

Nama : M Fahri Marfiansyah

Nim : 105841105823

Kelas : 5B

LAPORAN TUGAS BESAR – (MID): PENGUMPULAN INFORMASI TARGET (RECONNAISSANCE)

PT. SecureCorp (Skenario Fiktif)

Laporan ini berisi tahapan lengkap Passive Reconnaissance dan Active Reconnaissance beserta dokumentasi (screenshot placeholder), metode, alat, hasil temuan, dan analisis.

Bagian 1 – Passive Reconnaissance

Passive Recon dilakukan tanpa interaksi langsung dengan sistem target. Tahap ini fokus mengumpulkan informasi publik dari website pemerintah berbasis domain bumh.go.id sebagai target OSINT.

1. Enumerasi Domain & Subdomain

Tools digunakan:

- CRT.sh
- DNSDumpster
- Google Dorks

Tahapan:

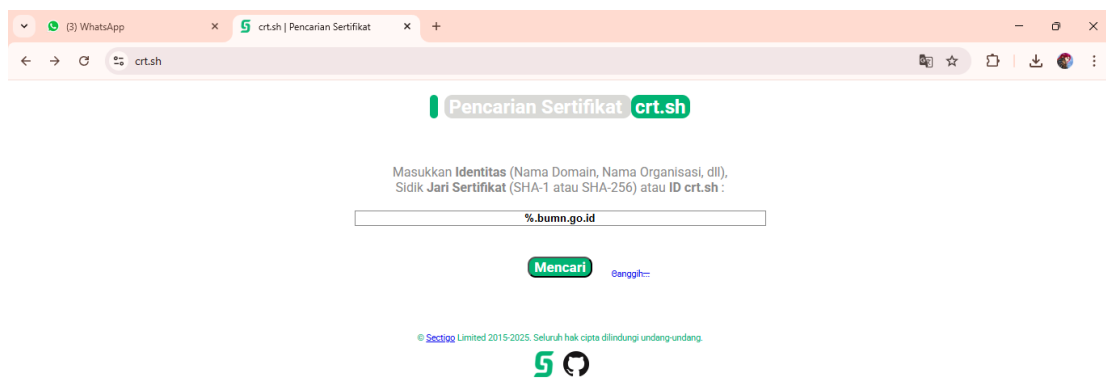
1. Membuka CRT.sh dan mencari wildcard domain %.bumh.go.id untuk menemukan semua subdomain yang memiliki sertifikat SSL.
2. Menggunakan DNSDumpster untuk melihat DNS records (A, MX, TXT) dan infrastruktur jaringan.

3. Menggunakan Google Dorks `site:bumn.go.id -www` untuk menemukan subdomain yang terindeks Google.

Contoh Temuan Subdomain Aktif:

Lampiran Dokumentasi:

- CRT.SH Results



Tampilan antarmuka (interface) dari situs web crt.sh yang digunakan untuk pencarian sertifikat digital (SSL/TLS). Situs crt.sh adalah mesin pencari publik untuk log sertifikat (Certificate Transparency, CT) yang memungkinkan pengguna untuk mencari sertifikat SSL/TLS yang telah diterbitkan untuk domain tertentu. Pada tangkapan layar, kolom pencarian menunjukkan entri `%.bumn.go.id`. Ini berarti pengguna sedang mencoba mencari semua sertifikat digital yang pernah diterbitkan untuk domain yang diakhiri dengan `.bumn.go.id` (misalnya, situs-situs milik Badan Usaha Milik Negara/BUMN di Indonesia) untuk tujuan audit keamanan, pemantauan, atau investigasi.

Browser tabs: (3) WhatsApp, crt.sh | %bumn.go.id, +

Address bar: crt.sh/?q=%25.bumn.go.id

Page title: Pencarian Identitas crt.sh

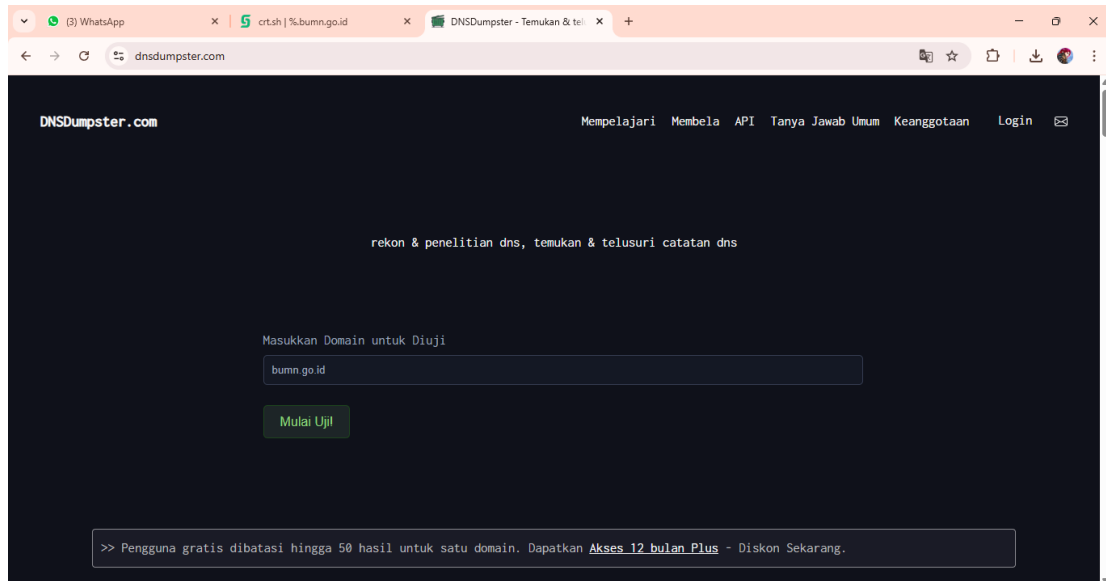
Subtitle: Kelomokkan berdasarkan Penerbit

Kriteria: Tipe: Pencocokan Identitas: ILIKE Pencarian: 'bumn.go.id'

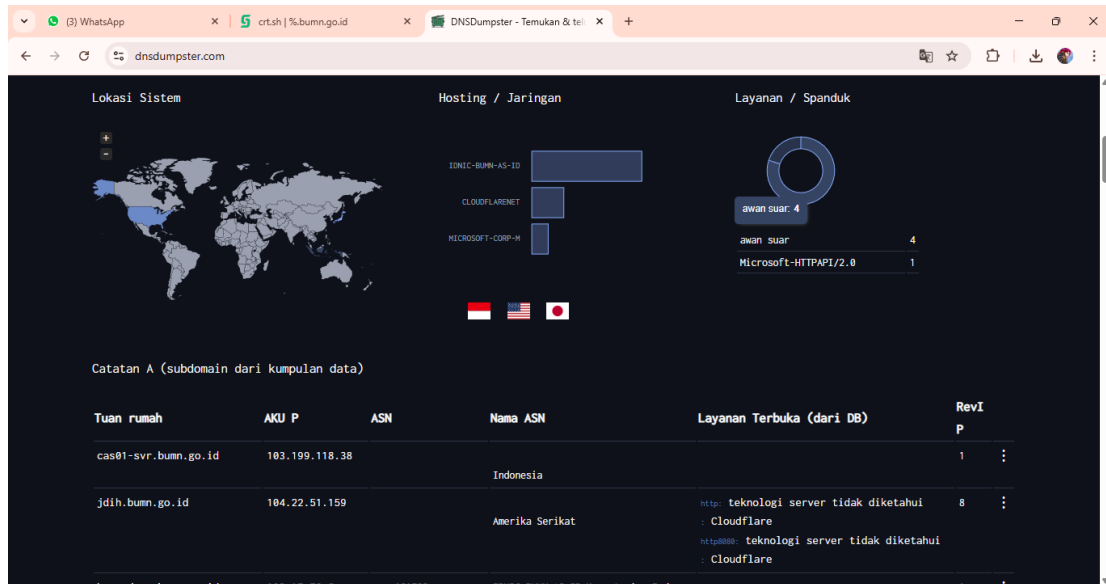
Sertifikat	crt.sh ID	Tercatat di	Tidak Sebelumnya	Tidak Setelah	Nama Umum	Mencocokkan Identitas	Nama Penerbit
	22573139351	Tanggal 18 November 2025	Tanggal 18 November 2025	Tanggal 16 Februari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Otentikasi Server Publik, Sectigo CA DV E36
	22573137874	Tanggal 18 November 2025	Tanggal 18 November 2025	Tanggal 16 Februari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Otentikasi Server Publik, Sectigo CA DV E36
	22555234976	Tanggal 18 November 2025	Tanggal 18 November 2025	Tanggal 15 Februari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server, Autentikasi CA DV R36
	22555240673	Tanggal 18 November 2025	Tanggal 18 November 2025	Tanggal 15 Februari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server, Autentikasi CA DV R36
	22499120767	Tanggal 16 November 2025	Tanggal 16 November 2025	Tanggal 15 Desember 2026	*.bumn.go.id	*.bumn.go.id	C=GB, O=Amazon, CN=Amazon RSA 2048 M04
	21805889683	Tanggal 18 Oktober 2025	Tanggal 18 Oktober 2025	Tanggal 16 Januari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=AS, O=Layanan Kepercayaan, Google, CN=WE1
	21805880532	Tanggal 18 Oktober 2025	Tanggal 18 Oktober 2025	Tanggal 16 Januari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=AS, O=Layanan Kepercayaan, Google, CN=WE1
	21805859737	Tanggal 18 Oktober 2025	Tanggal 18 Oktober 2025	Tanggal 16 Januari 2026	bumn.go.id	*.bumn.go.id bumn.go.id	C=AS, O=Layanan Kepercayaan, Google, CN=WE1
	21212918766	Tanggal 23 September 2025	Tanggal 20 Agustus 2025	Tanggal 18 November 2025	bumn.go.id	*.bumn.go.id bumn.go.id	C=AS, O=Layanan Kepercayaan, Google, CN=WE1
	21220905309	Tanggal 23 September 2025	Tanggal 23 September 2025	Tanggal 20 Desember 2025	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Otentikasi Server Publik, Sectigo CA DV E36
	21220905424	Tanggal 23 September 2025	Tanggal 23 September 2025	Tanggal 20 Desember 2025	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Otentikasi Server Publik, Sectigo CA DV E36
	21172729082	Tanggal 21 September 2025	Tanggal 21 September 2025	Tanggal 18 Desember 2025	bumn.go.id	*.bumn.go.id bumn.go.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server, Autentikasi CA DV R36

