LAPORAN TUGAS BESAR

PASSIVE DAN ACTIVE RECONNAISSANCE

OLEH:

NAMA : **ANDINI FEBRIANTI**

KELAS : **5A JK**

NIM : **105841113223**

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH MAKASSAR

2025

SKENARIO OPERASIONAL

Di tengah dunia digital yang penuh risiko, Anda ditunjuk sebagai Konsultan Keamanan Siber dengan misi krusial: mengidentifikasi setiap potensi titik lemah pada sistem target sebelum serangan yang sesungguhnya terjadi. Misi ini dimulai dari fase *Reconnaissance*, tahap pengumpulan intelijen yang senyap dan metodis.

Misi dibagi menjadi dua operasi berbeda. Operasi pertama berfokus pada observasi eksternal (Pasif) terhadap target publik, yaitu Portal Web Resmi Pemerintah Kabupaten Maros (maroskab.go.id). Di sini, aturan etika sangat ketat: tidak ada interaksi langsung, hanya pengumpulan informasi dari sumber terbuka (OSINT) untuk memetakan wajah publik organisasi tersebut.

Operasi kedua bergeser ke lingkungan yang terkendali, sebuah Mesin Virtual Lab Rentan dengan IP 172.20.10.4. Di sinilah aktivitas pemindaian intensif (*Active Reconnaissance*) diizinkan. Dengan *platform* Kali Linux dan *tools* canggih seperti Nmap dan Wireshark, tujuan adalah mengungkap setiap *port* yang terbuka, mengidentifikasi layanan yang usang, hingga memastikan jenis sistem operasi target.

Hasil dari kedua operasi ini akan menjadi peta harta karun bagi *hacker*—peta yang menunjukkan jalur masuk paling mudah (*entry point*) dan menetapkan target mana yang akan dieksploitasi di fase berikutnya**.**

1. PENDAHULUAN

Transisi menuju ekosistem digital telah menempatkan keamanan informasi sebagai pilar utama dalam menjamin keberlangsungan operasional dan menjaga kepercayaan publik. Setiap entitas, baik pemerintah maupun swasta, diwajibkan untuk secara proaktif melindungi aset digital mereka dari berbagai ancaman siber yang terus berkembang. Dalam kerangka kerja *Penetration Testing* (Pentest), fase awal dan paling krusial adalah tahap *Reconnaissance* (*pengintaian* atau *pengumpulan informasi*).

Tahap ini bertujuan untuk membangun peta rinci mengenai target, mengidentifikasi arsitektur jaringan, *host* yang aktif, dan potensi permukaan serangan (*attack surface*) yang dapat dieksploitasi di masa mendatang. Pengumpulan informasi ini secara fundamental memberikan landasan analitis sebelum tindakan intervensi teknis (seperti eksploitasi) dilakukan.

2. RUANG LINGKUP & SKENARIO PENGUJIAN

a. **Peran dan Tujuan**

- **Peran :** Konsultan Keamanan Siber
- **Tujuan :** Mengumpulkan informasi terkait infrastruktur target dan menemukan potensi titik masuk (entry point)

b. **Target Pengujian**

- **Passive Recconnaissance**

  Target : Website Pemerintah Kabupatem Maros (maroskab.go.id)
- **Active Recconnaissance**

  Target : VM Lab Rentan – **IP: 172.20.10.4**

c. **Rules of Engagement**

Penting untuk dicatat bahwa semua pemindaian aktif, seperti *port scanning* dan analisis trafik, hanya kami lakukan pada mesin yang ada di lab (IP 172.20.10.4). Sementara itu, saat mengamati *website* publik, kami hanya melakukan pengintaian pasif. Ini berarti tidak ada interaksi langsung atau aktivitas yang berpotensi merusak kami lakukan pada target publik, sehingga proses pengumpulan informasi tetap aman dan sesuai etika.

3. TOOLS & LINGKUNGAN PENGUJIAN

a. **Alat (Tools) dan Fungsinya**

- **Kali Linux :** digunakan sebagai lingkungan dasar untuk pengujian keamanan siber.
- **Netdiscover :** Digunakan untuk host discovery (penemuan host aktif) pada jaringan lokal melalui permintaan ARP.
- **Nmap :** Melaksanakan pemindaian port, identifikasi layanan (service), dan deteksi sistem operasi (OS fingerprinting).
- **Wireshark :** Berfungsi sebagai packet sniffer untuk analisis mendalam terhadap protokol dan lalu lintas jaringan (network traffic analysis).
- **Crt.sh :** Digunakan untuk pemetaan subdomain dan pengumpulan informasi melalui catatan Certificate Transparency.
- **Builtwith :** Melakukan identifikasi teknologi yang digunakan oleh situs web target, seperti frameworks dan web server.

