LAPORAN

ETHICAL HACKING AND PENETRATION TESTING I

Dosen Pengampuh : Runal Rezkiawan S,Kom., M.T

DI SUSUN OLEH

NAMA : **NUR ALIYAH AMALIANI**

NIM : **105841106923**

KELAS : **5 JK-B**

PROGRAM STUDI INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

PASSIVE RECONNAISSANCE (Pengintaian Pasif)

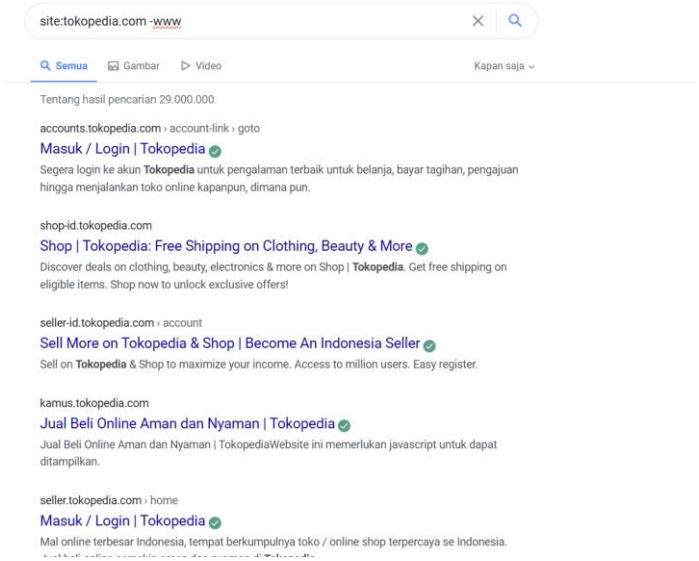
Tahap ini berfokus pada Passive Reconnaissance, yaitu metode pengumpulan informasi intelijen tanpa melakukan interaksi langsung yang agresif dengan sistem target. Pendekatan ini bertujuan untuk mengidentifikasi aset informasi publik milik target tanpa meninggalkan jejak digital (log) yang dapat memicu alarm keamanan.

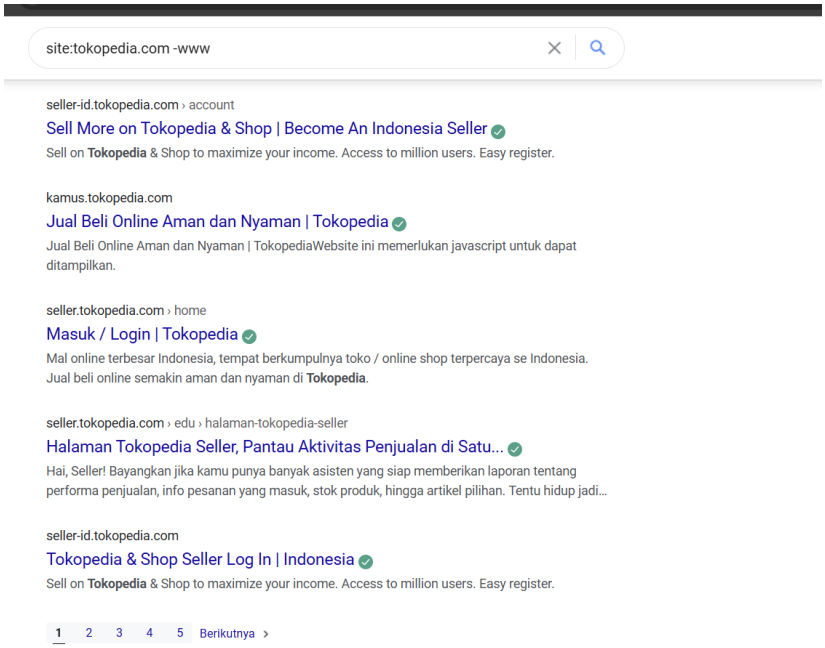
Dalam situasi ini, target yang dituju adalah **Tokopedia.** Proses pengumpulan data dilakukan menggunakan teknik Open-Source-Intelligance (OSINT) untuk memetakan permukaan serangan (attack surface), meliputi enumerasi sub-domain, identifikasi karyawan kunci, serta analisis tumpukan teknologi (tect stack) yang digunakan.

Berikut langkah langkah yang dilakukan dalam passive reconnaissance

1. **Tahap Pertama: Pencarian Domain dan Sub-Domain**

   Pada tahap pertama ini, dilakukan pencarian domain dan sub-domain dari target dengan teknik google Dorking menggunakan perintah site:tokopedia.com -www. Operator ini digunakan untuk memfilter domain utama dan mengeksport sub-domain spesifik seperti portal login atau layanan internal yang tidak terlihat pada navigasi publik.





Berdasarkna hasil temuan menggunakan Google Dorking, ditemukan bahwa attact surface pada target tidak terbatas pada domain utama yaitu tokopedia.com. terindetifikasi beberapa sub-domain kritis yang terekspos ke publik, antaralain accounts (portal autentikasi) dan seller (portal manajemen bisnis).

Sub-domain ini mengindikasikan adanya segmentasi fungsi yang jelas. Namun, eksposur ini juga membuka peluang bagi penyerang untuk menargetkan fungsi spesifik. Serangan krudensial pada portal login dan manipulasi bisnis pada portal penjual. Selain itu, ditemukan pula sub-domain berbasi konten (kaus) yang berpotensi memiliki kerentanan pada sisi aplikasi web seperti Cross-Site Scripting (XSS) jika tidak dikelola dengan pembaruan keamana yang rutin.

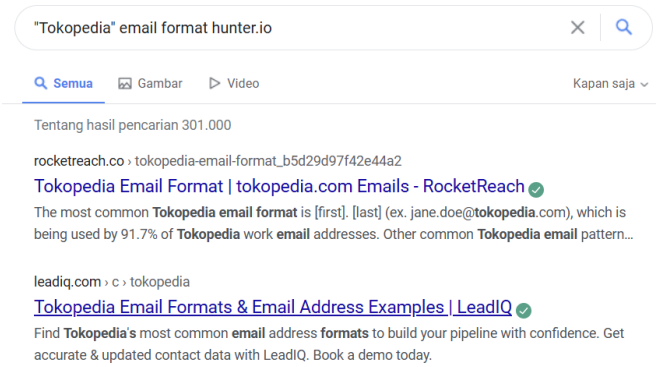
2. Tahap Kedua: Infromasi Email dan Karyawan

Setelah menemukan domain dan sub-domain, tahapan selanjutnya adalah pengumpulan informasi sumber daya manusia (human assets. Tahapan ini bertujuan untuk mengidentifikasi individu-individu yang memegang posisi strategi serta memahami standar komunikasi internal perusahaan.