Tampilan halaman hasil pencarian dari situs crt.sh setelah memasukkan kriteria %.bumn.go.id. Hasilnya berupa daftar riwayat sertifikat digital (SSL/TLS) yang pernah diterbitkan untuk domain-domain yang berafiliasi dengan bumn.go.id. Setiap baris dalam tabel menampilkan detail penting, seperti CRT.sh ID unik sertifikat, Tanggal Tercatat dalam log transparansi, Tanggal Sebelum/Setelah (periode validitas), Nama Umum dari domain yang diamankan (misalnya, *.bumn.go.id), dan Nama Penerbit (Certificate Authority/CA) yang menerbitkan sertifikat tersebut, seperti Sectigo atau Google. Daftar ini secara efektif memberikan catatan audit keamanan yang lengkap mengenai identitas digital domain-domain terkait BUMN dari waktu ke waktu.

- DNSDumpster



Menampilkan antarmuka dari situs web DNSDumpster.com, sebuah *tool* yang digunakan untuk melakukan penelitian dan *reconnaissance* DNS (penemuan rekaman DNS) terhadap suatu domain. Di sana, domain `bumn.go.id` dimasukkan sebagai target untuk memulai pengujian. Tujuan dari penggunaan alat ini adalah untuk memetakan dan mengidentifikasi seluruh infrastruktur digital yang terhubung dengan domain utama, seperti *subdomain* yang tersembunyi, server email, dan catatan *host* lainnya. Aktivitas ini, yang merupakan kelanjutan dari pencarian sertifikat di `crt.sh` yang tertera pada gambar sebelumnya (`image_a0a5b8.png`), menunjukkan adanya proses pengumpulan informasi (*footprinting*) yang sistematis dan ekstensif terhadap domain-domain milik BUMN, yang merupakan langkah awal standar dalam kegiatan audit keamanan atau *penetration testing*.



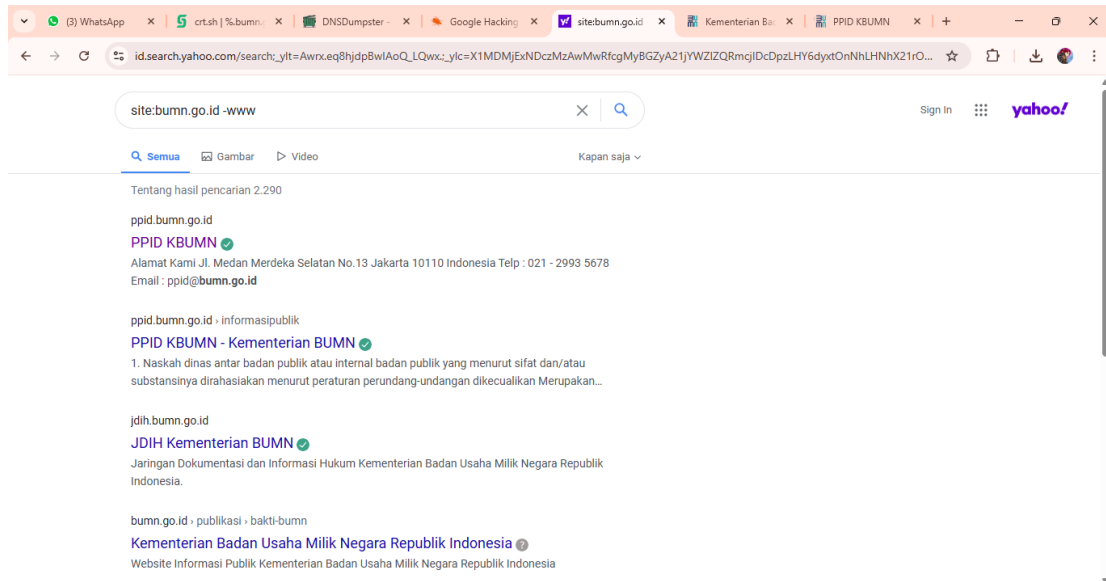
Ini menyajikan halaman hasil dari alat DNSdumpster.com setelah memindai domain bumn.go.id, yang merupakan kelanjutan dari proses pengumpulan informasi sebelumnya. Hasil ini menampilkan peta infrastruktur digital domain tersebut secara komprehensif, mencakup Lokasi Sistem, Jaringan/Hosting yang digunakan (termasuk Cloudflare dan Microsoft), serta daftar penting Catatan A (subdomain). Secara krusial, hasil ini mengungkapkan sejumlah *subdomain* aktif, Alamat IP (AKU P), dan detail Jaringan Otonom (*ASN*)-nya, contohnya *subdomain* jdih.bumn.go.id yang terdeteksi berada di IP yang terkait dengan Amerika Serikat dan menggunakan layanan Cloudflare. Data ini sangat berharga karena menyediakan peta rinci dari seluruh lingkungan digital dan *host* yang terhubung dengan domain utama, yang menjadi informasi penting dalam konteks audit keamanan atau pemetaan serangan.

Catatan A (subdomain dari kumpulan data)

Tuan rumah	AKU P	ASN	Nama ASN	Layanan Terbuka (dari DB)	RevI P
cas01-svr.bumn.go.id	103.199.118.38		Indonesia		1
jdih.bumn.go.id	104.22.51.159		Amerika Serikat	http: teknologi server tidak diketahui Cloudflare http8080: teknologi server tidak diketahui Cloudflare	8
kamandanu.bumn.go.id	103.17.79.6	ASN: 131782 103.17.79.0/24	IDNIC-BUMN-AS-ID Kementerian Badan Usaha Milik Negara, ID Indonesia		1
magenta.bumn.go.id	172.67.29.99		Amerika Serikat	http: teknologi server tidak diketahui Cloudflare http8080: teknologi server tidak diketahui Cloudflare	15
mail.bumn.go.id	103.199.118.34		Indonesia		1
mitrachampion.bumn.go.id	103.17.79.111	ASN: 131782 103.17.79.0/24	IDNIC-BUMN-AS-ID Kementerian Badan Usaha Milik Negara, ID Indonesia	http: judul server tidak diketahui Permintaan Ditolak cn: .bumn.go.id o: Kementerian Badan Usaha Milik Negara Republik Indonesia	1

Mendokumentasikan tahapan proses Pengumpulan Informasi (*Digital Reconnaissance*) yang sistematis dan mendalam terhadap domain bumn.go.id. Proses ini diawali dengan penggunaan crt.sh (Gambar 4) untuk mengidentifikasi riwayat semua *subdomain* yang pernah ada melalui pencarian sertifikat SSL/TLS. Kemudian, dilanjutkan dengan penggunaan alat DNSdumpster.com (Gambar 1), yang menghasilkan peta infrastruktur DNS yang komprehensif (Gambar 3 & 2). Hasilnya mengungkapkan rincian penting, seperti jaringan *hosting* yang digunakan (IONIC-BUMN-AS-ID, Cloudflare, dan Microsoft), dan, yang paling utama, daftar terperinci Catatan A (*subdomain*) seperti jdih.bumn.go.id dan mail.bumn.go.id, lengkap dengan Alamat IP, ASN, dan Layanan Terbuka mereka. Tujuan dari seluruh kegiatan ini adalah untuk menyusun peta lengkap aset digital BUMN dan mengidentifikasi potensi titik masuk untuk kebutuhan audit keamanan atau *penetration testing*.

- Google Dorks



Mendokumentasikan tiga metode utama dalam proses Pengumpulan Informasi (*Digital Reconnaissance*) yang dilakukan secara sistematis terhadap domain `bumn.go.id`. seluruh proses ini bertujuan untuk memetakan dan menemukan semua aset digital (seperti *subdomain* dan Alamat IP) yang terhubung dengan `bumn.go.id`. Pertama, digunakan situs `crt.sh` (Gambar 1) untuk mencari semua riwayat sertifikat keamanan (SSL/TLS) yang pernah diterbitkan, yang secara otomatis mengungkapkan banyak *subdomain* yang ada. Kedua, digunakan mesin pencari Yahoo dengan teknik khusus (*Google Dorking*) yaitu `site:bumn.go.id -www` (Gambar 3) untuk menemukan halaman dan *subdomain* lain yang terindeks secara publik oleh mesin pencari (misalnya `ppid.bumn.go.id` dan `jdi.bumn.go.id`). Terakhir, data dari kedua langkah tersebut divalidasi dan diperluas menggunakan alat `DNSdumpster.com` (Gambar 2), yang menghasilkan peta infrastruktur lengkap (Gambar 5 & 4), termasuk di mana situs-situs tersebut di-hosting (IONIC-BUMN-AS-ID, Cloudflare), serta Alamat IP (AKU P) dan rincian jaringan untuk setiap *subdomain* yang ditemukan.