- **Github Server :** Dioptimalkan untuk pencarian informasi sensitif yang terekspos dalam kode publik (code repositories).

4. METODOLOGI RECONNAISSANCE

Tahapan yang digunakan

a. Passive recconnaissance

- **Pengumpulan Data OSINT (Open Source Intelligence):**
  Tahap ini bertujuan untuk mengumpulkan informasi relevan mengenai target dari sumber-sumber yang tersedia secara publik (misalnya, melalui *tools* seperti crt.sh dan GitHub Search).
- **Non-Interaksi dengan Server:**
  Seluruh aktivitas dalam fase ini dilakukan tanpa *melibatkan* komunikasi langsung atau pengiriman paket data ke server target.

b. Active Recconnaissance

- **Pemindaian Port dan Layanan (Service Enumeration)**:
  Melakukan pemindaian langsung (misalnya, menggunakan Nmap) terhadap alamat host target di lingkungan lab untuk mengidentifikasi port TCP/UDP yang terbuka dan layanan (service) yang berjalan pada port tersebut.
- **Identifikasi Sistem dan Protokol Jaringan:**
  Menganalisis respons dari *host* target untuk mengidentifikasi Sistem Operasi (*OS Fingerprinting*) dan memastikan protokol jaringan yang digunakan untuk komunikasi (misalnya, melalui Wireshark).

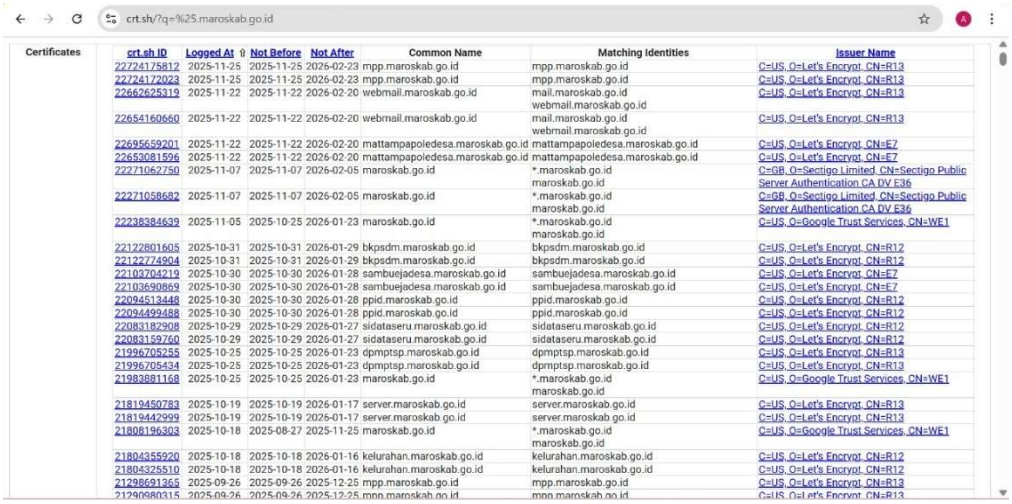
5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

Kategori Informasi	Informasi yang ditemukan	Alat / website	Alasan relevansi
Pencarian Sub-Domain	http://bkpsdm.maroskab.go.id http://mpp.maroskab.go.id http://mattampapoledesa.maroskab.go.id http://server.maroskab.go.id	Crt.sh crt.sh | %.maroskab.go.id	Menunjukkan permukaan serangan (attack surface) yang lebih luas.

	http://lpse.maroskab.go.id		
Informasi Karyawan	Muhammad Taufan (Kabid Dinas Komunikasi dan Informatika) Ihsan Najamuddin (Kabid Diseminasi Komunikasi dan Informasi Publik) Sumartini (Kabid Pengelolaan Data dan Layanan Publik)	PDF	Untuk memahami struktur organisasi dan pihak yang relevan.
Format Email	info@maroskab.go.id	https://maroskab.go.id/	Digunakan untuk validasi pola email dalam simulasi keamanan.
Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith https://builtwith.com/%20maroskab.go.id/	Menunjukkan penggunaan WAF dan potensi analisis keamanan sisi klien.
Informasi Sensitif Terpapar	Tidak ditemukan adanya informasi sensitif yang terekspos langsung ke publik (seperti *key* API atau kredensial yang *hardcoded*).	GitHub Search (OSINT)	Tidak **ditemukan** informasi sensitif yang terekspos secara publik **mengindikasikan** bahwa target (situs *website* publik) tela**menerapkan** praktik keamanan yang baik dalam manajemen kodenya.