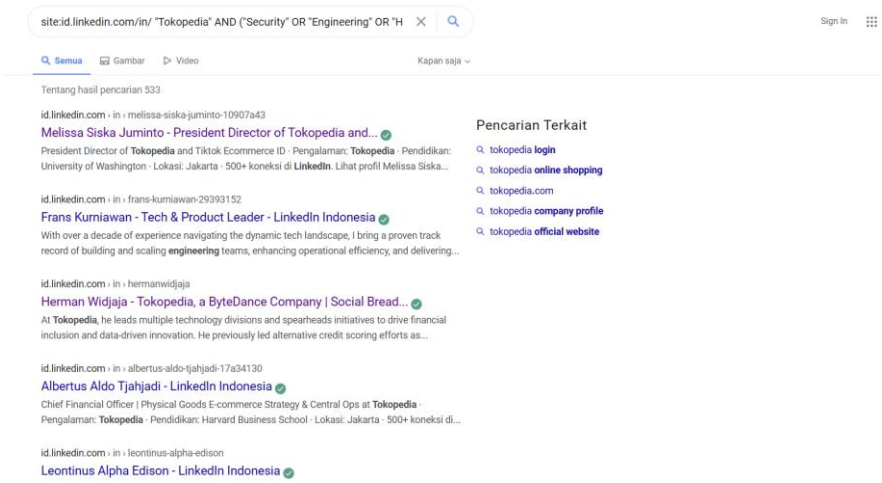
Pada tahapan ini, kita tetap menggunakan teknik OSINT yang ditargetkan pada platform profesional publik seperti LinkedIn, dengan melakukan

pencarian terhadap profil karyawan kunci (High Value Targets) dan pola penamaan alamat emali (email naming convention). Informasi ini krusial untuk memetakan potensi serangan berbasis rekayasa sosial (Sosial Engineering) seperti Whaling atau Phishing yang terarah

- **Format Email**



Berdasarkan hasil penelusuran terhadap database publik pihak ketiga (Hunter.io via Google Search snippet), berhasil diidentifikasi pola penamaaan alamat email perusahaan (Email Naming Convention) yang konsisten. Ditemukan bahwa format standar yang digunakan oleh mayoritas karyawan adalah {nama.depan}{nama.belakang}@tokopedia.com



site:id.linkedin.com/in/ "Tokopedia" AND ("Security" OR "Engineering" OR "H

Herman Widjaja - Tokopedia, a ByteDance Company | Social Bread...

At **Tokopedia**, he leads multiple technology divisions and spearheads initiatives to drive financial inclusion and data-driven innovation. He previously led alternative credit scoring efforts as...

id.linkedin.com › in › albertus-aldo-tjahjadi-17a34130

Albertus Aldo Tjahjadi - LinkedIn Indonesia

Chief Financial Officer | Physical Goods E-commerce Strategy & Central Ops at **Tokopedia** · Pengalaman: **Tokopedia** · Pendidikan: Harvard Business School · Lokasi: Jakarta · 500+ koneksi di...

id.linkedin.com › in › leontinus-alpha-edison

Leontinus Alpha Edison - LinkedIn Indonesia

Sejak mendirikan **Tokopedia** pada tahun 2009, Leon bertanggung jawab dalam memimpin berbagai fungsi teknologi dan operasional, serta yang terkait dengan manajemen sumber daya manusia,...

id.linkedin.com › in › donihanafi

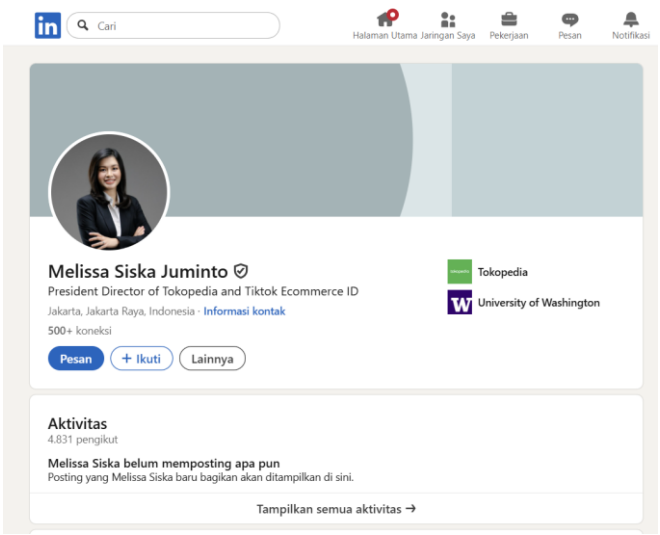
Doni Hanafi - VP of Engineering at Tokopedia, a ByteDance company...

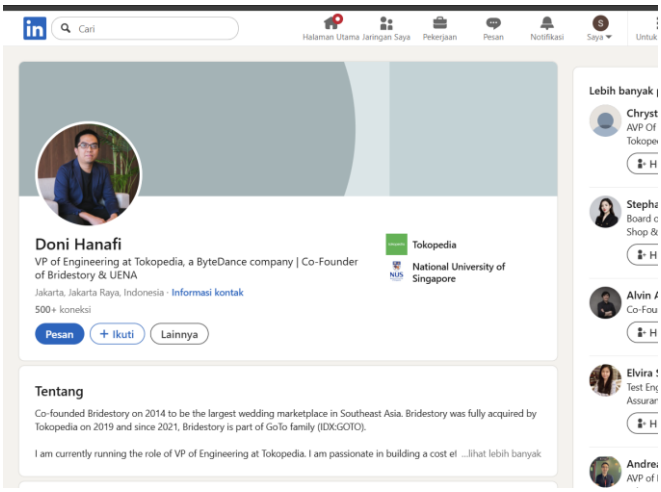
I am currently running the role of VP of **Engineering** at **Tokopedia**. I am passionate in building a cost effective technology team and I had been contributing to some early startups as Technical...