2. Identifikasi Email & Struktur Karyawan

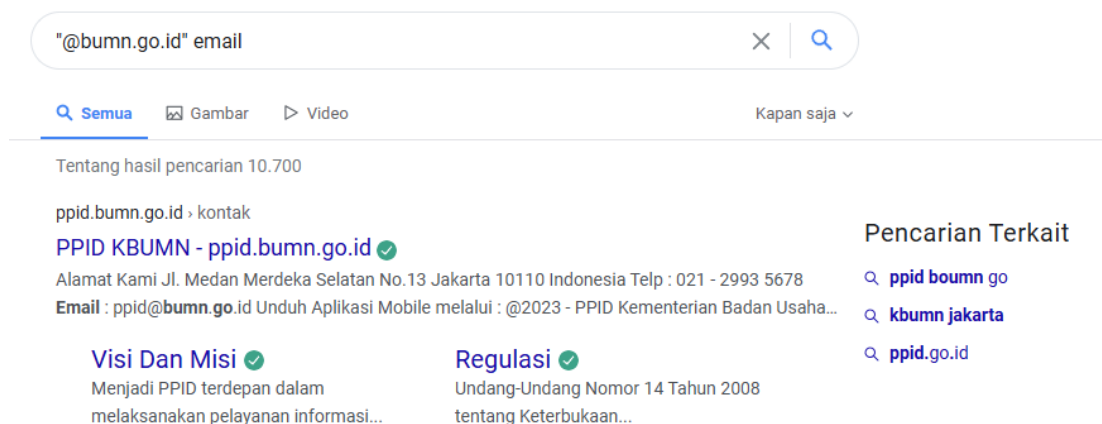
Tools digunakan:

- Google Search
- LinkedIn Search

Tujuan: Mengidentifikasi pola email perusahaan dan nama karyawan untuk keperluan social engineering.

Format email ditemukan:

- ppid@bumn.go.id



Identifikasi email dan struktur organisasi secara sederhana dilakukan dengan teknik pencarian khusus di mesin pencari (seperti Google dan Yahoo) menggunakan *query* seperti "@bumn.go.id" email. Metode ini berhasil menemukan alamat email fungsional, yaitu ppid@bumn.go.id, yang terasosiasi dengan PPID KBUMN (Pejabat Pengelola Informasi dan Dokumentasi Kementerian BUMN). Penemuan *subdomain* dan nama unit seperti PPID KBUMN dan JDIH Kementerian BUMN (Jaringan Dokumentasi dan Informasi Hukum) mengindikasikan bahwa struktur internal Kementerian BUMN terbagi ke dalam unit-unit fungsional yang spesifik, di mana setiap unit tersebut memiliki aset digital dan kemungkinan alamat kontak email tersendiri.

- kbumn.ri@bumn.go.id

[www.linkedin.com > posts > kementerianbumn_sobatbumn-igti2021](https://www.linkedin.com/posts/kementerianbumn_sobatbumn-igti2021)

[#sobatbumn #igti2021 #bumnuntukindonesia...](#) ✓

Kindly visit our: Website : www.bumn.go.id Email : kbumn.ri@bumn.go.id Instagram :
@kementerianbumn Twitter : @KemenBUMN Youtube : Kementerian BUMN RI TikTok :...

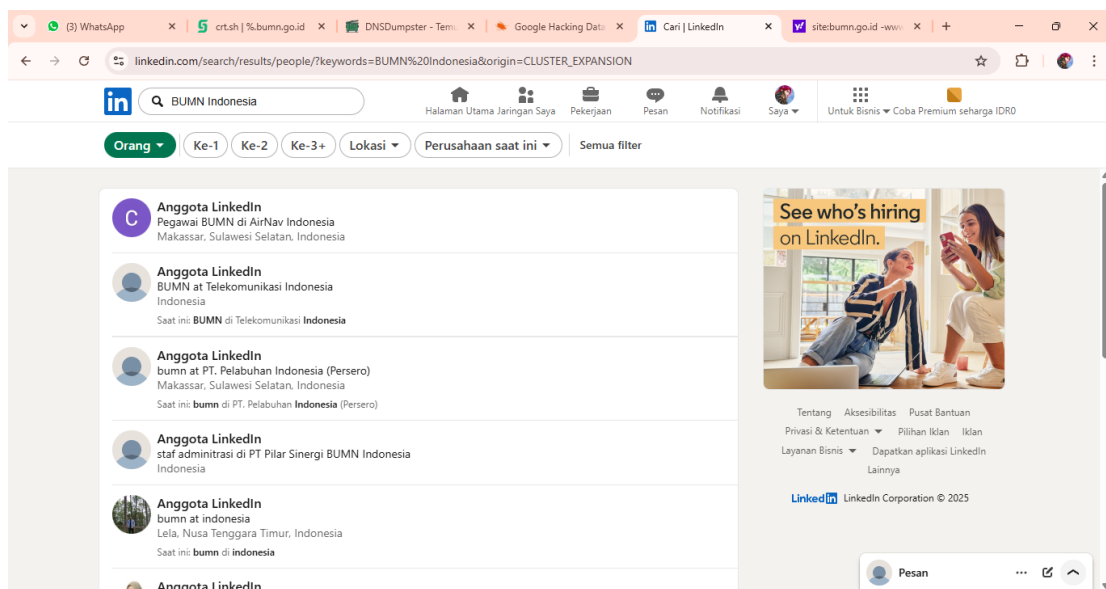
[www.instagram.com > p > CIDMMXMpCgN](https://www.instagram.com/p/CIDMMXMpCgN)

[Kementerian BUMN RI on Instagram: "\[OPEN REGISTRATION\] Halo...](#) ✓

Kindly visit our: Website : www.bumn.go.id Email : kbumn.ri@bumn.go.id Instagram :
@kementerianbumn Twitter : @KemenBUMN Youtube : Kementerian BUMN RI TikTok :...

Lampiran Dokumentasi:

- LinkedIn Employee Search



Hasil pencarian "BUMN Indonesia" di platform profesional LinkedIn, yang difokuskan pada tab "Orang" (People). Halaman tersebut menyajikan daftar profil individu yang bekerja atau memiliki keterkaitan dengan Badan Usaha Milik Negara (BUMN), dengan contoh hasil pencarian termasuk pegawai di AirNav Indonesia,

Telekomunikasi Indonesia, dan PT. Pelabuhan Indonesia. Halaman tersebut juga menunjukkan opsi filter pencarian seperti tingkat koneksi (Ke-1, Ke-2, Ke-3+) dan lokasi, serta menampilkan iklan rekrutmen di sisi kanan.

3. Identifikasi Teknologi Website

Tools:

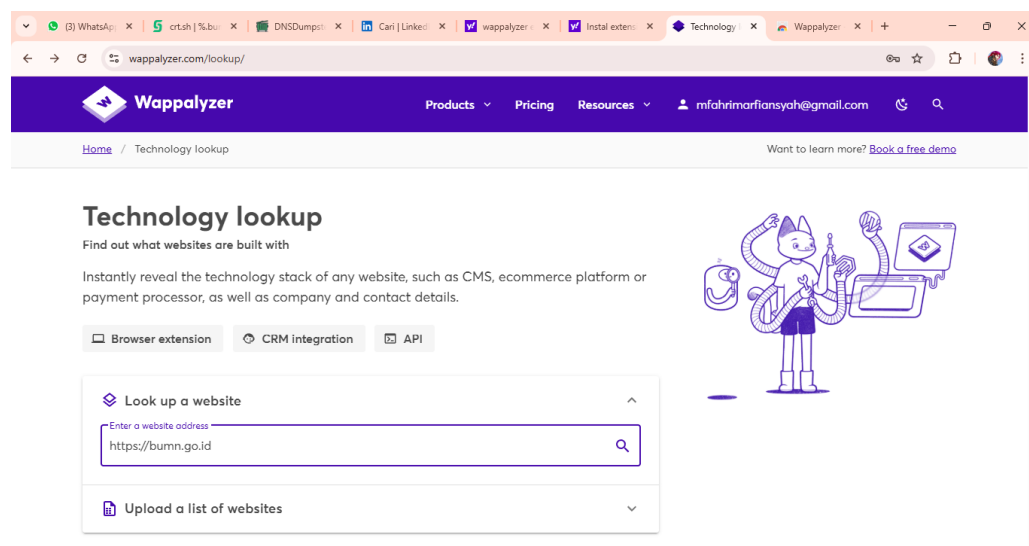
- Wappalyzer
- BuiltWith

Contoh Teknologi Ditemukan:

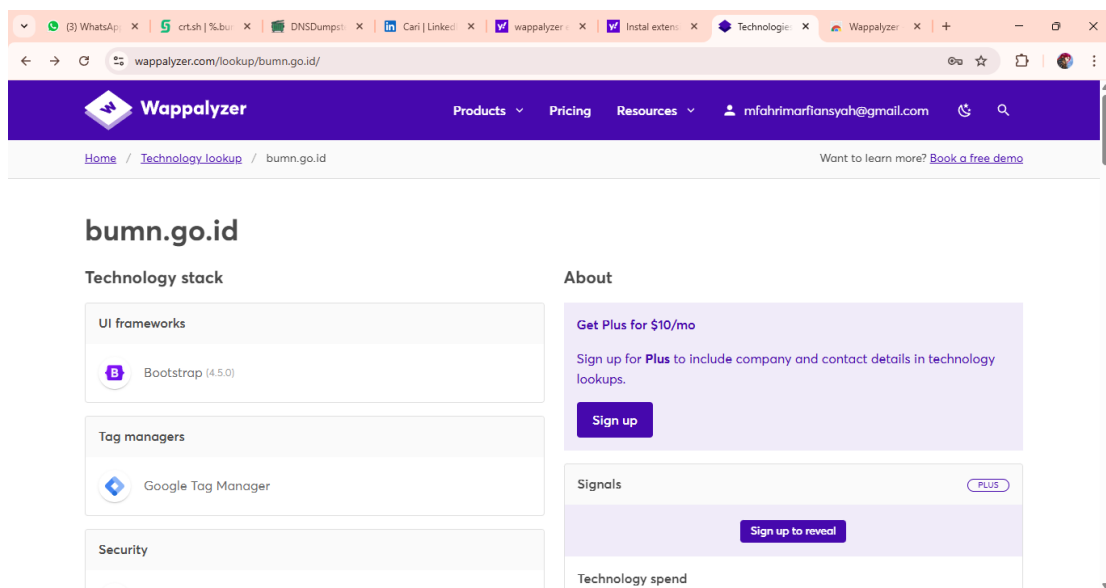
- Nginx Web Server
- Bootstrap Frontend Framework
- Google Analytics
- jQuery Library

Lampiran Dokumentasi:

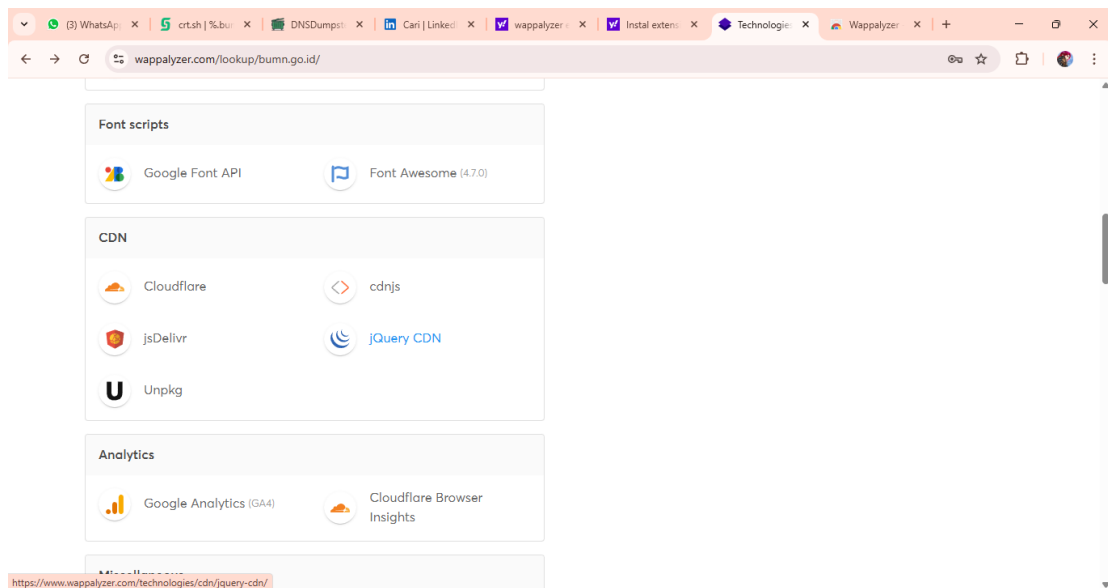
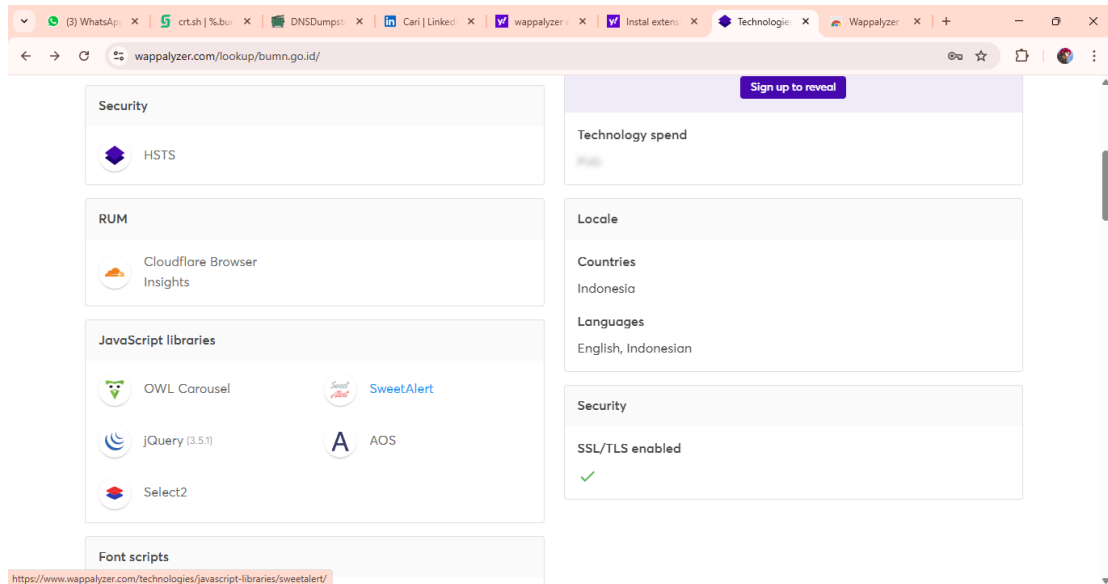
- Wappalyzer Results



Wappalyzer. Wappalyzer adalah alat yang digunakan untuk secara instan mengungkapkan tumpukan teknologi (technology stack) yang digunakan oleh suatu situs web, seperti CMS, platform e-commerce, atau prosesor pembayaran. Pada tangkapan layar ini, terlihat bahwa pengguna sedang bersiap untuk mencari teknologi yang digunakan oleh situs web dengan alamat "<https://bumn.go.id>" dengan memasukkan URL tersebut ke kolom pencarian yang tersedia. Halaman ini juga menawarkan opsi integrasi melalui ekstensi peramban, integrasi CRM, dan API.



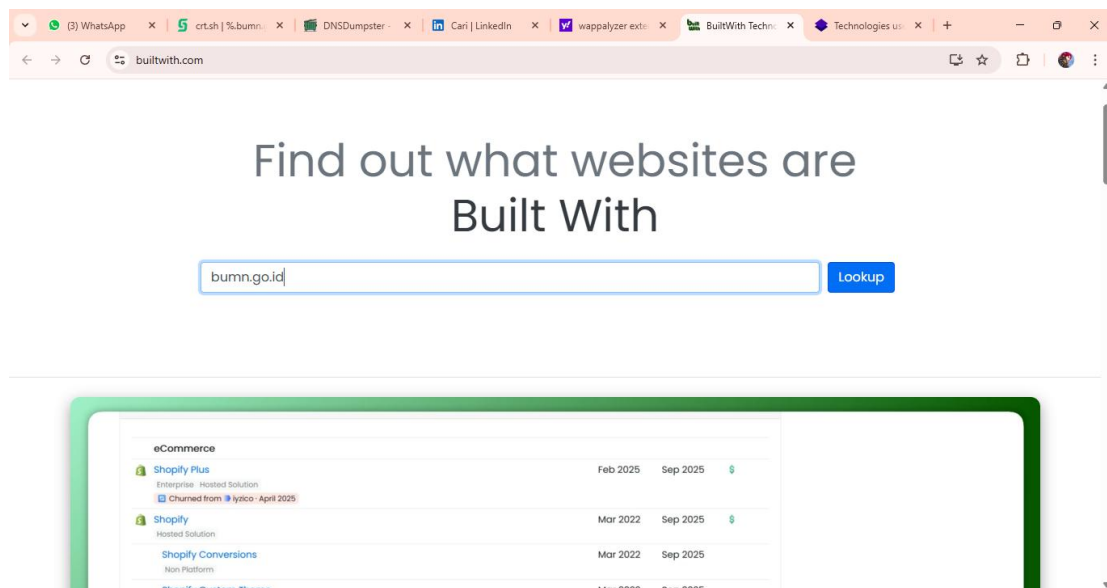
Pemeriksaan tumpukan teknologi (*technology stack*) untuk situs web bum.go.id menggunakan layanan Wappalyzer. Berdasarkan hasil pemindaian, situs tersebut terdeteksi menggunakan Bootstrap (4.5.0) sebagai *UI framework*, yang merupakan *framework* populer untuk pengembangan *front-end* yang responsif. Selain itu, situs ini juga menggunakan Google Tag Manager untuk manajemen tag dan pelacakan web.