a. Bukti dokumentasi

1. Pencarian Domain dan Sub-domain



crt.sh/?q=%25.maroskab.go.id

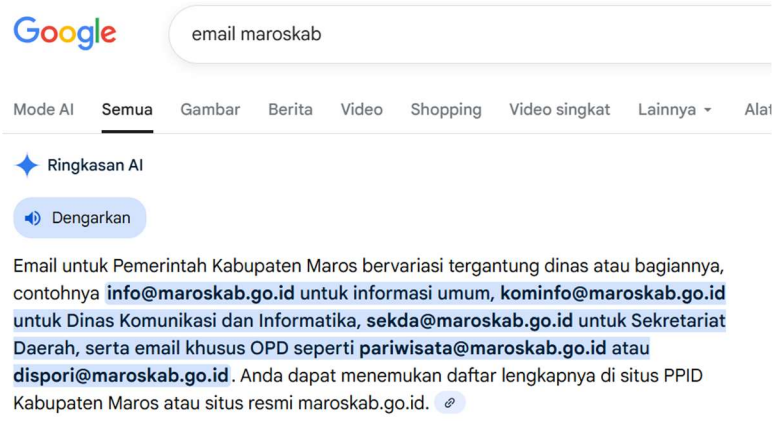
Certificates

crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
22724175812	2025-11-25	2025-11-25	2026-02-23	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
22724172023	2025-11-25	2025-11-25	2026-02-23	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
22662625319	2025-11-22	2025-11-22	2026-02-20	webmail.maroskab.go.id	mail.maroskab.go.id webmail.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
22654160660	2025-11-22	2025-11-22	2026-02-20	webmail.maroskab.go.id	mail.maroskab.go.id webmail.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
22695659201	2025-11-22	2025-11-22	2026-02-20	mattampapoledesa.maroskab.go.id	mattampapoledesa.maroskab.go.id	C=US, O=Let's Encrypt, CN=E7
22653081596	2025-11-22	2025-11-22	2026-02-20	mattampapoledesa.maroskab.go.id	mattampapoledesa.maroskab.go.id	C=US, O=Let's Encrypt, CN=E7
22271062750	2025-11-07	2025-11-07	2026-02-05	maroskab.go.id	*.maroskab.go.id maroskab.go.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV E36
22271058682	2025-11-07	2025-11-07	2026-02-05	maroskab.go.id	*.maroskab.go.id maroskab.go.id	C=GB, O=Sectigo Limited, CN=Sectigo Public Server Authentication CA DV E36
22238384639	2025-11-05	2025-10-25	2026-01-23	maroskab.go.id	*.maroskab.go.id maroskab.go.id	C=US, O=Google Trust Services, CN=WE1
22122801605	2025-10-31	2025-10-31	2026-01-29	bkpsdm.maroskab.go.id	bkpsdm.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
22122774904	2025-10-31	2025-10-31	2026-01-29	bkpsdm.maroskab.go.id	bkpsdm.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
22103704219	2025-10-30	2025-10-30	2026-01-28	sambuejadesa.maroskab.go.id	sambuejadesa.maroskab.go.id	C=US, O=Let's Encrypt, CN=E7
22103690869	2025-10-30	2025-10-30	2026-01-28	sambuejadesa.maroskab.go.id	sambuejadesa.maroskab.go.id	C=US, O=Let's Encrypt, CN=E7
22094513448	2025-10-30	2025-10-30	2026-01-28	ppid.maroskab.go.id	ppid.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
22094499488	2025-10-30	2025-10-30	2026-01-28	ppid.maroskab.go.id	ppid.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
22083182908	2025-10-29	2025-10-29	2026-01-27	sidataseru.maroskab.go.id	sidataseru.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
22083159760	2025-10-29	2025-10-29	2026-01-27	sidataseru.maroskab.go.id	sidataseru.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
21996705255	2025-10-25	2025-10-25	2026-01-23	dpmptsp.maroskab.go.id	dpmptsp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
21996705434	2025-10-25	2025-10-25	2026-01-23	dpmptsp.maroskab.go.id	dpmptsp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
21983881168	2025-10-25	2025-10-25	2026-01-23	maroskab.go.id	*.maroskab.go.id maroskab.go.id	C=US, O=Google Trust Services, CN=WE1
21819450783	2025-10-19	2025-10-19	2026-01-17	server.maroskab.go.id	server.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
21819442999	2025-10-19	2025-10-19	2026-01-17	server.maroskab.go.id	server.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
21808196303	2025-10-18	2025-08-27	2025-11-25	maroskab.go.id	*.maroskab.go.id maroskab.go.id	C=US, O=Google Trust Services, CN=WE1
21804355920	2025-10-18	2025-10-18	2026-01-16	kelurahan.maroskab.go.id	kelurahan.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
21804325510	2025-10-18	2025-10-18	2026-01-16	kelurahan.maroskab.go.id	kelurahan.maroskab.go.id	C=US, O=Let's Encrypt, CN=R12
21298691365	2025-09-26	2025-09-26	2025-12-25	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
21290980315	2025-09-26	2025-09-26	2025-12-25	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13

