

**LAPORAN PENGUJIAN PENETRASI KOMPREHENSIF:
ANALISIS PASSIVE (OSINT) DAN ACTIVE
RECONNAISSANCE PADA INFRASTRUKTUR TARGET**



UMMUL MU'MININ

105841117323

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

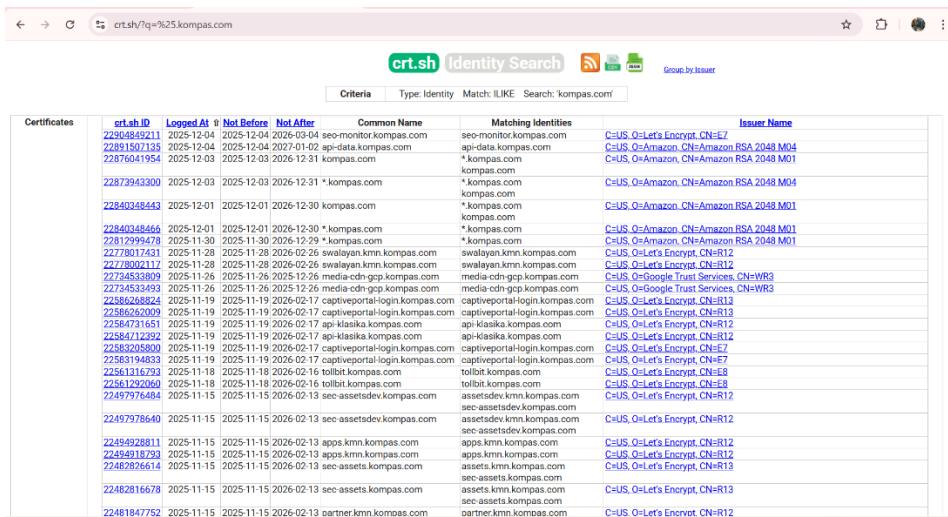
1. Passive Reconnaissance

a. Mencari Domain

Domain **kompas.com** telah dipilih sebagai target utama untuk pelaksanaan pengumpulan informasi publik (*Passive Reconnaissance*). Pemilihan ini didasarkan pada kebutuhan untuk mendemonstrasikan penerapan teknik *Open Source Intelligence* (OSINT) yang efektif pada sebuah entitas digital yang besar dan aktif.

b. Pencarian Sub-domain

Langkah awal dalam *Passive Reconnaissance* adalah mengidentifikasi aset digital tersembunyi target. Untuk tujuan ini, kami membuka website crt.sh. crt.sh berfungsi sebagai *Certificate Transparency Log*, sebuah *database* publik yang mencatat setiap sertifikat SSL/TLS yang diterbitkan untuk domain kompas.com. Tujuannya adalah untuk mencari sub-domain aktif yang mungkin tidak terdaftar secara publik di DNS. Berdasarkan hasil analisis, ditemukan beberapa sub-domain yang aktif dan relevan, di antaranya adalah seo-monitor.kompas.com, api-data.kompas.com, captiveportal-login.kompas.com, tolbit.kompas.com, dan sec-assetsdev.kompas.com.