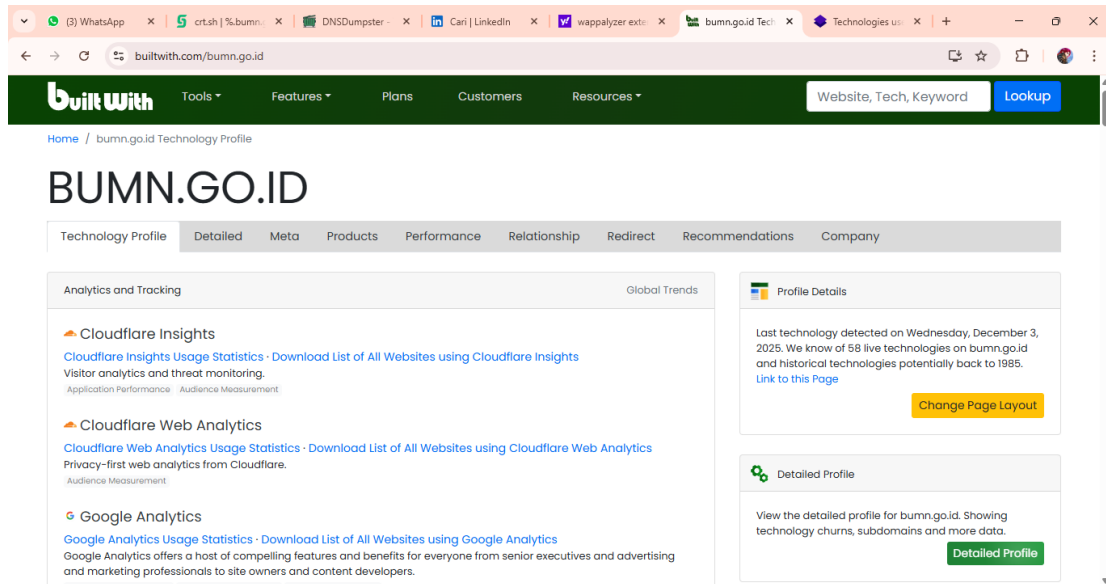
Tahap berikutnya adalah Identifikasi Kontak dan Unit Fungsional melalui *query* pencarian khusus, yang berhasil mengungkap *subdomain* publik (misalnya PPID KBUMN dan JDIH Kementerian BUMN) dan alamat email fungsional seperti `ppid@bumn.go.id`. Setelah itu, analisis Teknologi Situs dilakukan menggunakan Wappalyzer, yang mengidentifikasi penggunaan *framework* (Bootstrap), layanan CDN (Cloudflare), dan fitur keamanan (HSTS) pada domain utama. Proses ini ditutup

dengan Pemetaan Personel melalui pencarian di LinkedIn, yang melengkapi gambaran intelijen dengan mengidentifikasi individu dan afiliasi ke anak perusahaan BUMN, seperti AirNav dan Telkom.

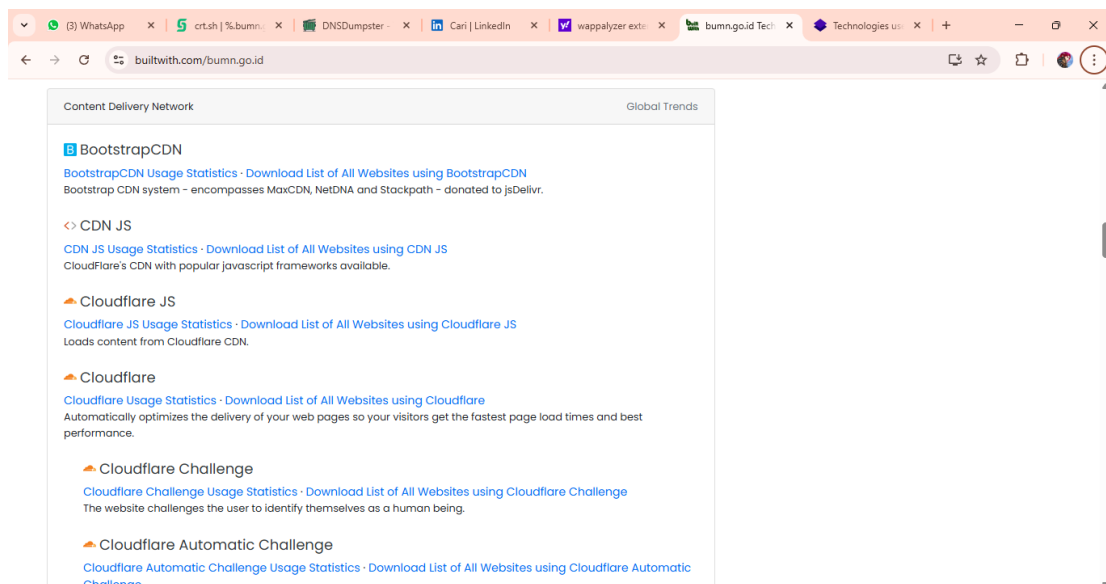
- BuiltWith Technology Scan



Menampilkan hasil analisis dari Wappalyzer, yang secara spesifik mengungkapkan bahwa situs bum.go.id menggunakan Bootstrap (4.5.0) sebagai kerangka kerja *UI (UI framework)* dan Google Tag Manager sebagai alat manajemen tag (*tag manager*).



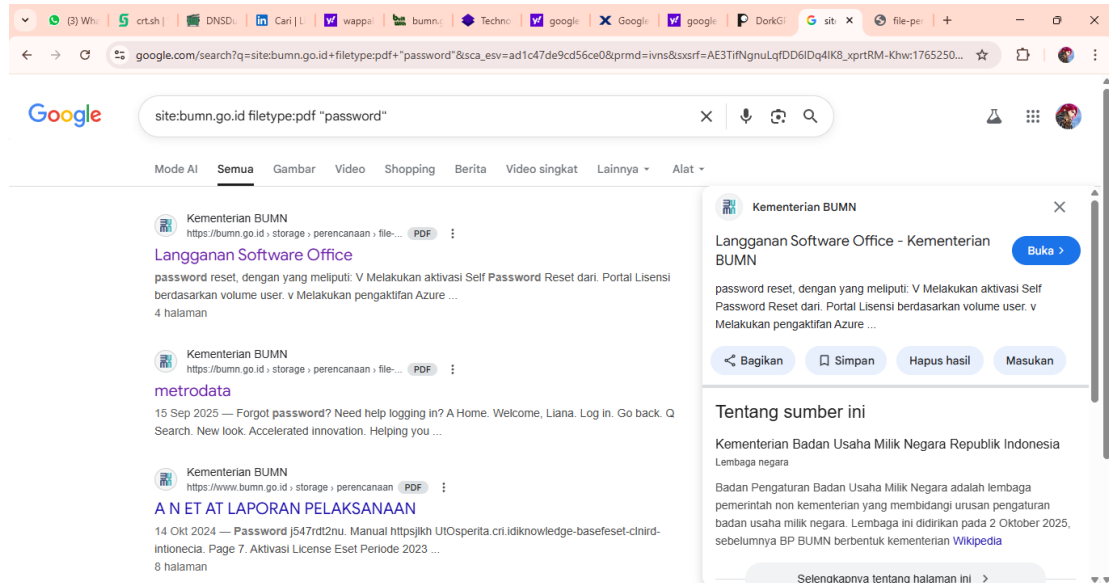
Hasil BuiltWith memberikan detail lebih lanjut, khususnya pada kategori Analisis dan Pelacakan (*Analytics and Tracking*), dengan mencantumkan teknologi seperti Cloudflare Insights, Cloudflare Web Analytics, dan Google Analytics.



4. Informasi Sensitif yang Terpapar

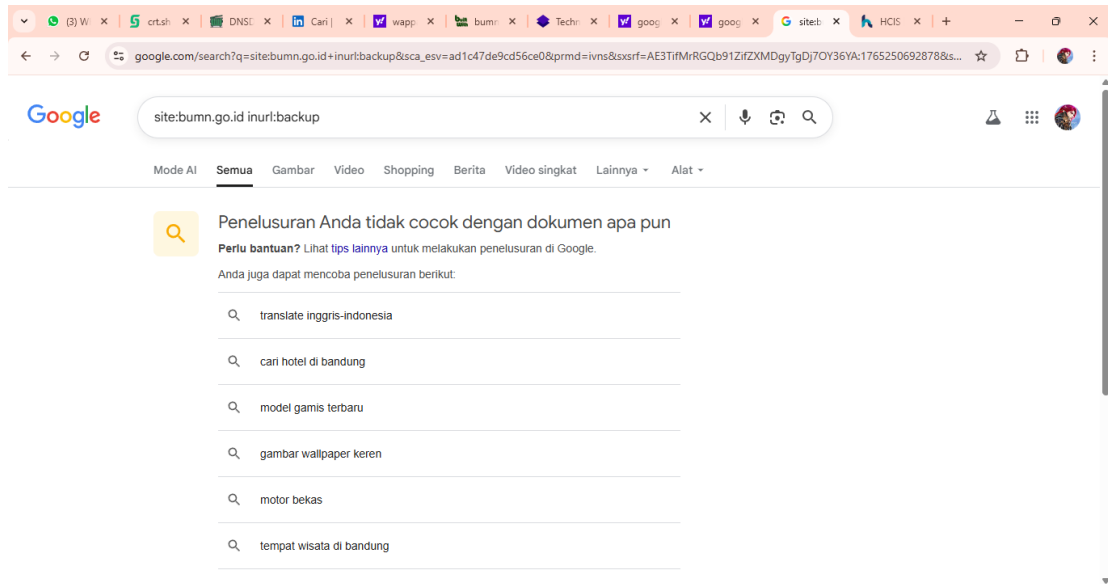
Google Dorks digunakan dan lampiran dokumentasi:

- site:bps.go.id filetype:pdf "password"