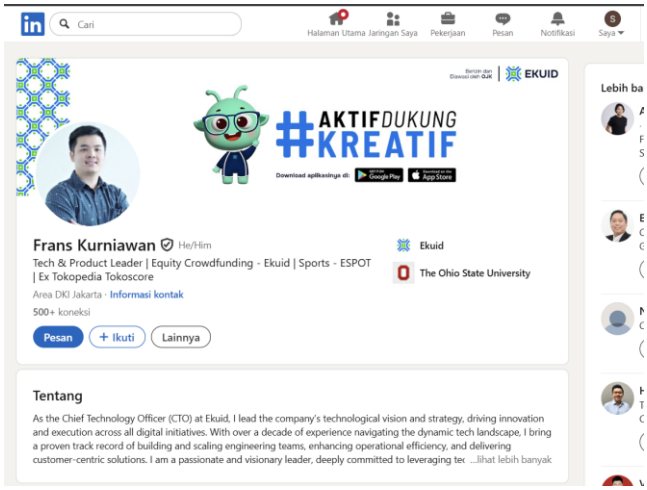
id.linkedin.com › in › rudydalimunthe

12K+ Followers | Senior Vice President - LinkedIn Indonesia

· Pengalaman: **Tokopedia** · Pendidikan: University of Indonesia · Lokasi: Jakarta Raya · 500+ koneksi di **LinkedIn**. Lihat profil Rudy A. Dalimunthe di LinkedIn, komunitas profesional yang terdiri...







Berdasarkan hasil pencarian di Linkedin dengan menggunakan teknik dorking dengan perintah yang spesifik yaitu *site:id.linkedin.com/in/'Tokopedia' AND ('Security' OR 'Engineering' OR 'Head')*. Perintah ini digunakan untuk menyaring jutaan profil agar hanya menampilkan individu yang bekerja di Tokopedia dengan jabatan teknis atau manager tingkat tinggi. Berdasarkan hasil pencarian tersebut, disini kita menemukan dan memilih tiga profil yang dijadikan target simulasi yaitu ada *Melisa Siska Juminto (Presiden Director), Doni Hanafi (VP Engineering), dan Frans Kurniawan (Tech & Product Leader).* Ketiga profil ini dipilih karena level akses mereka yang sangat luas. Kompromi pada salah satu akun ini dapat memberikan dampak katastropik, mulai dari manipulasi keputusan bisnis hingga akses penuh ke infrastruktur teknis perusahaan

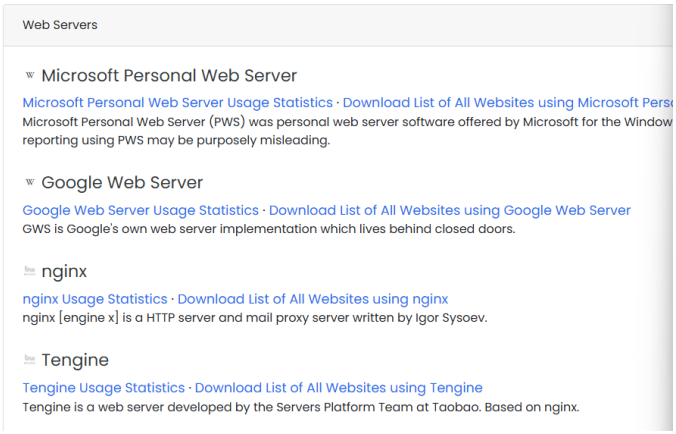
3. Teknologi yang digunakan

Setelah pemetaan terhadap doiman dan email serta profil karyawan yang kita dapatkan, tahapan selanjutnya berfokus pada analisis infrastruktur teknis yang menopang layanan tokopedia.com. proses ini, yang dikenal sebagai Technology Fingerprinting, bertujuan untuk membedah spesifikasi perangkat lunak, framework, dan konfigurasi server tanpa melakukan interaksi intrusif yang dapat memicu log keamanan

Pada tahap ini, digunakan alat bantu analisis yaitu BuiltWith untuk mengidentifikasi teknologi apa yang digunakan oleh target. Analisis dilakukan

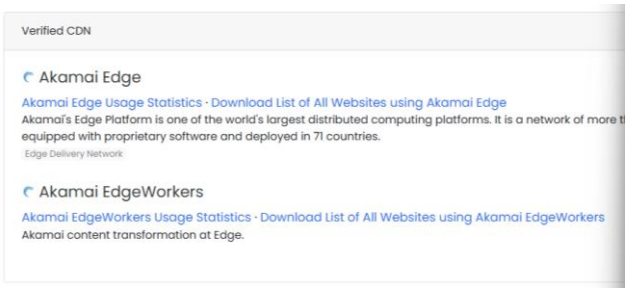
terhadap komponen-komponen vital seperti jenis Web server, Content Delivery Network (CDN), dan pustaka JavaScript yang berjalan di sisi client.

- **Web Server**



Berdasarkan hasil pencarian menggunakan BuiltWith, terlihat bahwa infrastruktur utama website target dijalankan menggunakan Tengine. Tengine sendiri adalah jenis web server yang dikembangkan dari basis Nginx. Informasi ini sangat berguna karena mempersempit fokus pencarian celah keamanan. Dengan mengetahui target menggunakan Tengine, pencarian kerentanan (CVE) selanjutnya dapat difokuskan spesifik pada kelemahan Tengine/Nginx, dan mengabaikan serangan yang hanya berlaku untuk server lain seperti Apache atau Windows Server

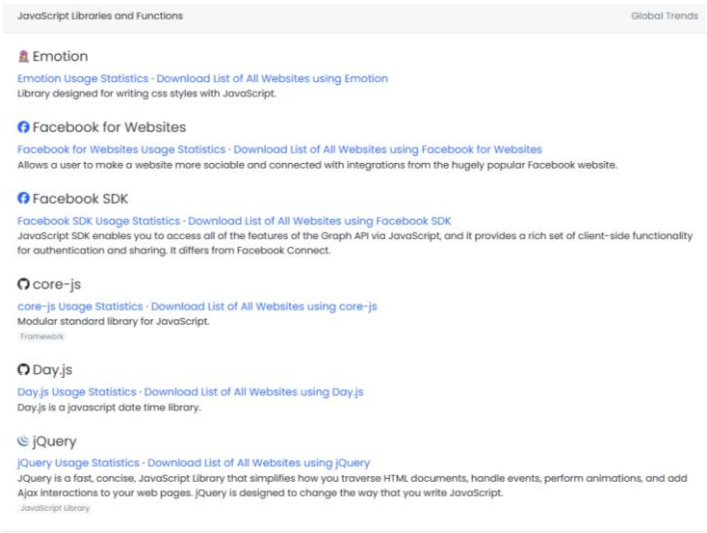
- **Content Delivery Network (CDN)**



Selanjutnya pada lapisan jaringan, terlihat adanya penggunaan Akamai Edge sebagai Content Delivery Network (CDN). Keberadaan Akamai menunjukkan bahwa target memiliki sistem pertahanan yang menyembunyikan alamat IP asli server. Implikasinya bagi penguji keamanan adalah serangan langsung ke domain utama kemungkinan besar

akan terblokir oleh firewall Akamai, sehingga diperlukan teknik khusus untuk memutari proteksi ini.