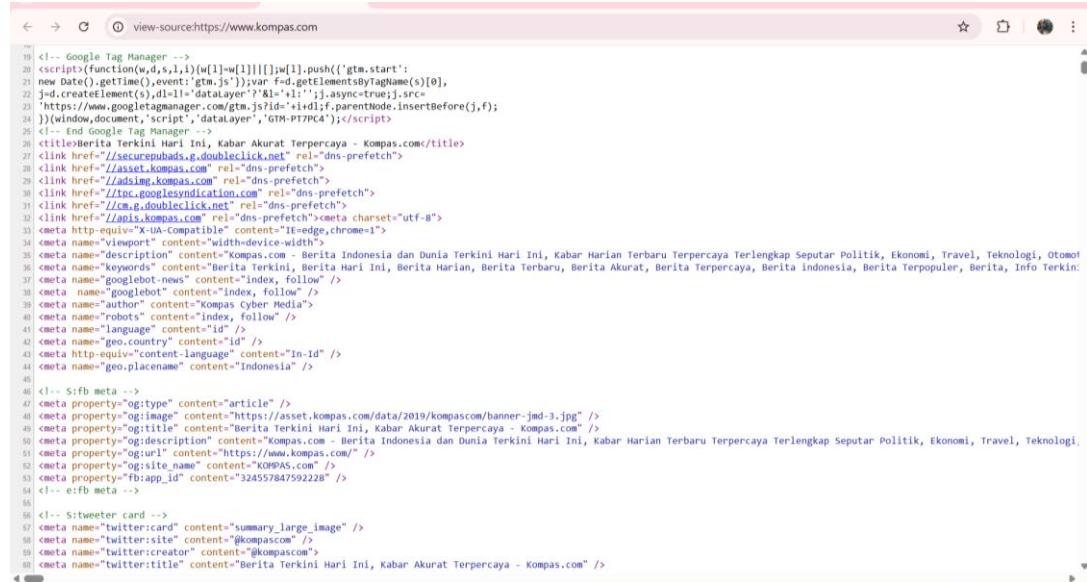
The screenshot shows a web browser displaying the crt.sh website. The search bar contains 'crt.sh/?q=%25.kompas.com'. The results table has columns: Certificates, crt.sh ID, Looped At, Not Before, Not After, Common Name, Matching Identities, and Issuer Name. The table lists numerous certificates issued to various sub-domains of kompas.com, such as seo-monitor.kompas.com, api-data.kompas.com, and various AWS certificates for Amazon services like CloudFront and Lambda@Edge.

Certificates	crt.sh ID	Looped At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	2290484921	2025-12-04	2025-12-04	2026-03-04	seo-monitor.kompas.com	seo-monitor.kompas.com	C=US,O=Let's Encrypt,CN=R12
	22851507135	2025-12-04	2025-12-04	2027-01-02	api-data.kompas.com	api-data.kompas.com	C=US,O=Amazon,CN=Amazon RSA 2048 M04
	22876041954	2025-12-03	2025-12-03	2026-12-31	kompas.com	* kompas.com	C=US,O=Amazon,CN=Amazon RSA 2048 M01
	22873943300	2025-12-03	2025-12-03	2026-12-31	* kompas.com	* kompas.com	C=US,O=Amazon,CN=Amazon RSA 2048 M04
	22840348443	2025-12-01	2025-12-01	2026-12-30	kompas.com	* kompas.com	C=US,O=Amazon,CN=Amazon RSA 2048 M01
	22840348466	2025-12-01	2025-12-01	2026-12-30	* kompas.com	* kompas.com	C=US,O=Amazon,CN=Amazon RSA 2048 M01
	2281299478	2025-11-30	2025-11-30	2026-12-29	* kompas.com	* kompas.com	C=US,O=Amazon,CN=Amazon RSA 2048 M01
	22778017431	2025-11-28	2025-11-28	2026-02-26	swalyan.kmn.kompas.com	swalyan.kmn.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22778002112	2025-11-28	2025-11-28	2026-02-26	swalyan.kmn.kompas.com	swalyan.kmn.kompas.com	C=US,OU=lets Encrypt,CN=R12
	2273453309	2025-11-26	2025-12-26	2025-12-26	media-cdn-gcp.kompas.com	media-cdn-gcp.kompas.com	C=US,OU=Google Trust Services,CN=WR3
	22734533493	2025-11-26	2025-11-26	2025-01-02	media-cdn-gcp.kompas.com	media-cdn-gcp.kompas.com	C=US,OU=Google Trust Services,CN=WR3
	22865230242	2025-11-19	2025-11-19	2025-02-02	captcha-reporter-login.kompas.com	captcha-reporter-login.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22865230209	2025-11-19	2025-11-19	2026-02-17	captcha-reporter-login.kompas.com	captcha-reporter-login.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22584712651	2025-11-19	2025-11-19	2026-02-17	api-klasika.kompas.com	api-klasika.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22584712392	2025-11-19	2025-11-19	2026-02-17	api-klasika.kompas.com	api-klasika.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22583205800	2025-11-19	2025-11-19	2026-02-17	captiveportal-login.kompas.com	captiveportal-login.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22583194833	2025-11-19	2025-11-19	2026-02-17	captiveportal-login.kompas.com	captiveportal-login.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22561316793	2025-11-18	2025-11-18	2026-02-16	tollbit.kompas.com	tollbit.kompas.com	C=US,OU=lets Encrypt,CN=E8
	22561292069	2025-11-18	2025-11-18	2026-02-16	sec-asset.kompas.com	sec-asset.kompas.com	C=US,OU=lets Encrypt,CN=E8
	22497976484	2025-11-15	2025-11-15	2026-02-13	sec-assetdev.kompas.com	sec-assetdev.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22497978640	2025-11-15	2025-11-15	2026-02-13	sec-assetdev.kompas.com	sec-assetdev.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22494928811	2025-11-15	2025-11-15	2026-02-13	apps.kmn.kompas.com	apps.kmn.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22494918793	2025-11-15	2025-11-15	2026-02-13	apps.kmn.kompas.com	apps.kmn.kompas.com	C=US,OU=lets Encrypt,CN=R12
	22462976614	2025-11-15	2025-11-15	2026-02-13	sec-assets.kompas.com	sec-assets.kompas.com	C=US,OU=lets Encrypt,CN=R13
	22462816678	2025-11-15	2025-11-15	2026-02-13	sec-assets.kompas.com	sec-assets.kompas.com	C=US,OU=lets Encrypt,CN=R13
	22461847752	2025-11-15	2025-11-15	2026-02-13	partner.kmn.kompas.com	partner.kmn.kompas.com	C=US,OU=lets Encrypt,CN=R12

