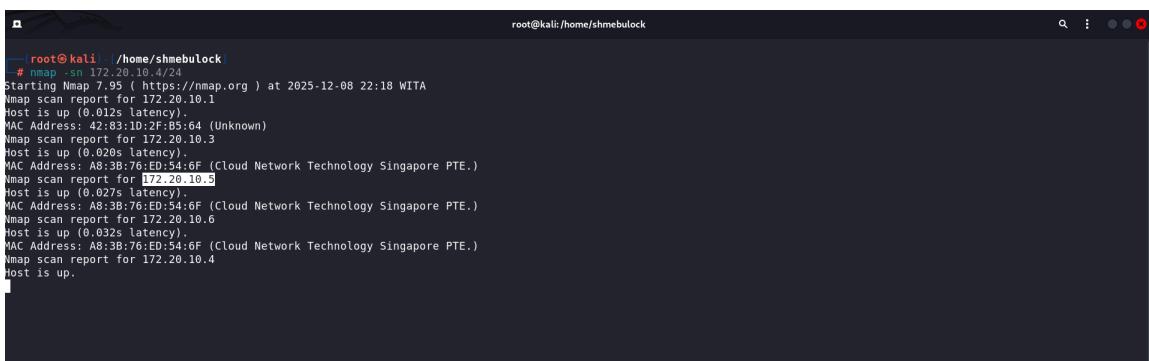
## TOOLS

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)



```
root@kali: /home/shmebulock$ # nmap -sn 172.20.10.4/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 22:18 WITA
Nmap scan report for 172.20.10.1
Host is up (0.012s latency).
MAC Address: 42:82:D0:2F:B5:64 (Unknown)
Nmap scan report for 172.20.10.3
Host is up (0.020s latency).
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Nmap scan report for 172.20.10.5
Host is up (0.027s latency).
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Nmap scan report for 172.20.10.6
Host is up (0.032s latency).
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Nmap scan report for 172.20.10.4
Host is up.
```

- 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)

```
root@kali:~/home/shmebulock
# nmap -sn 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 22:20 WITA
Nmap scan report for 172.20.10.5
Host is up (0.11s latency).
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
#
```

- 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)

```
root@kali:~/home/shmebulock
# nmap -sS -p- 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 22:21 WITA
Nmap scan report for 172.20.10.5
Host is up (0.055s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
6667/tcp  open  irc
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Nmap done: 1 IP address (1 host up) scanned in 40.15 seconds
#
```

- 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)

```
root@kali:~/home/shmebulock
# nmap -sU --top-ports 50 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 22:32 WITA
Nmap scan report for 172.20.10.5
Host is up (0.021s latency).
Not shown: 38 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    closed  dns
67/udp    closed  dhcps
80/udp    closed  http
138/udp   closed  netbios-dgm
139/udp   closed  netbios-ssn
996/udp   closed  vsinet
997/udp   closed  maitrd
999/udp   closed  applix
1026/udp  closed  win-rpc
1434/udp  closed  ms-sql-m
1812/udp  closed  radius
3456/udp  closed  IISrpc-or-vat
4500/udp  closed  nat-t-ike
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Nmap done: 1 IP address (1 host up) scanned in 20.90 seconds
#
```

## 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.

```
root@kali:~/home/shmebulock
# nmap -sv -sc -p 80 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 23:05 WITA
Nmap scan report for 172.20.10.5
Host is up (0.012s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: VulnOSv2
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.89 seconds

--- root@kali:~/home/shmebulock
# nmap -sv -sc -A -p 80 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 23:05 WITA
Nmap scan report for 172.20.10.5
Host is up (0.0087s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-title: VulnOSv2
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-favicon: None
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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

TRACEROUTE
HOP RTT      ADDRESS
1  8.73 ms  172.20.10.5

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.23 seconds
```