- **Library JavaScript**



Bagian terakhir pada sisi aplikasi, antarmuka website dibangun menggunakan Framework React. Penemuaan ini menandakan bahwa mayoritas logika aplikasi berjalan di sisi pengguna (client-side). Hal ini mengubah arah strategi serangan, di mana potensi kerentanan terbesar kemungkinan bukan berada di server, melainkan pada manipulasi kode JavaScript di browser, seperti serangan Cross-Site Scripting (XSS) atau eksploitasi jalur komunikasi API

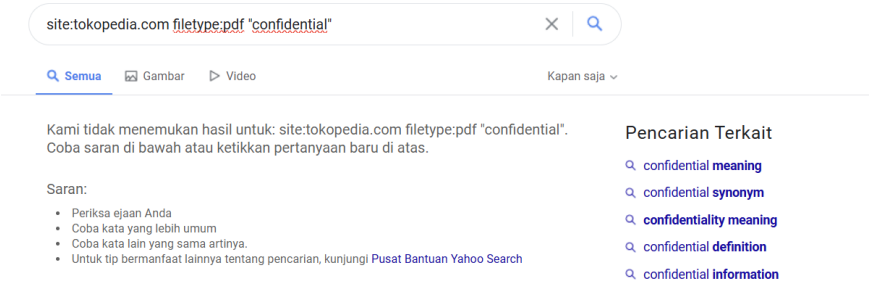
4. Informasi sensitif yang terpapar

Tahapan selanjutnya adalah mencari jejak informasi sensitif yang mungkin tidak sengaja terekspos ke publik akibat kelalaian manusia (human error). Tahapan ini sangat krusial karena sering kali pengembang aplikasi atau

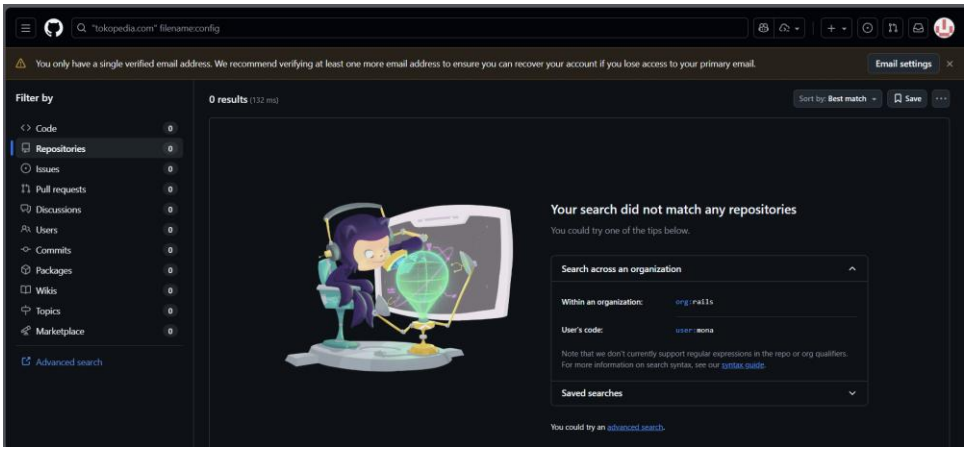
karyawan meninggalkan jejak digital berupa kode program, file konfigurasi, atau dokumentasi internal di platform terbuka seperti GitHub.

Proses pencari dilakukan dengan menggunakan teknik dorking spesifik pada repositori publik untuk menemukan kredensial yang tertanam, kunci API, atau alamat server internal yang seharusnya rahasia. Tujuannya adalah untuk menunjukkan jalan pintas akses atau memahami logika internal aplikasi tanpa perlu melakukan serangan teknis yang rumit terhadap sistem pertahanan utama.

Pada tahap ini dilakukan beberapa cara untuk mencari informasi sensitif yaitu pertama dengan menggunakan teknik google dorking dengan memasukkan perintah *site:tokopedia.com filetype:pdf "confidential"* dan *site:tokopedia.com filetype:docx*. Perintah ini diguanakan untuk mencari file dengan ekstention pdf dan docx yang bersifat rahasia, yang bocor ke publik. Namun hasil yang ditemukan tidak ada yang menandakan bahwa tim keamanan tokopedia sudah sangat baik dalam menyembuntikan dokumen internal mereka dari mesin pencarian seperti google dorking. Namun tidak berhenti disitu, masih dengan menggunakan google dorking saya terus mencari file sensitif yang kemungkinan bocor ke publik, perintah yang saya gunakan yaitu *site:tokopedia.com filetype:pdf*. perintah ini digunakan untuk menampilkan semua file pdf tanpa kata kunci spesifik. Namun lagi lagi hasil yang ditemukan nihil atau tidak ada