c. Identifikasi Teknologi dan Metadata (View Source Code)

Pengumpulan informasi dilanjutkan dengan analisis kode sumber (View Source Code) dari halaman utama kompas.com. Analisis ini bertujuan untuk mengidentifikasi teknologi *front-end* yang digunakan. Hasilnya, ditemukan implementasi Google Tag Manager (GTM) dan berbagai tag <meta>. Penggunaan GTM ini mengindikasikan target bergantung pada *third-party scripts*, yang dapat membuka vektor Supply Chain Attack jika sistem pihak ketiga tersebut disusupi. Selain itu, metadata yang terekspos,

termasuk ID Aplikasi Facebook (fb:app_id), dapat digunakan untuk membuat serangan *social engineering* yang lebih kredibel.



```
1<!-- Google Tag Manager -->
2<script>(function(w,d,s,l,i){l=[].push||[];l.push(['gtm.start']);
3  var f=d.getElementsByTagName(s)[0];
4  var j=d.createElement(s),j.async=true;j.src=
5  "https://www.googletagmanager.com/gtm.js?id="+i+";parent.je.insertBefore(j,f);
6 })(window,document,'script','dataLayer','GM-PT7PQ4');
7<!-- End Google Tag Manager -->
8<title>Berita Terkini Hari Ini, Kabar Akurat Terpercaya - Kompas.com</title>
9<link href="/secpubads.g.doubleclick.net" rel="dns-prefetch">
10<link href="//asset.kompas.com" rel="dns-prefetch">
11<link href="//adsimg.kompas.com" rel="dns-prefetch">
12<link href="https://www.googleadservices.com" rel="dns-prefetch">
13<link href="https://apis.kompas.com" rel="dns-prefetch">
14<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
15<meta name="viewport" content="width=device-width">
16<meta name="description" content="Kompas.com - Berita Indonesia dan Dunia Terkini Hari Ini, Kabar Harian Terbaru Terpercaya Terlengkap Seputar Politik, Ekonomi, Travel, Teknologi, Otomo..." data-bbox="187 245 871 265">
17<meta name="keywords" content="Berita Terkini, Berita Hari Ini, Berita Harian, Berita Terbaru, Berita Akurat, Berita Terpercaya, Berita indonesia, Berita Terpopuler, Berita, Info Terkin..." data-bbox="187 265 871 285">
18<meta name="googlebot-newspaper" content="index,follow" />
19<meta name="author" content="Kompas Cyber Media" />
20<meta name="robots" content="index,follow" />
21<meta name="language" content="id" />
22<meta name="geo.country" content="ID" />
23<meta http-equiv="content-language" content="in-ID" />
24<meta name="geo.placename" content="Indonesia" />
25<!-- Sifb meta -->
26<meta property="og:type" content="article" />
27<meta property="og:image" content="https://asset.kompas.com/data/2019/kompascom/banner-jmd-3.jpg" />
28<meta property="og:title" content="Berita Terkini Hari Ini, Kabar Akurat Terpercaya - Kompas.com" />
29<meta property="og:description" content="Kompas.com - Berita Indonesia dan Dunia Terkini Hari Ini, Kabar Harian Terbaru Terpercaya Terlengkap Seputar Politik, Ekonomi, Travel, Teknologi,..." data-bbox="187 325 871 335"/>
30<meta property="og:url" content="https://www.kompas.com/" />
31<meta property="og:site_name" content="KOMPAS.com" />
32<meta property="fb:app_id" content="32455784592228" />
33<!-- eifb meta -->
34<!-- Sifwter card -->
35<meta name="twitter:card" content="summary_large_image" />
36<meta name="twitter:site" content="@kompascom" />
37<meta name="twitter:creator" content="@kompascom" />
38<meta name="twitter:title" content="Berita Terkini Hari Ini, Kabar Akurat Terpercaya - Kompas.com" />
```