Menampilkan daftar subdomain yang terdaftar pada sertifikat SSL, memperluas attack surface.

2. Informasi dan Email karyawan

- Informasi email



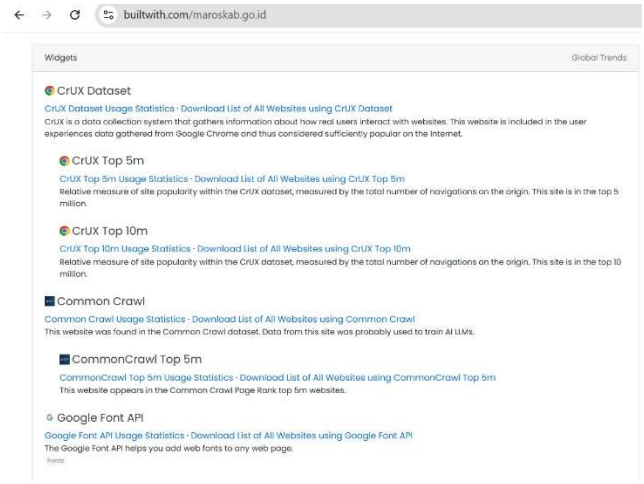
Penemuan alamat email generik (info@maroskab.go.id) yang memvalidasi format domain email organisasi.

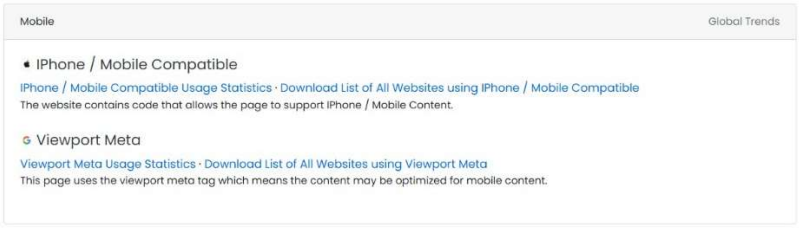
- Karyawan diskominfo

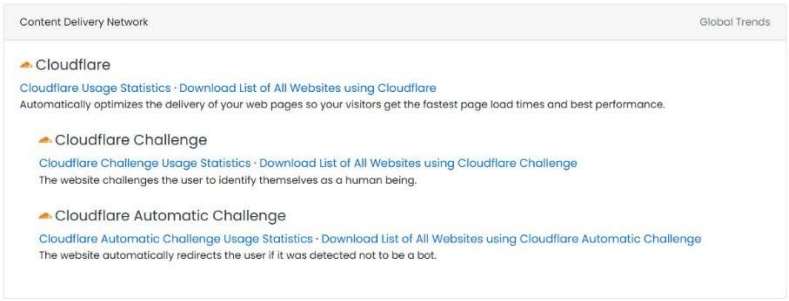
No.	Nama	NIP	Jabatan-Unit Kerja-Subunit Kerja	NHK	Status Akun WL	Tahun WL	Jenis Laporan	Status Pelapora
29	SUMARTINI	'196911151989032004	KEPALA BIDANG PENGELOLAAN DATA DAN LAYANAN PUBLIK - DINAS KOMUNIKASI DAN INFORMATIKA - BIDANG PENGELOLAAN DATA DAN LAYANAN PUBLIK	441042	Online	2020	Periodik	Sudah Lapor
156	MUHAMMAD TAUFAN	'198407312003121001	KEPALA BIDANG - DINAS KOMUNIKASI DAN INFORMATIKA - BIDANG LAYANAN E-GOVERNMENT	719444	Online	2020	Periodik	Sudah Lapor
82	IHSAN NADJAMUDDIN	'197208082001121005	KEPALA BIDANG DISEMINASI KOMUNIKASI DAN INFORMASI PUBLIK - DINAS KOMUNIKASI DAN INFORMATIKA - BIDANG DISEMINASI KOMUNIKASI DAN INFORMASI PUBLIK	144339	Online	2020	Periodik	Sudah Lapor