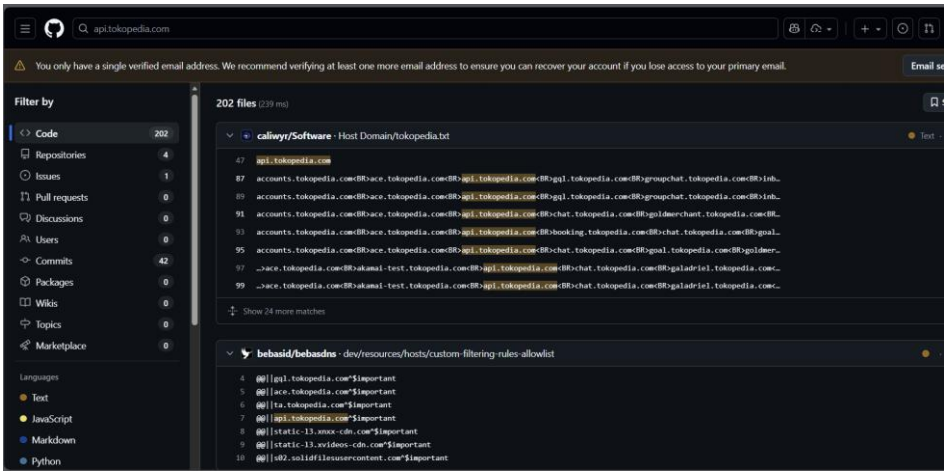


Tidak berhenti sampai disini saja, setelah saya mencari data sensitif menggunakan google dorking, sekarang kita menggunakan GitHub sebagai tempat pencarian informasi sensitif selanjutnya. Seringkali, developer atau pengembang aplikasi tidak sengaja mengunggah kode program yang berisi alamat server internal atau pola API saat mereka membuat aplikasi pribadi yang terhubung ke Tokopedia. Pada tahap ini, pertama saya masuk ke situs GitHub.com kemudian login setelah itu, dikolom pencarian ketik *"tokopedia.com" filename:config*, kode ini berfungsi untuk mencari file konfigurasi yang menyebut nama Tokopedia. Namun lagi lagi hasil yang ditemukan nihil atau tidak ada. Sehingga bisa dibilang keamanan tokopedia memang bekerja.



Tidak berhenti sampai disitu, kita masih terus mencoba mencari sesuatu yang munkin bisa menjadi bahan analisis, disini saya mencoba menggunakan perintah yang lebih umum yaitu *api.tokopedia.com* kode ini berfungsi untuk

menembak langsung ke API server mereka. Dan amazing kita menemukan sesuatu.



Dari hasi pencarian pada repositori kode GitHub menggunakan kata kunci *api.tokopedia.com* yang difilter pada kategori code. Ditemukan sebuah file teks dalam repositori publik yang berisi daftar panjang alamat sub-domain dan endpoint API target, seperti *gql.tokopedia.com* dan *ace.tokopedia.com.*

Meskipun file ini tidak memuat password, temuan ini sangat berbahaya karena membocorkan Peta Infrastruktur (Network Map). Penyerang mendapatkan daftar target valid yang mungkin tidak terdeteksi oleh mesin pencarian biasa seperti google. Informasi ini memungkinkan penyerang untuk langsung menargetkan server spesifik, misalnya server gpl (GraphQL), tanpa perlu melakukan pemindaian jaringan yang berisiko terdeteksi.

Sebagai kesimpulan dari tahap pengumpulan informasi ini, seluruh hasil yang diperoleh dari berbagai metode pencarian telah dirangkum dalam tabel berikut:

No	Informasi Yang Ditemukan	Sumber (Alat/Website)	Alasan Relevansi
1	A. Domain yang ditemukan adalah tokopedia.com B. Sub-domain yang ditemukan diantaranya :	Google Dorks (site:tokopedia.com -www)	A. Informasi ini penting karena ini adalah titik masuk

	• Accounts.tokopedia.com • Shop-id.tokopedia.com • Seller.tokopedia.com • Kamus.tokopedia.com • Seller.id.tokopedia.com • Affiliate-id.tokopedia.com		autentikasi. Ini rentan terhadap serangan Phishing atau Credential Harvesting untuk mencuri data pengguna. B. Informasi sub-domain karena portal ini memberikan akses ke fungsi bisnis dan data keuangan. Pengambilalihan akun disini beresiko menyebabkan kerugian finansial dan kobocoran data pelanggan.
2	A. Format email standar yang digunakan perusahaan tokopedia yaitu {first}.{last}@tokopedia.com B. 3 nama keryawan di level teknis serta jabatannya yaitu :	Google Dorks • "Tokopedia" email format hunter.io • site:id.linkedin.com/in/ "Tokopedia" AND	Akun level eksekutif memiliki akses luas ke data strategis. VP Engineering kemungkinan memiliki akses administratif ke infrastruktur kritis.

	• Melisa Siska Juminto (President Director) • Frans Kurniawan (Tech & Product Leader) • Doni Hanafi (VP of Engineering)	("Security" OR "Engineering" OR "Head")	Jika akun mereka jebol, dampaknya katastropik bagi perusahaan
3	Teknologi yang digunakan antara lain yaitu • CDN: Akamai Edge • Web Server: Tengine • Framework: React	BuiltWith.com	• Penyembunyian IP Asli & WAF. Akamai melindungi server asli. Penyerang tahu bahwa serangan langsung mungkin akan diblokir, sehingga perlu mencari cela miskonfigurasi pada WAF atau mencari IP asli yang bocor. • Fingerprinting Server: mengetahui versi Tengine (basis Nginx) membantu penyerang mencari CVE spesifik atau kelemahan konfigurasi default

			yang belum ditutup oleh admin • Client-side Attact Surface: Aplikasi Reace sangat bergantung pada API. Ini memberi sinyal pada penyerang untuk memburu cela keamanan pada API (seperti IDOR atau Broken Access Control) dan kerentanan XSS jika pengembang tidak hati hati memfilter input
4	Daftar Endpoint API (gql, ace, api)	Githup Search (code)	Ditemukannya file teks berisi daftar domain internal API publik memberikan peta jaringan instan bagi penyerang untuk menargetkan layanan backend spesifik tanpa perlu melakukan pemindaian aktif yang berisiko.