d. Analisis Otomatis Menggunakan Wappalyzer

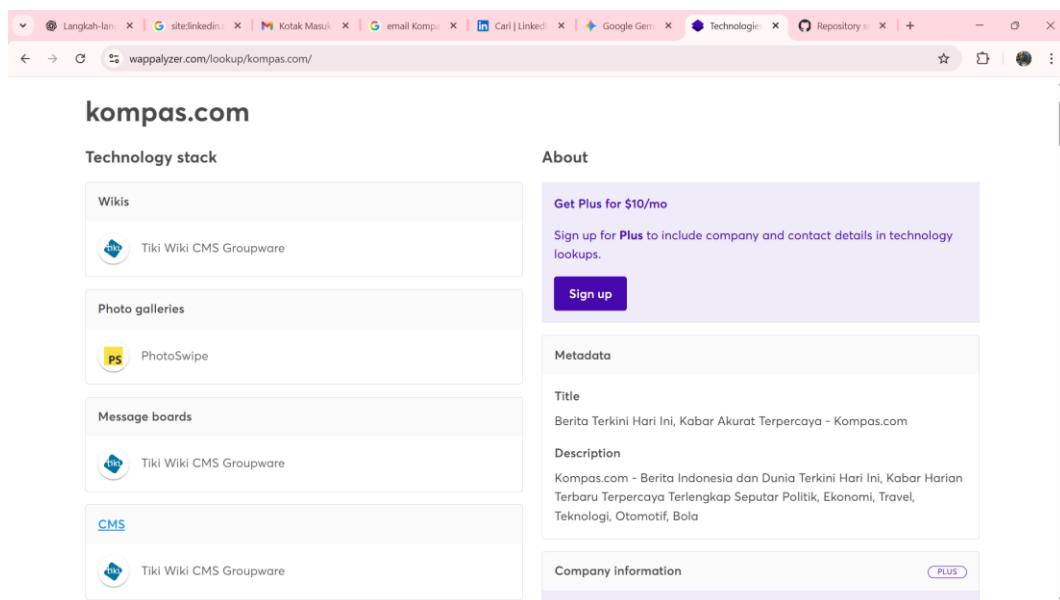
Untuk mengkonfirmasi dan memperluas temuan yang diperoleh secara manual, kami menggunakan alat otomatis Wappalyzer. Analisis ini memberikan gambaran lengkap mengenai tumpukan teknologi target. Di sisi infrastruktur, diidentifikasi penggunaan layanan *Platform as a Service* (PaaS) Amazon Web Services (AWS) dan Nginx yang berfungsi ganda sebagai *Reverse Proxy* dan *Web Server*. Untuk pengiriman konten, Wappalyzer mendeteksi penggunaan *Content Delivery Network* (CDN) Amazon CloudFront dan Cloudflare. Lebih lanjut, di sisi *front-end*, terdeteksi penggunaan bahasa pemrograman seperti Node.js dan PHP, serta *framework* Bootstrap dan *library* JQuery.