## 3. OS Fingerprinting:

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

```
root@kali:~/home/shmebulock
# nmap -O -sS -sV -p 80 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 23:06 WITA
Nmap scan report for 172.20.10.5
Host is up (0.015s 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: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
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 14.98 seconds

--- root@kali:~/home/shmebulock
# sudo nmap -O -sS -sV -p 80 172.20.10.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 23:07 WITA
Nmap scan report for 172.20.10.5
Host is up (0.0085s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
MAC Address: A8:3B:76:ED:54:6F (Cloud Network Technology Singapore PTE.)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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

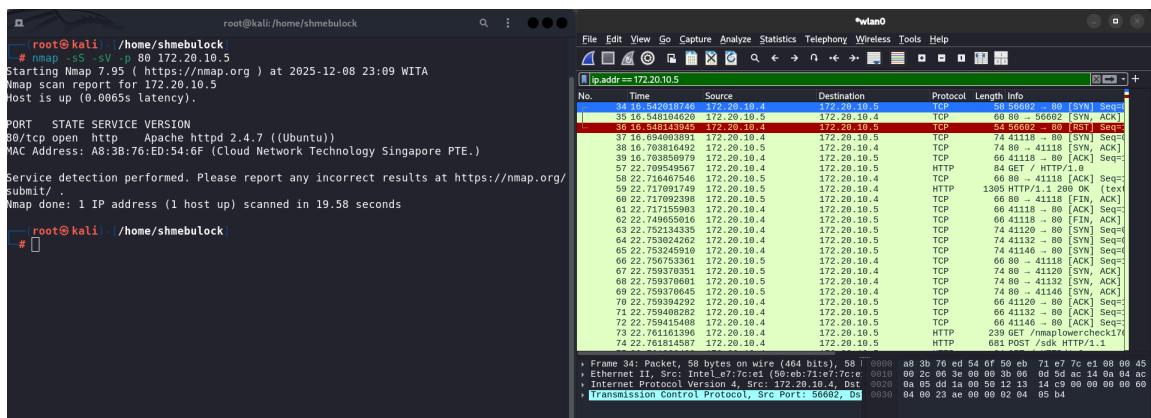
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.00 seconds
```

## 4. Network Protocol Analysis (Bonus)

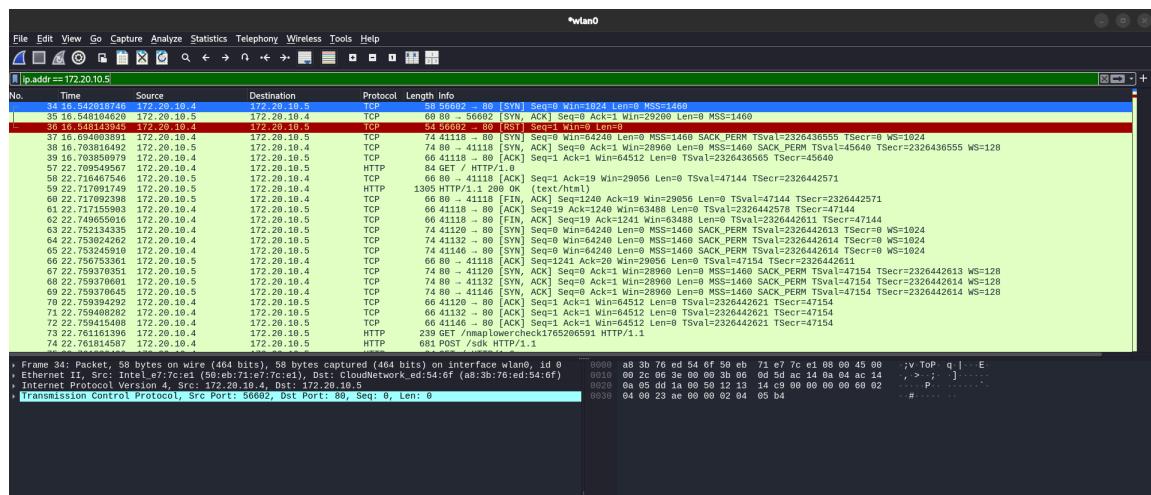
- Jika memungkinkan secara teknis (tergantung pada lingkungan laboratorium Anda): Ambil sampel network traffic kecil (menggunakan Wireshark) antara Anda dan target selama proses pemindaian aktif dan jelaskan protokol utama yang Anda lihat.

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

## 2. Hasil Output (Port, Layanan, Versi)

Port	Protoko l	Layana n	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	<b>Backdoor vulnerability</b> 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 dieksloitasi 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 eksloitasi,
- 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.