ACTIVE RECONNAISSANCE (Pengintaian Aktif)

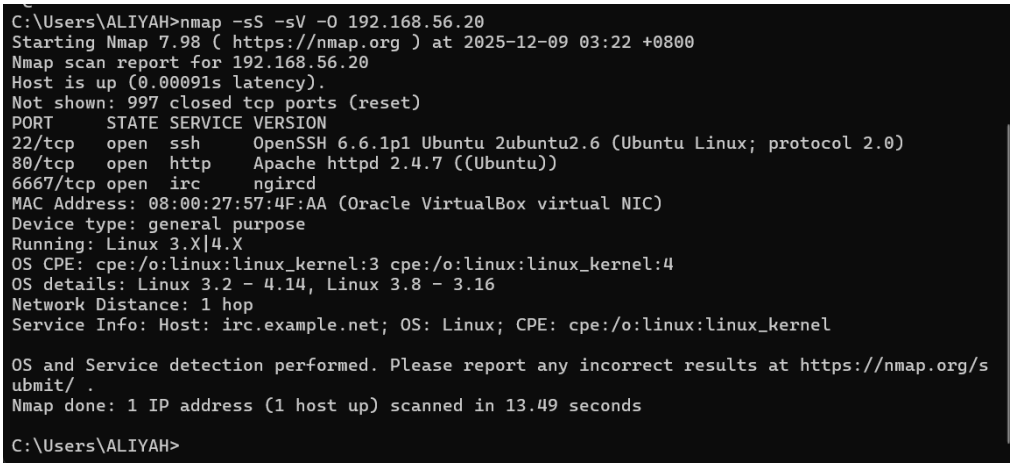
Setelah selesai mengumpulkan informasi publik (Passive Recon) sekarang kita masuk pada tahapan Active reconnaissance. Ditahap ini, kita akan berinteraksi langsung dengan jaringan target untuk mencari tahu "Pintu" mana saja yang terbuka dan layanan apa yang sedang berjalan di dalamnya.

Tujuan utama dari fase ini adalah untuk memetakan topologi jaringan (Network Discovery), mengidentifikasi port yang terbuka serta mendeteksi jenis layanan dan versi sistem operasi berjalan di sisi target. Informasi ini sangat krusial untuk menemukan cela keamanan spesifik yang dpaat dieksploitasi.

Target yang digunakan dalam simulasi ini adalah VulnOS dengan IP yang ditemukan yaitu 192.168.56.20. sebelum memulai melakukan scanning, terlebih dahulu siap kan lab dan alat yang akan digunakan, berhubung karena kali linux saya bermasalah, pada tahap ini saya akan langsung scanning melalu windows dengan terlebih dahulu mendownload dan menginstall nmap pada website resmi nmap Nmap: the Network Mapper - Free Security Scanner . Setelah alat dan target tersedia, kita akan masuk di bagian scanning untuk memindai target. Ada beberapa poin yang akan dilakukan pada tahapan Active reconnaissance ini yaitu:

1. **Host Discovery dan Port Scanning**

   Setelah berhasil mengidentifikasi bahwa target vulnOS aktif pada alamat IP 192.168.56.20, Tahap awal dari pengintaian aktif adalah memastikan target dapat dijangkau (*Host Discovery*) dan memetakan pintu akses jaringan yang terbuka (*Port Scanning*). Tujuan dari langkah ini adalah untuk mendapatkan daftar alamat IP yang aktif dan mengetahui layanan apa saja yang terekspos ke jaringan, baik melalui protokol TCP maupun UDP. Untuk melakukan hal ini, digunakan alat Nmap melalui Command Prompt dengan serangkaian parameter khusus agar informasi yang didapatkan bersifat menyeluruh dalam sekali eksekusi.



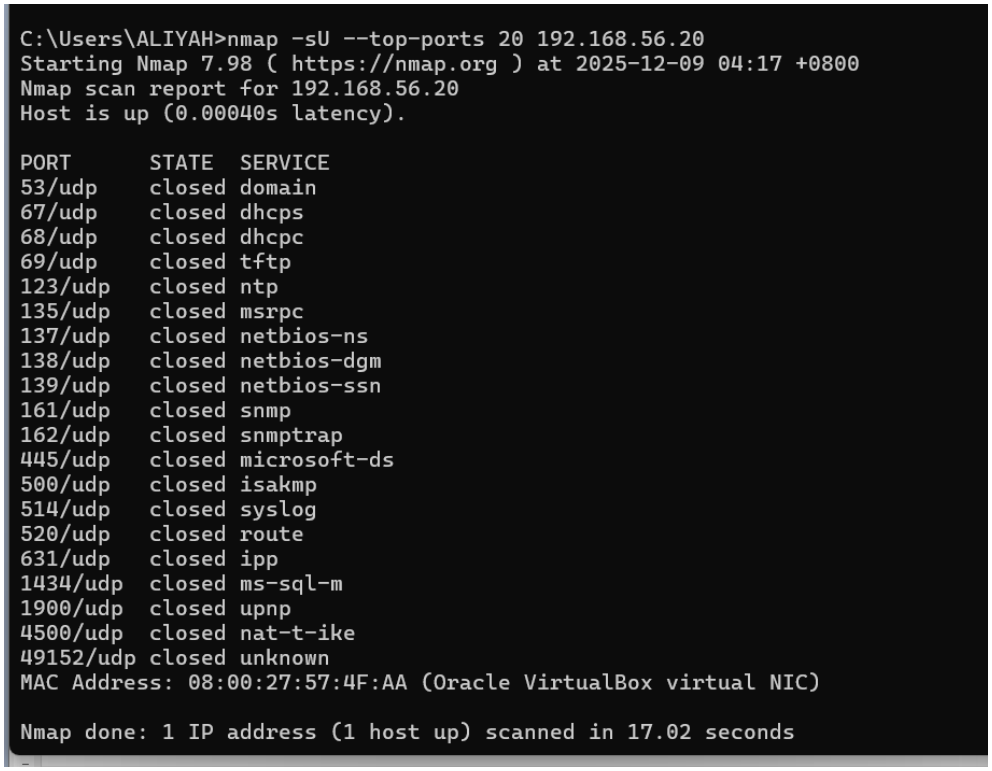
Pada gambar diatas menampilkan hasil output dari pemindaian Nmap. Perintah yang dijalankan adalah nmap -sS -sV -0 192.168.56.20. -sS (TCP SYN Scan): Digunakan untuk melakukan pemindaian stealth (diam-diam) dengan mengirimkan paket SYN tanpa menyelesaikan koneksi TCP penuh. Ini membuat proses scan lebih cepat.

Berdasarkan hasil pemindaian di atas, ditemukan 3 port TCP yang berstatus *open* (terbuka):

- Port 22 (SSH): Layanan akses jarak jauh.
- Port 80 (HTTP): Layanan web server.
- Port 6667 (IRC): Layanan percakapan *relay chat*.

Penemuan port-port ini mengonfirmasi bahwa target merupakan sebuah server yang menjalankan aplikasi web dan layanan komunikasi, sekaligus membuka permukaan serangan (*attack surface*) awal bagi penguji."