- Infrastruktur dan Layanan Back-End

Pencarian otomatis menggunakan Wappalyzer mengkonfirmasi tumpukan teknologi inti target. Di sisi infrastruktur, diidentifikasi penggunaan layanan *Platform as a Service* (PaaS) dari Amazon Web Services (AWS). Selain itu, Nginx digunakan sebagai *Reverse Proxy* dan *Web Server*. Untuk pengiriman konten dan optimasi kecepatan, Wappalyzer mendeteksi penggunaan *Content Delivery Network* (CDN) Amazon CloudFront dan Cloudflare. Temuan ini penting karena mengidentifikasi komponen yang mungkin rentan terhadap *misconfiguration* atau eksloitasi pada layanan server.

- Bahasa Pemrograman dan Framework Front-End

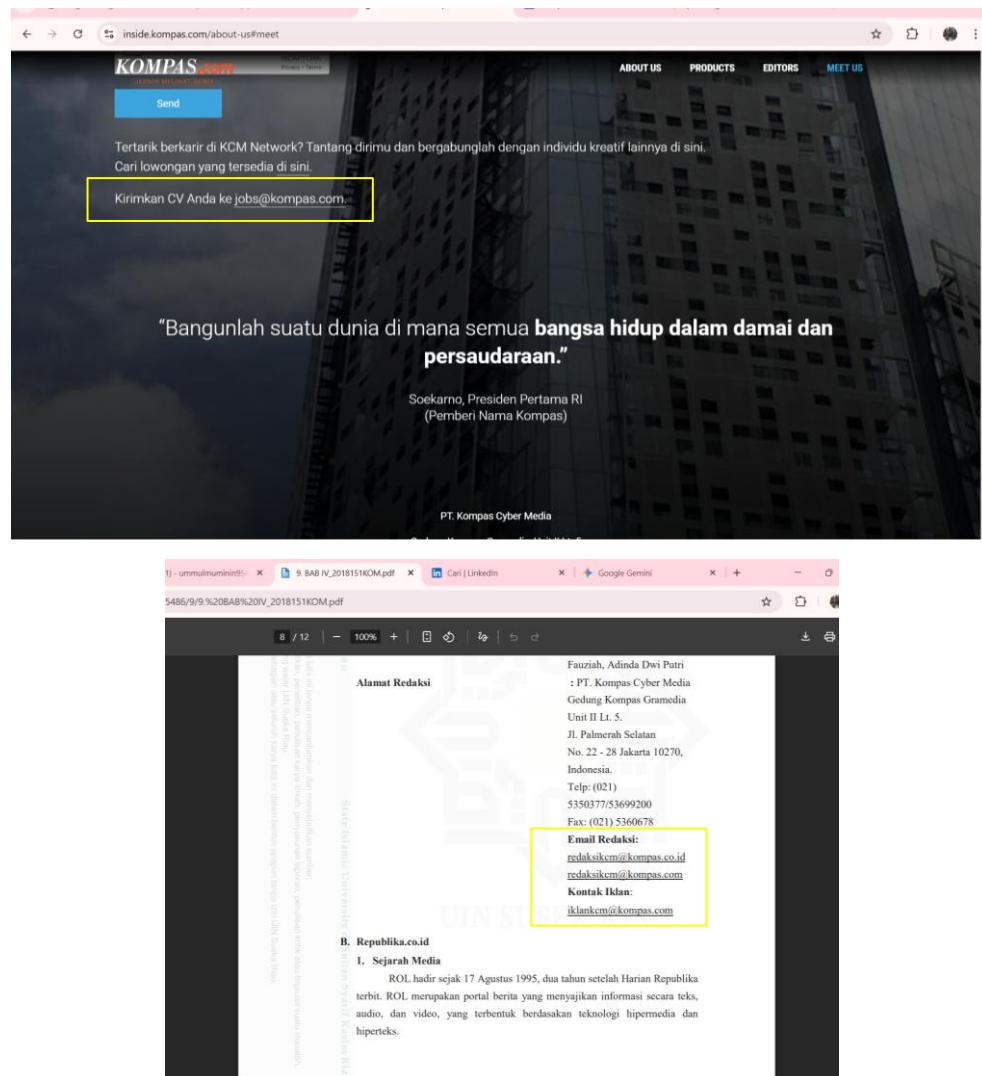
Analisis Wappalyzer juga memberikan gambaran mengenai teknologi yang digunakan di sisi *front-end* dan pendukung. Ditemukan penggunaan bahasa pemrograman Node.js dan PHP sebagai dasar *scripting*. Selain itu, Wappalyzer mendeteksi penggunaan *framework* Bootstrap dan *library* JQuery. Informasi ini sangat berguna untuk fase pengujian kerentanan (*Vulnerability Assessment*), di mana *penetration tester* dapat mencari kerentanan yang spesifik pada versi *framework* dan bahasa pemrograman tersebut.