Pengumpulan data personel kunci (High-Value Targets) melalui halaman profil publik untuk pemetaan struktur organisasi.

3. Teknologi yang digunakan

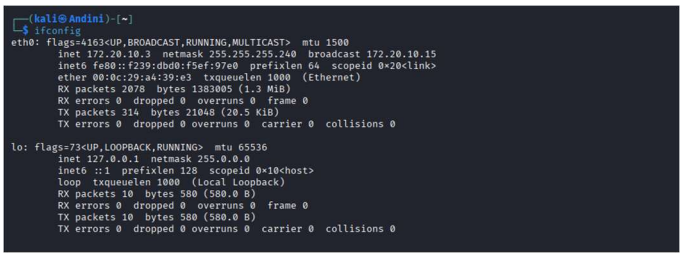






Deteksi penggunaan Cloudflare dan daftar pejabat terkait yang rentan terhadap serangan Social Engineering.

6. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)



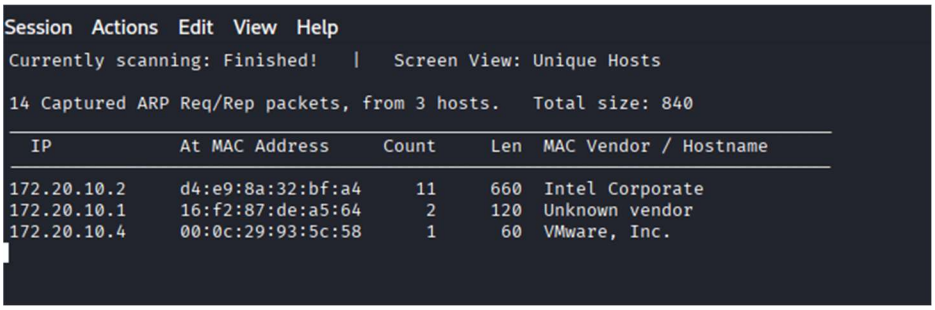
Sebelum melanjutkan ke tahap pemindaian aktif (Active Reconnaissance), verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah ip a dan ifconfig. Output dari perintah tersebut mengidentifikasi bahwa interface eth0

memiliki alamat IP 172.20.10.4 dengan netmask 255.255.255.240. Konfigurasi ini secara kritis mengonfirmasi bahwa host penyerang berada dalam satu segmen jaringan (subnet) yang sama dengan target pengujian. Kesamaan segmen jaringan ini memvalidasi skenario Internal Network Attack, memastikan konektivitas pada Layer 2 (Data Link) dan memungkinkan efektivitas teknik ARP Scanning. Selain itu, berada pada subnet yang sama menjamin bahwa paket probe dari tools seperti Nmap dapat mencapai target secara langsung tanpa perlu melintasi Network Firewall atau perangkat router eksternal yang berpotensi menghalangi proses scanning.