Selain melakuakn TCP Scanning, disini kita juga mencari setidaknya satu port UDP. Dengan melakukan pemindaian terpisah pada 20 port UDP terpopuler (Top Ports). Perintah yang digunakan adalah *nmap -sU --top-ports 20 192.168.56.20.*



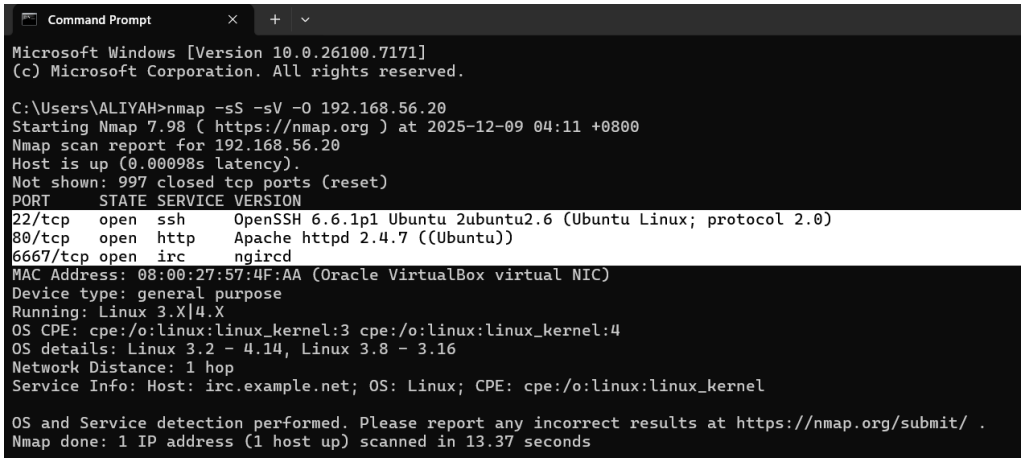
Hasil pemindaian menunjukkan bahwa ke-20 port UDP prioritas termasuk DNS port 53 dan DHCP port 67 berstatus closed. Meskipun tidak ditemukan UDP yang terbuka, informasi ini tetap bernilai karena menunjukkan bahwa target tidak mengekspos layanan UDP standar yang sering menjadi cela keamanan seperti SNMP atau TFTP, atau kemungkinan dilindungi oleh firewall yang menolah paket UDP masuk.

2. Service and Version Detection

Setelah mengetahui port mana saja yang terbuka, langkah selanjutnya adalah melakukan interogasi mendalam untuk mengetahui identitas layanan (service) dan versi perangkat lunak yang berjalan di balik port tersebut. Informasi versi ini sangat vital karena kerentanan keamanan (CVE) biasanya melekat pada versi spesifik dari sebuah perangkat lunak.

Untuk melakukan hal ini, digunakan perintah Nmap dengan penambahan parameter -sV (Version Detection). Parameter ini memerintahkan Nmap untuk

menganalisis respon dari target dan mencocokkannya dengan basis data tanda tangan layanan (nmap-service-probes).



Berdasarkan hasil scannya, ditemukan 3 port utama yang terbuka yaitu:

Port	State	Service	Version Detected
22/tcp	Open	SSH	OpenSSH 6.6.1p1 ubuntu 2ubuntu2.6
80/tcp	Open	HTTP	Apache httpd 2.4.7 ((Ubuntu))
6667/tcp	Open	IRC	ngircd

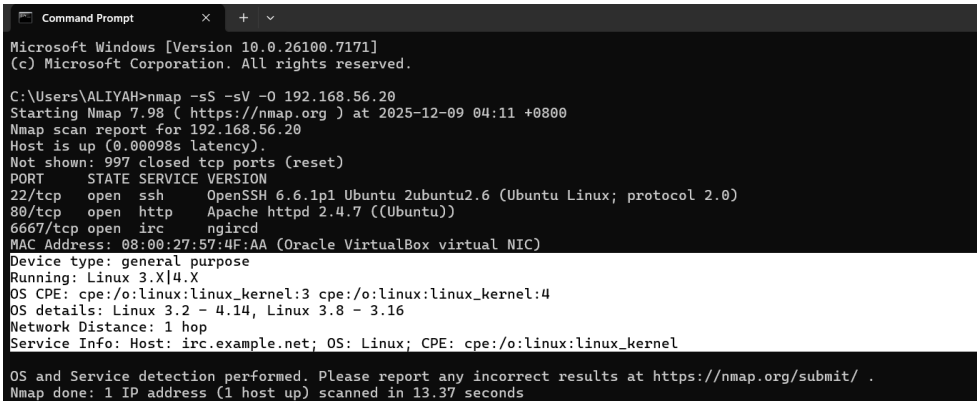
Berdasarkan hasil deteksi tersebut, ditemukan indikasi risiko kemanan yang sangat serius pada target. Pertama, perangkat lunak yang diguanakn tergolong sangat usang (outdated), yakni Apache 2.4.7 dan OpenSSH 6.6.1p1. Kedua versi ini merupakan standar lama dari era tahun 2014 (Ubuntu 14.04) yang diketahui memiliki banyak riwayat kerentanan publik (*Common Vulnerabilities and Exposures* / CVE) yang siap dieksploitasi. Selain masalah versi, keberadaan port 6667 yang menjalankan layanan IRC juga menjadi anomali yang sangat mencurigakan pada sebuah server bisnis. Layanan *chat* kuno ini umumnya tidak terenkripsi, dan dalam konteks simulasi serangan seperti VulnOS, port ini sering kali menjadi indikator kuat adanya jalur akses tersembunyi (*backdoor*) yang sengaja dibuka sebagai celah masuk utama bagi penyerang.

3. OS Fingerprinting

Selain mengetahui layanan aplikasi, mengetahui jenis Sistem Operasi (OS) yang digunakan target adalah langkah krusial dalam Active Reconnaissance.

Informasi ini membantu penyerang untuk mempersempit jenis serangan yang efektif (misalnya: tidak mungkin menggunakan virus .exe Windows pada server Linux).

Untuk tujuan ini, digunakan parameter -O (OS Detection) pada perintah Nmap. Parameter ini bekerja dengan cara mengirimkan serangkaian paket TCP/IP khusus ke target dan menganalisis karakteristik respon teknisnya (seperti nilai TTL, Window Size, dan flag TCP) untuk dicocokkan dengan database sidik jari sistem operasi Nmap.