e. Informasi Email dan Karyawan

- Informasi Email

Pengumpulan informasi dilanjutkan dengan mengidentifikasi alamat kontak penting. Dari halaman *About Us* kompas.com, ditemukan alamat kontak rekrutmen yaitu jobs@kompas.com. Selain itu, melalui penelusuran di repositori publik (laporan penelitian), ditemukan alamat email redaksi dan iklan, yaitu redaksikcm@kompas.com dan iklankcm@kompas.com. Temuan ini mengindikasikan bahwa format email standar perusahaan kemungkinan besar adalah [fungsi/posisi]@kompas.com atau [nama]@kompas.com. Informasi ini sangat penting karena format email yang tervalidasi dapat digunakan untuk melakukan serangan *phishing* yang ditargetkan (*spear-phishing*) atau *brute-force* kredensial *login*.

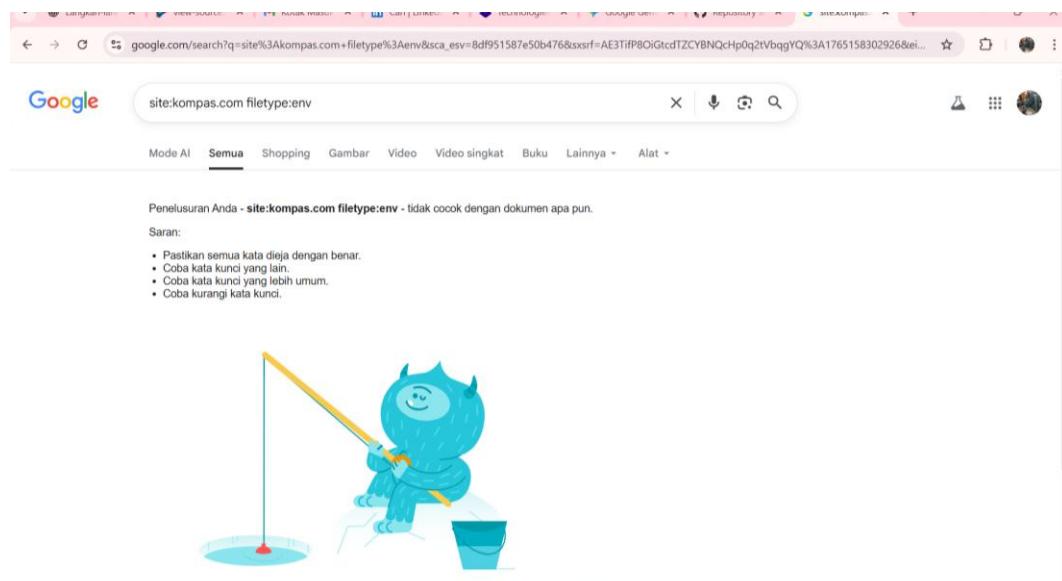


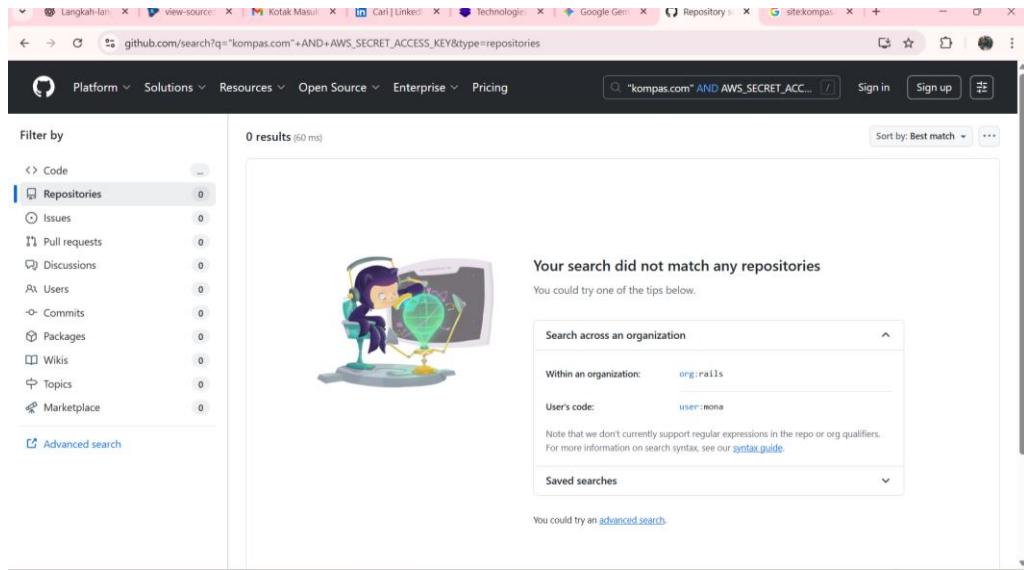
- **Informasi Karyawan**

Informasi yang dikumpulkan dari platform profesional (LinkedIn) juga mengkonfirmasi keberadaan dan posisi beberapa karyawan target. Karyawan yang teridentifikasi memiliki beragam peran, termasuk Reporter Intern, Asisten Editor di Kompas Tekno, dan Marketing Strategist. Penemuan nama dan jabatan karyawan ini sangat bernilai dalam *penetration test* karena memungkinkan penyerang untuk memilih target dengan *privilege* tertentu atau yang bekerja di divisi sensitif. Informasi ini akan digunakan untuk merancang pesan *phishing* yang kredibel dan sangat meyakinkan untuk mendapatkan akses awal ke dalam jaringan internal.