a. Host Discovery dan Port Scanning

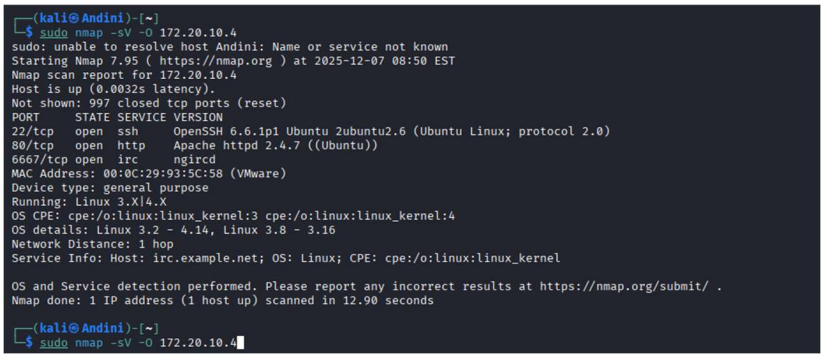
Tugas	Command	Hasil	Potensi Dampak
Host Discovery	sudo netdiscover -r 172.20.10.0/24	Target ditemukan: 172.20.10.4	Memastikan host aktif di jaringan.
TCP SYN Scan	sudo nmap -sS 172.20.10.4	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	sudo nmap -sU --top ports 20 172.20.10.4	Open/Filtered: 53, 67,68	DNS dan DHCP berpotensi menjadi target analisis.

- **Dokumentasi**
  - Host discovery



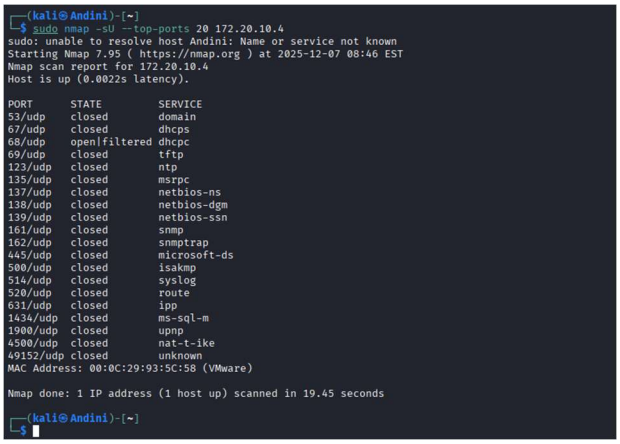
Mengidentifikasi host yang aktif. Target 172.20.10.4 teridentifikasi menggunakan vendor VMware (volunsOS)

– TCP SYN scan



Menemukan port TCP terbuka (22, 80, 6667) tanpa menyelesaikan 3-way handshake

– UDP scn



Identifikasi layanan berbasis UDP seperti DNS (53) dan DHCP (67) yang berstatus open/filtered

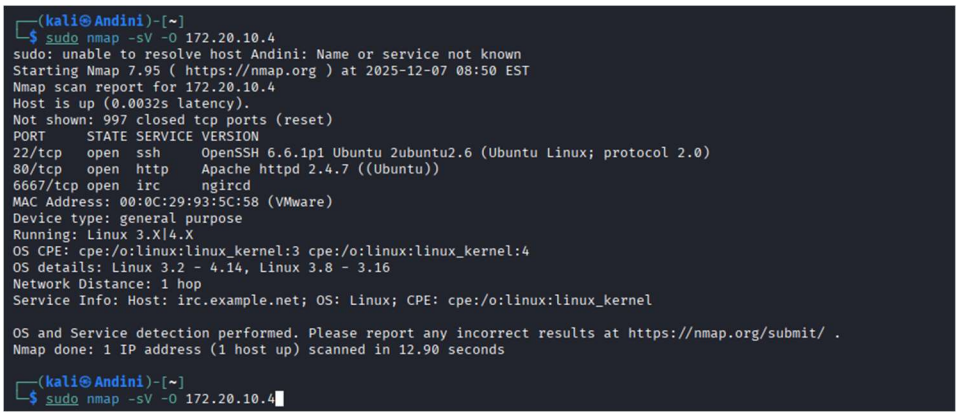
b. Service and Version Detection

sudo nmap -sV 172.20.10.4

Port	Service	Version	Analisis Risiko
22	SSH	OpenSSH 6.6.1p1	Versi lama SSH (rilisan tahun 2014) berpotensi memiliki celah keamanan yang sudah dipublikasikan. Risiko utama meliputi potensi *brute force*, *enumeration* nama pengguna, atau

			serangan yang menargetkan *bug* spesifik pada versi 6.6.1p1.
80	HTTP	Apache 2.4.7	Banyak CVE publik untuk versi lama.
6667	IRC	Ngircd	Ditemukannya *Port* 6667 dengan layanan ngircd merupakan anomali signifikan untuk server yang diasumsikan sebagai *server* umum. *Port* ini sering dikaitkan dengan *backdoor*, *botnet* untuk *Command & Control* (C2), atau *vulnerability* pada implementasi IRC. Ini menjadi prioritas utama untuk tahap eksploitasi selanjutnya