Berdasarkan baris output Device type, Running, dan OS details pada gambar di atas, diperoleh informasi sebagai berikut:

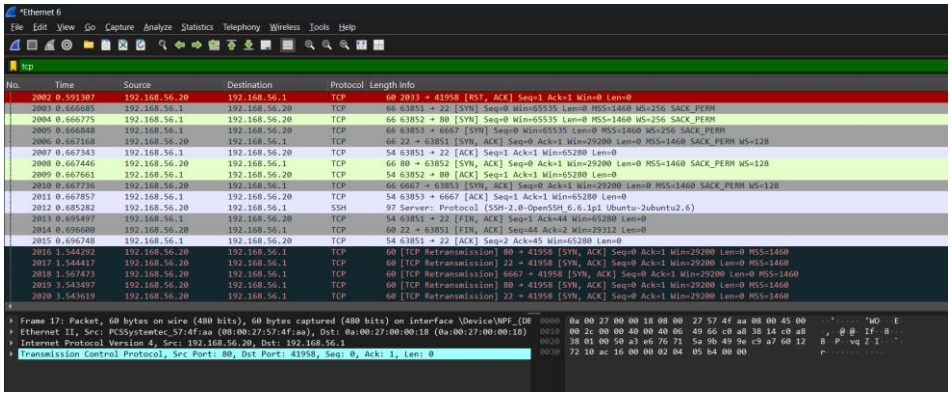
- Tipe Perangkat: General purpose (Komputer umum/Server).
- Prediksi OS: Linux 3.X | 4.X.
- Detail OS: Linux Kernel versi 3.2 hingga 4.14, Linux 3.8 – 3.16

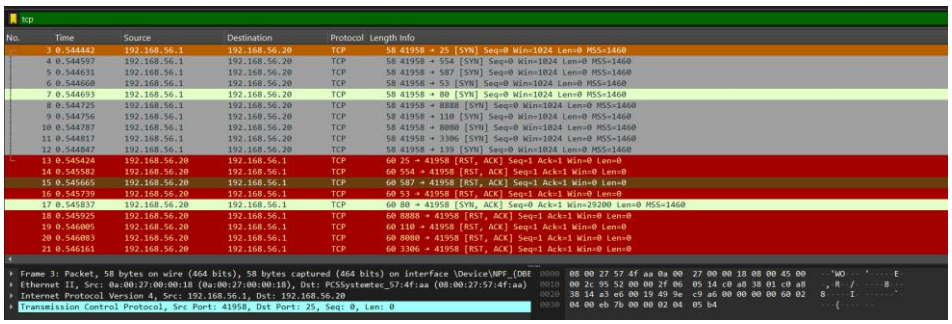
Nmap mendeteksi dengan probabilitas tinggi bahwa target menjalankan sistem operasi berbasis Linux. Jika data ini dikorelasikan dengan hasil Service Detection sebelumnya (yang menemukan 'Ubuntu' pada banner SSH dan HTTP), dapat disimpulkan secara akurat bahwa target adalah Linux Ubuntu versi lawas (dengan Kernel 3.x/4.x). Mengetahui versi OS yang spesifik ini sangat berbahaya karena membuka peluang bagi penyerang untuk mencari eksploitasi level kernel (Kernel Exploits) untuk mendapatkan hak akses root, seperti kerentanan Dirty COW yang terkenal pada kernel versi tersebut.

4. Network Protocol Analisis

Sebagai langkah validasi teknis (technical validation), dilakukan analisis lalu lintas jaringan (traffic capture) secara real-time menggunakan Wireshark selama proses pemindaian Nmap berlangsung. Tujuan dari langkah ini adalah untuk membedah paket data yang dikirimkan oleh mesin penyerang dan melihat bagaimana respon mesin target di tingkat protokol jaringan.

Analisis ini bertujuan untuk membuktikan secara visual bagaimana perintah nmap -sS (TCP SYN Scan) bekerja 'di balik layar', yaitu dengan memanipulasi bendera (flag) pada header TCP untuk memetakan port tanpa menyelesaikan koneksi penuh (handshake).





Berdasarkan hasil tangkapan layar Wireshark di atas, berikut adalah analisis mendalam mengenai protokol yang teridentifikasi selama proses pemindaian:

A. Protokol ARP (Address Resolution Protocol)

Sebelum paket Nmap dikirim, terlihat adanya paket ARP Request. Komputer penyerang bertanya "Who has 192.168.56.20?". Ini adalah

langkah fundamental di mana penyerang mencari alamat fisik (MAC Address) dari target sebelum komunikasi TCP/IP dapat dimulai.

B. Mekanisme TCP SYN Scan (-sS)

Visualisasi Wireshark mengonfirmasi mekanika perintah nmap -sS. Terlihat dominasi paket berwarna abu-abu/hijau dengan bendera [SYN].

- Indikator Port Terbuka (Open): Pada port 22, 80, dan 6667, terlihat pola: Penyerang mengirim [SYN] $\rightarrow$ Target membalas [SYN, ACK]. Ini menandakan layanan aktif menerima koneksi. Nmap kemudian memutusnya dengan [RST] agar tidak terjadi koneksi penuh (*stealth*).
- Indikator Port Tertutup (Closed): Pada port acak lainnya (seperti port 25 atau 41958), terlihat pola: Penyerang mengirim [SYN] $\rightarrow$ Target membalas [RST, ACK]. Paket *Reset* (RST) ini adalah cara target memberitahu bahwa "Pintu tertutup, jangan masuk".

C. Korelasi dengan Hasil Output Nmap

Lalu lintas jaringan ini secara akurat menghasilkan output Nmap yang melaporkan tiga layanan spesifik:

- SSH (Port 22): Teridentifikasi OpenSSH versi lawas.
- HTTP (Port 80): Teridentifikasi Apache Web Server.
- IRC (Port 6667): Teridentifikasi layanan ngircd.

Analisis paket ini memvalidasi bahwa target memiliki kelemahan pada protokol TCP, di mana layanan-layanan kritis (Web dan Remote Access) terekspos tanpa perlindungan firewall yang memadai (seperti IDS/IPS), karena paket SYN scan berhasil menembus dan mendapatkan balasan langsung dari sistem operasi target.