f. Informasi Sensitif yang Terpapar

Pencarian informasi sensitif yang terekspos dilakukan menggunakan teknik Google Dorking dan penelusuran platform repositori kode. Fokus utama pencarian diarahkan pada *file* konfigurasi yang terekspos seperti filetype:env, serta kredensial *hardcoded* seperti AWS_SECRET_ACCESS_KEY di GitHub. Setelah pencarian yang teliti, tidak ditemukan *file* atau *credential* internal yang langsung terekspos di domain publik. Hasil ini menunjukkan bahwa tim pengembangan target telah mengambil langkah yang tepat dalam mencegah paparan *file* konfigurasi kritis ke mesin pencari dan repositori kode. Namun, upaya pencarian ini tetap krusial dalam fase *penetration testing* untuk memverifikasi integritas keamanan target.





2. Active Reconnaissance

a. Persiapan Lingkungan dan Akses Root

Proses *Active Reconnaissance* dimulai dengan membuka terminal pada sistem operasi pengujian (Kali Linux atau sejenisnya). Untuk memastikan semua fungsi Nmap, terutama TCP SYN Scan (-sS), dapat berjalan dengan hak akses yang diperlukan, kami terlebih dahulu mengubah hak akses menjadi root. Akses *root* ini penting karena pemindaian *stealth* memerlukan manipulasi paket jaringan tingkat rendah yang hanya diizinkan oleh pengguna dengan hak administratif.

```

Session Actions Edit View Help
(ummul㉿kali)-[~]
$ sudo su
[sudo] password for ummul:
[root@kali]-[/home/ummul]

```

b. Pemindaian Port TCP dan Deteksi Perangkat (Menggunakan Nmap)