- Bukti service detection



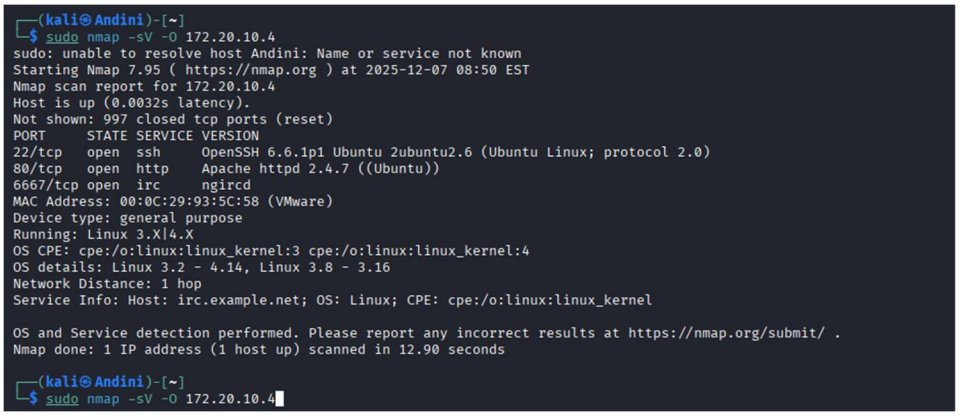
Target teridentifikasi menggunakan Ubuntu Linux lawas dengan layanan OpenSSH 6.6.1p1 dan Apache 2.4.7.

c. OS Fingerprinting

Hasil	Detail OS	Analisis
OS Terdeteksi	Linux Kernel 3.x – 4.x	Berdasarkan hasil pemindaian, Nmap memprediksi bahwa sistem operasi target berjalan di atas Kernel Linux versi 3.2 – 4.14. Temuan ini sangat kritis karena kernel versi

		lawas tersebut umumnya diasosiasikan dengan distribusi Linux lama (seperti Ubuntu 14.04 Trusty Tahr). Sistem operasi yang sudah mencapai status *End-of-Life (EOL)* tidak lagi menerima pembaruan keamanan, sehingga sangat rentan terhadap serangan *Kernel Exploit* lokal (misalnya kerentanan *Dirty COW* - CVE-2016-5195) yang memungkinkan penyerang menaikkan hak akses (*Privilege Escalation*) menjadi *root*.

- Bukti Dokumentasi



Deteksi kernel Linux versi 3.x - 4.x menggunakan opsi -O pada Nmap, mengindikasikan target menggunakan sistem operasi yang sudah usang (End-of-Life).

d. Network Protocol Analysis

Tools : wireshark

Melalui pemeriksaan mendalam pada tangkapan lalu lintas (packet capture) Wireshark, teramati adanya pola anomali dalam proses pembentukan koneksi TCP Three-Way Handshake. Urutan komunikasi standar (SYN $\rightarrow$ SYN-ACK $\rightarrow$ ACK) tidak diselesaikan secara normal.

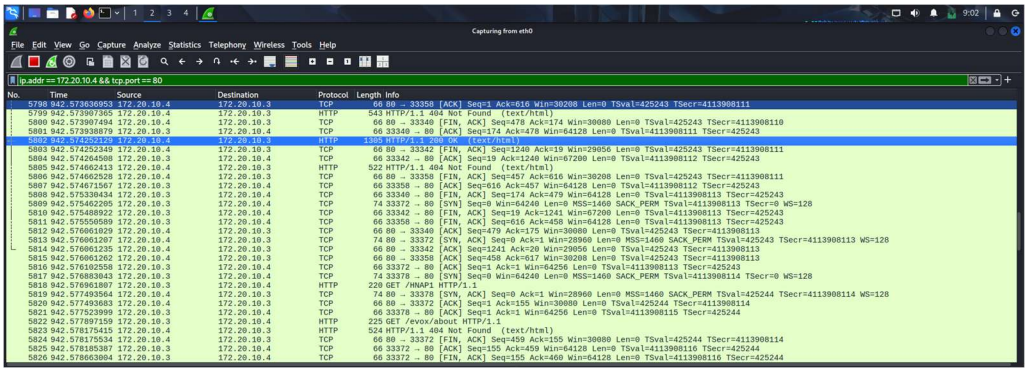
Secara spesifik, pola yang terekam adalah sebagai berikut:

1. Host Penyerang mengirim paket SYN (Synchronize) ke port target.

2. Host Target merespons dengan paket SYN-ACK (Synchronize-Acknowledge), yang mengindikasikan bahwa port tersebut berstatus Open (terbuka) dan siap untuk handshake penuh.
3. Alih-alih menyelesaikan koneksi dengan paket ACK, Host Penyerang justru menghentikan proses dengan mengirim paket RST (Reset).