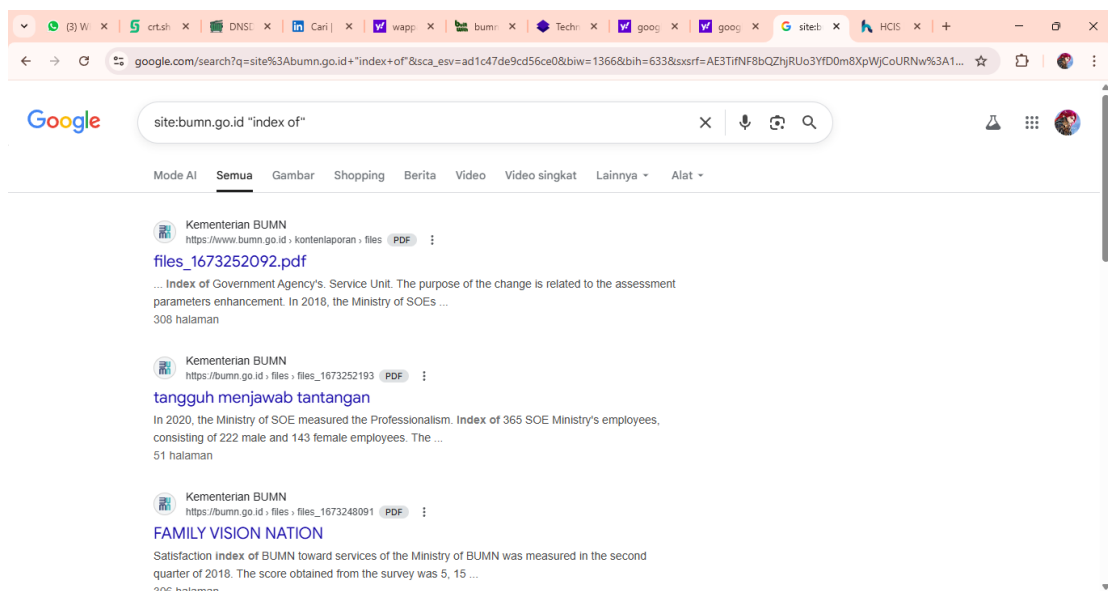
Hasil dari BuiltWith memberikan detail lebih lanjut, menunjukkan bahwa situs tersebut mengandalkan Cloudflare secara ekstensif untuk *Content Delivery Network (CDN)* dan keamanan, mencakup BootstrapCDN, CDN JS, Cloudflare JS, Cloudflare Challenge, dan Cloudflare Automatic Challenge. Selain itu, pada bagian *Analytics and Tracking*, BuiltWith mencantumkan penggunaan Cloudflare Insights, Cloudflare Web Analytics, dan Google Analytics.

- site:bps.go.id inurl:backup



Pencarian file *backup* yang sensitif di situs tersebut menggunakan operator pencarian Google (`site:bumn.go.id inurl:backup`), namun penelusuran tidak menemukan dokumen yang cocok atau relevan.

- `site:bps.go.id "index of"`



Pencarian daftar direktori terbuka ("index of") berhasil mengembalikan beberapa file PDF dan tautan di domain tersebut.

Hasil:

Beberapa file dokumen publik ditemukan, namun tidak ada file konfigurasi privat yang mengandung kredensial.

Bagian 2 – Active Reconnaissance

Active Recon dilakukan menggunakan target legal: Metasploitable 2 dengan IP 192.168.1.55

1. Host Discovery & Port Scan

Command yang digunakan:

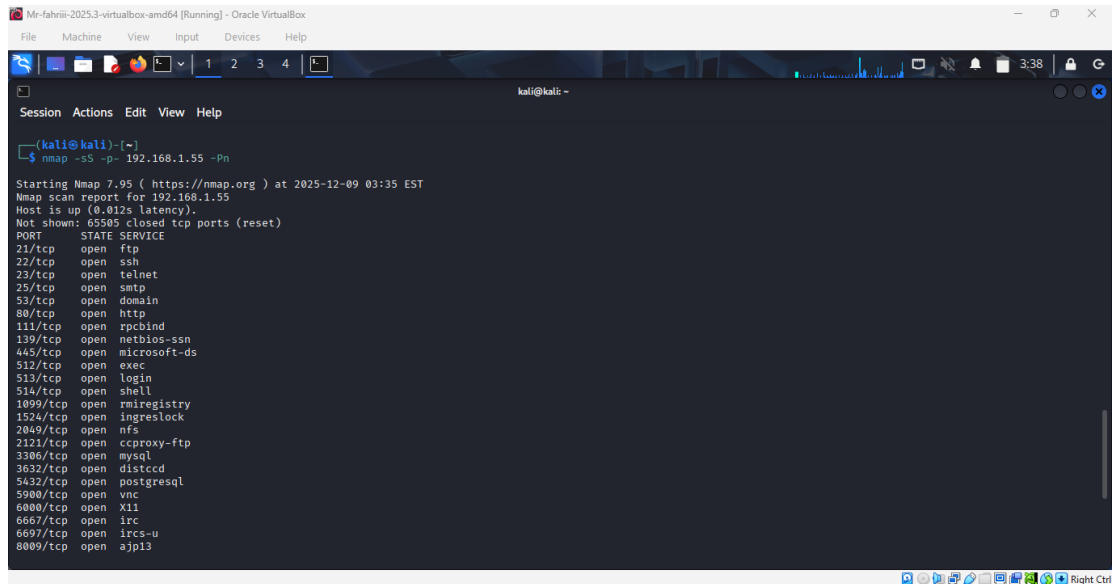
```
nmap -sS -p- 192.168.1.55 -Pn
```

Temuan Port Terbuka:

- 21/tcp – FTP
- 22/tcp – SSH
- 23/tcp – Telnet
- 25/tcp – SMTP
- 80/tcp – HTTP
- 3306/tcp – MySQL

Lampiran Dokumentasi:

- Nmap SYN Scan Results

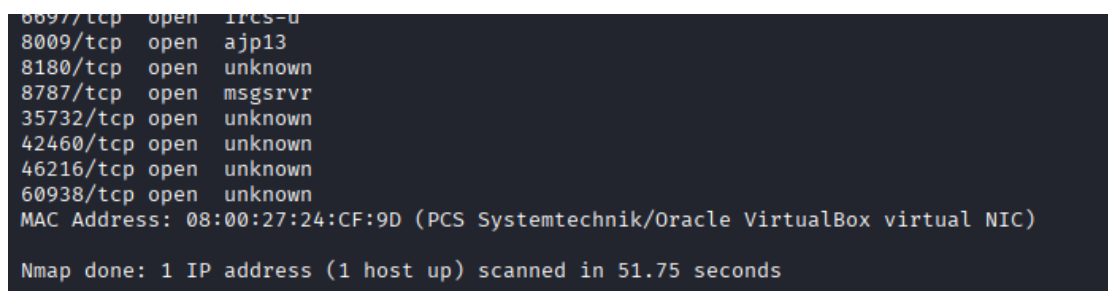


```
Mr-fahrii-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~
(kali@kali)~$ nmap -sS -p- 192.168.1.55 -Pn

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 03:35 EST
Nmap scan report for 192.168.1.55
Host is up (0.012s latency).
Not shown: 65505 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
```

Mendokumentasikan tahap Pengintaian Aktif (*Active Reconnaissance*) terhadap target. Pengintaian dimulai dengan analisis tumpukan teknologi eksternal menggunakan Wappalyzer dan BuiltWith untuk mengidentifikasi komponen kunci seperti *UI framework* Bootstrap, Google Tag Manager, dan ketergantungan pada Cloudflare (CDN/Analitik). Pengujian keamanan dasar melalui Google Dorking berhasil menemukan beberapa dokumen publik yang terindeks ("index of") di domain bumh.go.id, meskipun pencarian file *backup* tidak berhasil. Bagian kunci dari Pengintaian Aktif ditunjukkan melalui pemindaian jaringan Nmap (-sV -p-) terhadap IP internal (192.168.1.55), yang secara eksplisit mengungkapkan banyak port dan layanan terbuka, termasuk FTP (21), SSH (22), HTTP (80), dan MySQL (3306).



```
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35732/tcp open  unknown
42460/tcp open  unknown
46216/tcp open  unknown
60938/tcp open  unknown
MAC Address: 08:00:27:24:CF:9D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 51.75 seconds
```

2. Service & Version Detection

Command:

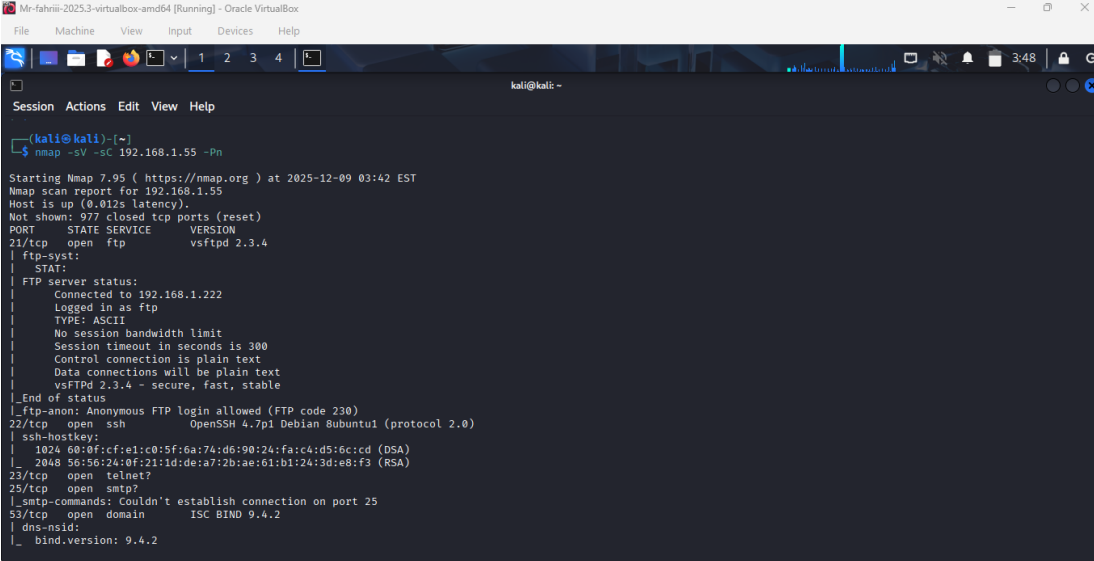
```
nmap -sV -sC 192.168.1.55
```

Temuan Versi Rentan:

- vsftpd 2.3.4 – Backdoor vulnerability
- Apache 2.2.8 – Outdated, banyak CVE
- MySQL 5.0.51a – Rentan remote exploit

Lampiran Dokumentasi:

- Nmap Service Scan



```
Mr-fahrini-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~
Session Actions Edit View Help

kali@kali: ~
$ nmap -sV -sC 192.168.1.55 -Pn

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 03:42 EST
Nmap scan report for 192.168.1.55
Host is up (0.012s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ ftp-syst:
|_ STAT:
|_ FTP server status:
|_   Connected to 192.168.1.222
|_   Logged in as ftp
|_   TYPE: ASCII
|_   No session bandwidth limit
|_   Session timeout in seconds is 300
|_   Control connection is plain text
|_   Data connections will be plain text
|_   vsFTPD 2.3.4 - secure, fast, stable
|_ End of status
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet?
25/tcp    open  smtp?
|_ smtp-command: Couldn't establish connection on port 25
53/tcp    open  domain       ISC BIND 9.4.2
|_ dns-nsid:
|_   bind.version: 9.4.2
```

Pemindaian Layanan Nmap (*Nmap Service Scan*) dilakukan pada alamat IP internal 192.168.1.55 menggunakan perintah `-sV -p-` untuk mengidentifikasi semua port terbuka dan versi layanan yang berjalan. Pemindaian tersebut mengungkap sejumlah besar port yang terbuka, termasuk layanan penting seperti 80/HTTP,

3306/MySQL, dan 5432/PostgreSQL. Secara spesifik, layanan FTP (port 21) ditemukan menjalankan vsftpd 2.3.4 dan, yang menjadi temuan paling signifikan, mengizinkan login Anonymous FTP. Selain itu, layanan SSH (port 22) terdeteksi berjalan pada versi OpenSSH 4.7p1.

```
Mr-fahmi-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: -
Session Actions Edit View Help
53/tcp open domain ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp open http Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-title: Metasploitable2 - Linux
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp open rpcbind 2 (RPC #100000)
| rpcinfo:
|_ program version port/proto service
|_ 100000 2 111/tcp rpcbind
|_ 100000 2 111/udp rpcbind
|_ 100003 2,3,4 2049/tcp nfs
|_ 100003 2,3,4 2049/udp nfs
|_ 100005 1,2,3 35732/tcp mountd
|_ 100005 1,2,3 58216/udp mountd
|_ 100021 1,3,4 42460/tcp nlockmgr
|_ 100021 1,3,4 48555/udp nlockmgr
|_ 100024 1 46216/tcp status
|_ 100024 1 49346/udp status
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
1099/tcp open java-rmi GNU Classpath gmicregistry
1524/tcp open bindshell Metasploitable root shell
2049/tcp open nfs 2-4 (RPC #100003)
2121/tcp open cproxy-ftp?
3306/tcp open mysql?
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ ssl-cert: Subject: commonName=ubuntu004-base.localdomain/organizationName=OCOSA
|_ stateOrProvinceName=There is no such thing outside US/countryName=XX
|_ Not valid before: 2018-03-17T14:07:45
```

```
Mr-fahmi-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: -
Session Actions Edit View Help
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_ http-title: Apache Tomcat/5.5
|_ http-favicon: Apache Tomcat
MAC Address: 08:00:27:24:CF:9D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Host: irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:l
inux_kernel

Host script results:
| smb-os-discovery:
|_ OS: Unix (Samba 3.0.20-Debian)
|_ Computer name: metasploitable
|_ NetBIOS computer name:
|_ Domain name: localdomain
|_ FQDN: metasploitable.localdomain
|_ System time: 2025-12-09T03:26:22-05:00
|_ nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <un
known> (unknown)
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ smb-security-mode:
|_ account_used: guest
|_ authentication_level: user
|_ challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 1h21m03s, deviation: 2h53m32s, median: -18m35s

Service detection performed. Please report any incorrect results at https://nmap.
org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 332.81 seconds

kali@kali: ~$
```

3. UDP Scan

Command:

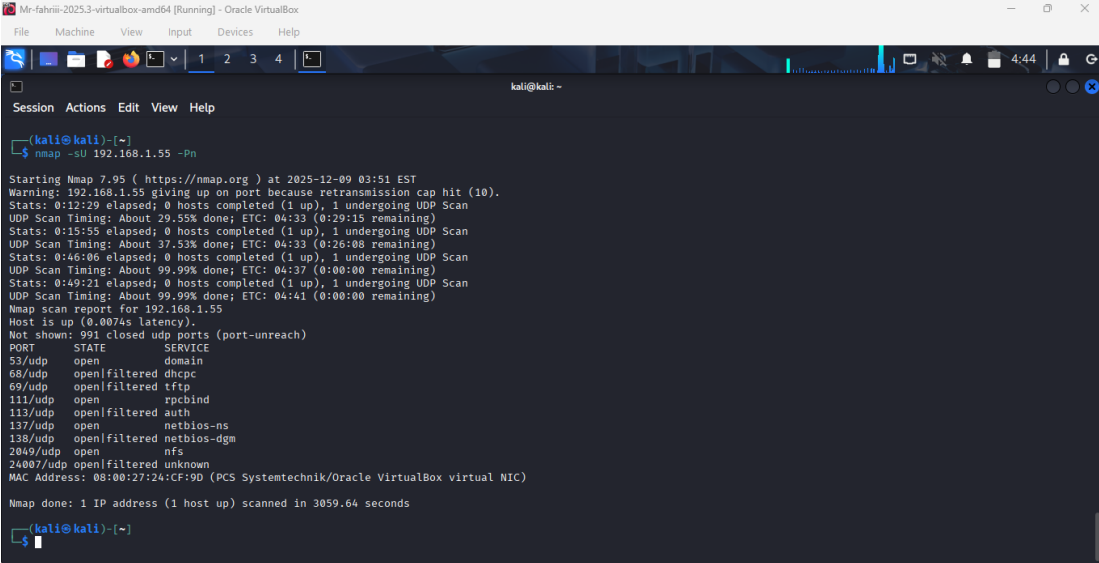
`nmap -sU 192.168.1.55 -Pn`

Temuan:

- 161/udp – SNMP (open|filtered)

Lampiran Dokumentasi:

- Nmap UDP Scan



```
Mr-fahrii-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help

kali@kali: ~
Session Actions Edit View Help

kali@kali: ~
$ nmap -sU 192.168.1.55 -Pn

Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 03:51 EST
Warning: 192.168.1.55 giving up on port because retransmission cap hit (10).
Stats: 0:12:29 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 29.55% done; ETC: 04:33 (0:29:15 remaining)
Stats: 0:15:55 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 37.53% done; ETC: 04:33 (0:26:08 remaining)
Stats: 0:46:06 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:37 (0:00:00 remaining)
Stats: 0:49:21 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 99.99% done; ETC: 04:41 (0:00:00 remaining)
Nmap scan report for 192.168.1.55
Host is up (0.0074s latency).
Not shown: 991 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp    open  domain
68/udp    open|filtered dhcp
69/udp    open|filtered tftp
111/udp   open  rpcbind
113/udp   open|filtered auth
137/udp   open  netbios-ns
138/udp   open|filtered netbios-dgm
2049/udp  open  nfs
24007/udp open|filtered unknown
MAC Address: 08:00:27:24:CF:90 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3059.64 seconds

kali@kali: ~
$
```

Pemindaian UDP Nmap (*Nmap UDP Scan*) dilakukan terhadap alamat IP internal 192.168.1.55 menggunakan perintah `nmap -sU -Pn`. Pemindaian ini memakan waktu yang signifikan (sekitar 3059 detik) dan berhasil mengidentifikasi beberapa port UDP yang terbuka atau *open|filtered*. Port-port yang teridentifikasi terbuka termasuk 53/udp (domain) dan 2049/udp (nfs). Sementara itu, port lain seperti 69/udp (tftp), 111/udp (rpcbind), dan port NetBIOS (137/138) terdeteksi dalam status *open|filtered*, mengindikasikan bahwa layanan tersebut mungkin aktif.