Setelah mendapatkan hak akses *root*, perintah Nmap dieksekusi pada target 192.168.56.101 (lingkungan VulnOS). TCP SYN Scan (-sS) dilakukan untuk mengidentifikasi layanan yang terbuka. Hasilnya menunjukkan bahwa 999 port TCP tertutup dan *host* dideteksi sebagai perangkat keamanan jaringan (*firewall/router*). Temuan ini mengindikasikan adanya filter jaringan yang sangat ketat pada target.

```

Session Actions Edit View Help
(ummul㉿kali)-[~]
$ sudo su
[sudo] password for ummul:
[root@kali]-[/home/ummul]
# nmap -sS 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 12:23 WITA
Nmap scan report for 192.168.56.101
Host is up (0.047s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE      SERVICE
9/tcp     filtered   discard
Nmap done: 1 IP address (1 host up) scanned in 2.45 seconds

```

c. Pemindaian Port UDP (Menggunakan Nmap -sU)

Setelah menyelesaikan pemindaian TCP, kami melanjutkan pemindaian dengan fokus pada *port* UDP menggunakan perintah nmap -sU 192.168.56.101. Pemindaian UDP dilakukan karena layanan penting, seperti DNS, sering berjalan di protokol ini, dan pemindaian TCP tidak dapat mendeteksinya. Hasil pemindaian ini menunjukkan bahwa 999 *port* UDP tidak merespons, namun mengidentifikasi Port 53 (layanan domain) dalam status open|filtered. Temuan ini sangat penting karena Port 53 adalah satu-satunya titik interaksi yang terdeteksi, dan mengarahkan *penetration tester* untuk fokus pada potensi serangan *Zone Transfer* atau kerentanan lain pada layanan DNS tersebut.

```
[root@kali:~/home/ummul]
# nmap -sU 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 12:23 WITA
Nmap scan report for 192.168.56.101
Host is up (0.057s latency).
Not shown: 999 open|filtered udp ports (no-response)
PORT      STATE SERVICE
53/udp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 24.22 seconds
```

d. Pemindaian UDP dan Deteksi OS/Versi (Menggunakan Nmap Lanjutan)

Setelah pemindaian awal, pemindaian *stealth* TCP (disertai deteksi OS dan Versi) dieksekusi. Hasil pemindaian pada terminal menunjukkan bahwa *Host is up* (Host hidup), namun 999 closed tcp ports (reset) dilaporkan. Pada bagian deteksi OS, Nmap menebak bahwa *Device type* adalah general purpose | WAP | switch | firewall. Nmap melakukan *Aggressive OS guesses* dengan tingkat kepercayaan tinggi, yaitu ETH Zurich Bluebottle OS (91%), D-Link embedded (89%), dan Cisco IOS 12.x (87%).

```
[root@kali:~/home/ummul]
# nmap -sS -sV -O 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-08 12:24 WITA
Nmap scan report for 192.168.56.101
Host is up (0.042s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
Device type: general purpose|WAP|switch|firewall
OS/Service info: OS:OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|WAP|switch|firewall
Running ([JUST GUESSING]): ETH Zurich Bluebottle (91%), D-Link embedded (89%), Cisco IOS 12.X (87%)
OS CPE: cpe:/o:ethzurich:bluebottle cpe:/h:dlink:di-524 cpe:/o:cisco:ios:12.2 cpe:/h:dlink:dfl-700
Aggressive OS guesses: Bluebottle OS (91%), D-Link DI-524 wireless broadband router (89%), Cisco 3550 switch (IOS 12.2) (87%), D-Link DFL-700 firewall (86%)
No exact OS matches for host (test conditions non-ideal).

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 8.61 seconds
```

e. Analisis Lalu Lintas Jaringan (Menggunakan Wireshark)

Secara paralel dengan pemindaian Nmap, aplikasi Wireshark dibuka untuk melakukan *packet capture* dan menganalisis lalu lintas jaringan secara langsung. Analisis ini mengkonfirmasi bahwa *host* target merespons upaya pemindaian Nmap dengan paket TCP dan ICMP. Kehadiran paket ICMP memvalidasi bahwa

host target berada dalam status *live (host discovery)*, sedangkan paket TCP yang dikirimkan oleh Nmap (SYN) dan respons yang terpotong mengkonfirmasi bahwa target memproses permintaan koneksi, meskipun akhirnya dibatasi oleh *firewall* yang aktif. Dengan demikian, Wireshark berhasil memvalidasi bahwa temuan Nmap berasal dari perangkat yang berfungsi, bukan dari *host* yang mati.