Pola pemutusan tiba-tiba ini secara teknis memvalidasi penggunaan metode TCP SYN Scan (Stealth Scan) yang diaktifkan oleh opsi -sS pada tool Nmap. Teknik ini dikenal sebagai Half-Open Scanning karena koneksi TCP tidak pernah dibentuk secara lengkap. Tujuan utama dari metode Stealth Scan ini adalah untuk mendeteksi port terbuka sambil meminimalkan jejak kaki, khususnya untuk menghindari pencatatan (logging) pada lapisan aplikasi web server target, yang umumnya hanya mencatat sesi yang berhasil dibuat sepenuhnya.

- Bukti dokumentasi



Menangkap pola scanning Nmap, terlihat adanya paket RST yang dikirimkan kembali oleh attacker.

7. KESIMPULAN DAN SARAN

a. Kesimpulan

Fase Reconnaissance telah berhasil mencapai tujuannya, yaitu memetakan attack surface target dan mengidentifikasi titik masuk (entry point) yang dapat dieksploitasi.

1. Passive Reconnaissance (maroskab.go.id):
    - Permukaan Serangan Luas: Ditemukan sejumlah sub domain, menunjukkan attack surface yang luas dan terpisah.

- Eksposur Data Personel: Terkumpulnya data mengenai personel kunci dan format email meningkatkan risiko Social Engineering terhadap organisasi.
- Keamanan Kode Efektif: Tidak ditemukan kebocoran informasi sensitif (seperti key API atau kredensial hardcoded) di ranah publik, mengindikasikan implementasi praktik secure coding yang baik.

2. Active Reconnaissance (VM Lab 172.20.10.4):
   - Anomali Pemindaian: Analisis protokol mengonfirmasi bahwa port scanning dilakukan secara sembunyi-sembunyi (Stealth Scan / Half-Open Scanning) menggunakan paket RST untuk menghindari logging.
   - Kerentanan Kritis OS: Sistem operasi target teridentifikasi menggunakan Linux Kernel versi 3.x–4.x , yang telah mencapai status End-of-Life (EOL). Kerentanan ini menyebabkan host sangat rentan terhadap serangan Kernel Exploit lokal (misalnya Dirty COW - CVE-2016-5195) yang memungkinkan Privilege Escalation ke tingkat root.
   - Layanan Rentan: Tiga port terbuka (22, 80, 6667) menjalankan layanan dengan versi lama dan berisiko, terutama:
     - OpenSSH 6.6.1p1 dan Apache 2.4.7 memiliki banyak CVE publik.
     - Layanan Ngircd pada Port 6667 merupakan anomali signifikan yang menjadi prioritas utama sebagai potensi backdoor atau botnet C2.

b. Saran

Berdasarkan temuan kritis tersebut, direkomendasikan tindakan perbaikan segera (remediation) sebagai berikut:

1. Perbarui dan Migrasi OS (Penting Sekali):
   - Lakukan patch atau migrasi sistem operasi target dari Kernel Linux 3.x–4.x ke versi yang didukung dan terbaru untuk menghilangkan risiko serangan Kernel Exploit.
2. Perbarui Layanan Publik:
   - Tingkatkan versi OpenSSH (22) dan Apache HTTPD (80) ke versi terbaru untuk mengurangi paparan terhadap CVE yang sudah diketahui.
3. Audit dan Nonaktifkan Layanan Anomali:

- Lakukan audit keamanan mendalam terhadap layanan ngircd pada Port 6667. Jika layanan ini tidak diperlukan untuk fungsi bisnis, segera nonaktifkan (disable) dan filter port ini melalui firewall.

4. Tingkatkan Kontrol Data Publik:
    - Tinjau kembali kebijakan publikasi data personel untuk meminimalkan eksposur informasi kunci, sehingga mengurangi risiko keberhasilan serangan Social Engineering