4. OS Fingerprinting

Command:

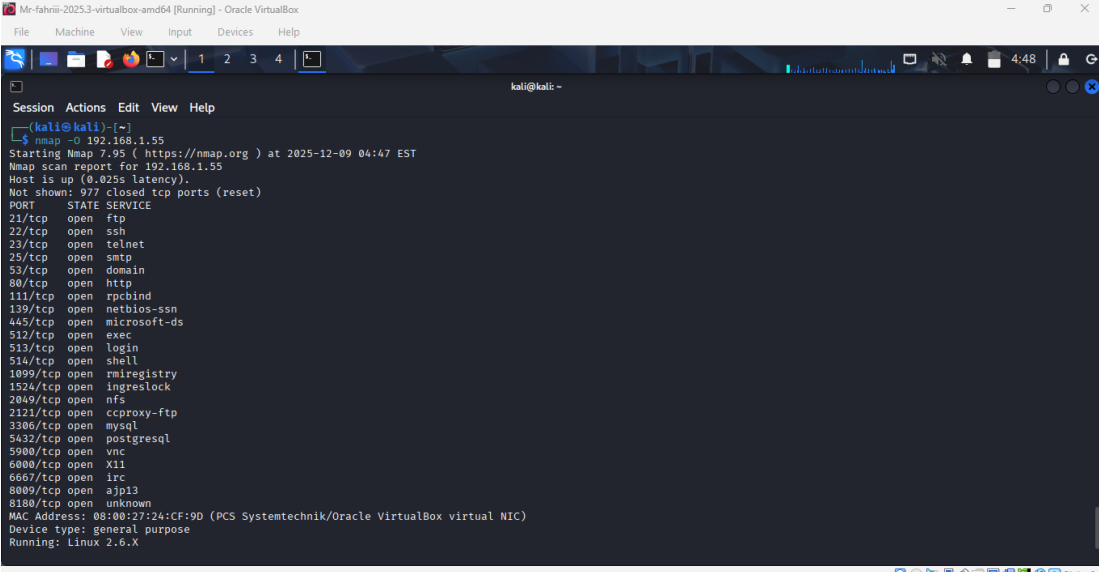
```
nmap -O 192.168.1.55
```

Hasil:

- OS: Linux Kernel 2.6.x (Metasploitable)

Lampiran Dokumentasi:

- Nmap OS Fingerprint



```
Mr-fahrill-2025.3-virtualbox-amd64 [Running] - Oracle VirtualBox
File Machine View Input Devices Help
kali@kali: ~
Session Actions Edit View Help
kali@kali: ~
$ nmap -O 192.168.1.55
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 04:47 EST
Nmap scan report for 192.168.1.55
Host is up (0.025s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  x11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 08:00:27:24:CF:9D (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
```

```
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
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 4.15 seconds
```

Pemindaian Sidik Jari OS Nmap (*Nmap OS Fingerprint*) berhasil mengidentifikasi bahwa target adalah perangkat general purpose yang menjalankan

sistem operasi Linux 2.6.X. Nmap lebih lanjut mempersempit detail OS ke kisaran versi kernel Linux 2.6.9 - 2.6.33. Informasi tentang penggunaan kernel Linux versi 2.6.X yang sudah tua ini sangat penting dalam fase pengintaian karena versi lama tersebut cenderung memiliki banyak kerentanan publik yang diketahui dan dapat dicari untuk eksploitasi.

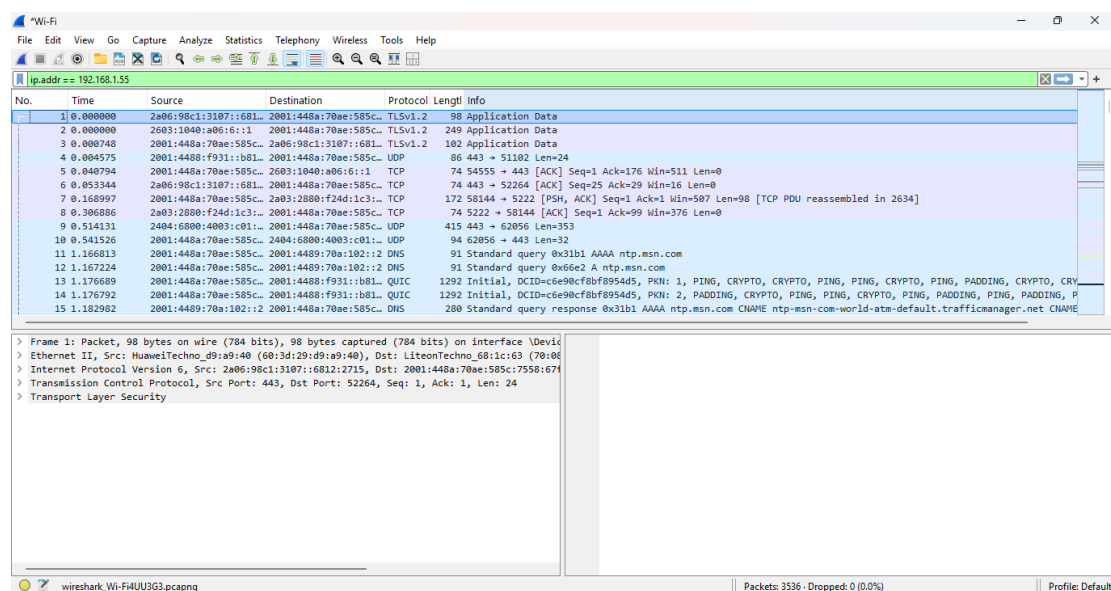
5. Network Protocol Capture (Wireshark)

Protokol ditemukan:

- ARP – Resolusi alamat jaringan
- TCP SYN/ACK – Handshake selama Nmap Scan
- DNS Query – Ketika resolving domain
- HTTP – Komunikasi plaintext

Lampiran Dokumentasi:

- Wireshark Protocol Capture



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2001:448a:70ae:585c...	2001:4488:f931::17d...	HTTP	429	HEAD /filestreamingservice/files/86061e48-63b3-483f-8dac-609df0cbb238?P1=1765312931&P2=404&P3=2&P4=ktCjP1e7...
2	0.117718	2001:4488:f931::17d...	2001:448a:70ae:585c...	HTTP	678	HTTP/1.1 200 OK
3	0.151876	2001:448a:70ae:585c...	2001:4489:70ae:1821:2	DNS	121	Standard query 0xd995 AAAA msedge.b.tlu.dl.delivery.mp.microsoft.com
4	0.168929	2001:448a:70ae:585c...	2001:4488:f931::17d...	TCP	74	51541 → 80 [ACK] Seq=356 Ack=685 Win=1019 Len=0
5	0.219890	2001:4489:70ae:1821:2	2001:448a:70ae:585c...	DNS	298	Standard query response 0xd995 AAAA msedge.b.tlu.dl.delivery.mp.microsoft.com CNAME star.b.tlu.dl.delivery.m...
6	0.221633	2001:448a:70ae:585c...	2001:4488:f931::17d...	HTTP	480	GET /filestreamingservice/files/86061e48-63b3-483f-8dac-609df0cbb238?P1=1765312931&P2=404&P3=2&P4=ktCjP1e7...
7	0.322254	2001:4488:f931::17d...	2001:448a:70ae:585c...	TCP	1466	80 → 51541 [ACK] Seq=605 Ack=762 Win=501 Len=1392 [TCP PDU reassembled in 11]
8	0.322444	2001:4488:f931::17d...	2001:448a:70ae:585c...	TCP	1466	80 → 51541 [PSH, ACK] Seq=1997 Ack=762 Win=501 Len=1392 [TCP PDU reassembled in 11]
9	0.322488	2001:448a:70ae:585c...	2001:4488:f931::17d...	TCP	74	51541 → 80 [ACK] Seq=762 Ack=3389 Win=1023 Len=0
10	0.323098	2001:4488:f931::17d...	2001:448a:70ae:585c...	TCP	28954	80 → 51541 [PSH, ACK] Seq=3389 Ack=762 Win=501 Len=28880 [TCP PDU reassembled in 11]
11	0.323098	2001:4488:f931::17d...	2001:448a:70ae:585c...	HTTP	373	HTTP/1.1 200 OK (application/x-chrome-extension)
12	0.323265	2001:448a:70ae:585c...	2001:4488:f931::17d...	TCP	74	51541 → 80 [ACK] Seq=762 Ack=24568 Win=1023 Len=0
13	1.445177	192.168.100.6	224.0.0.251	MDNS	103	Standard query 0x0019 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local,
14	1.448609	fe80::5884:ceff:fea...	ff02::fb	MDNS	123	Standard query 0x0019 PTR _googlecast._tcp.local, "QM" question PTR _233637DE._sub._googlecast._tcp.local,
15	1.752473	20.190.144.161	192.168.100.9	TCP	54	443 → 49733 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

> Frame 13: Packet, 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface
 > Ethernet II, Src: LGInnotek_58:6e:bc (d8:e3:5e:58:6e:bc), Dst: LiteonTechno_68:1c:63 (70:08:94...)
 > Internet Protocol Version 4, Src: 192.168.100.18, Dst: 239.255.255.250
 > User Datagram Protocol, Src Port: 38927, Dst Port: 1900
 > Simple Service Discovery Protocol

Wireshark_Wi-FUMT6G3.pcapng | Packets: 142 · Dropped: 0 (0.0%) | Profile: Default

Wireshark Protocol Capture digunakan untuk menganalisis lalu lintas jaringan secara *real-time*, sering kali difokuskan pada komunikasi yang melibatkan alamat IP target, yaitu **192.168.1.55**. Hasil tangkapan menunjukkan adanya lalu lintas terenkripsi yang signifikan menggunakan protokol **TLSv1.2**. Selain itu, tangkapan juga merekam berbagai protokol jaringan standar, termasuk permintaan **DNS** (ke *domain* eksternal seperti Microsoft), sesi **TCP** (SYN/ACK), permintaan **HTTP**, serta lalu lintas penemuan *host* seperti **mDNS** dan **Simple Service Discovery Protocol (SSDP)**, yang memberikan gambaran menyeluruh tentang aktivitas jaringan *host* target.

Kesimpulan

Passive Recon mengungkapkan banyak subdomain, teknologi, dan data publik relevan yang dapat digunakan dalam tahap selanjutnya (Social Engineering, Attack Surface Mapping).

Active Recon memvalidasi bahwa Metasploitable 2 memiliki banyak layanan rentan, terutama versi lama dari FTP, Apache, dan MySQL.

Semua temuan ini akan menjadi dasar untuk tahapan Vulnerability Assessment atau Exploitation.