

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 Reconnaissance**
Target : Website Pemerintah Kabupaten Maros (maroskab.go.id)
- **Active Reconnaissance**
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 reconnaissance

- **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 Reconnaissance

- **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).

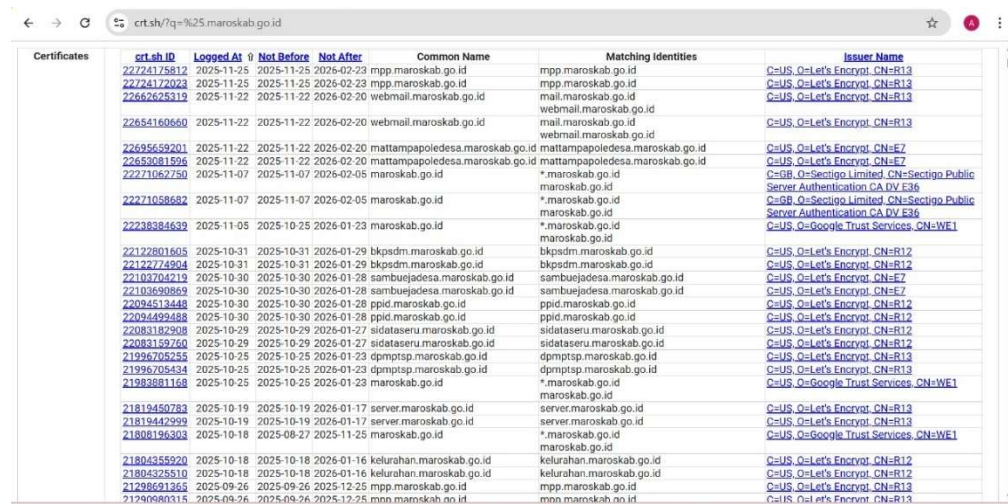
5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

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 https://crt.sh/?q=%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 <i>key</i> API atau kredensial yang <i>hardcoded</i>).	GitHub Search (OSINT)	Tidak ditemukan informasi sensitif yang terekspos secara publik mengindikasikan bahwa target (situs <i>website</i> publik) telamenerapkan praktik keamanan yang baik dalam manajemen kodenya.

a. Bukti dokumentasi

1. Pencarian Domain dan Sub-domain

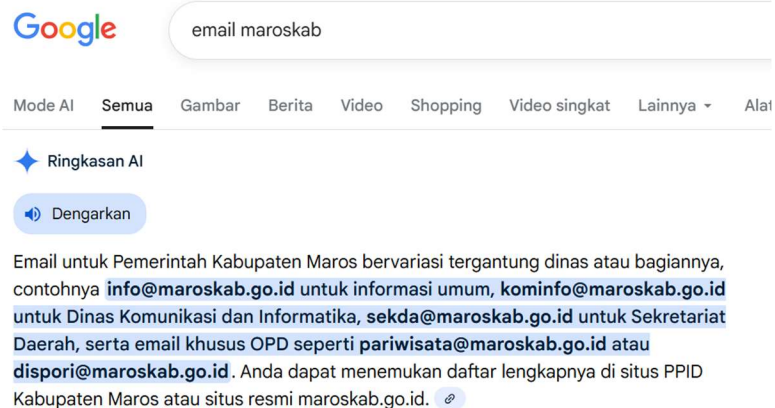


Certificates	crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
	22724175812	2025-11-25	2025-11-25	2026-02-23	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	22724172023	2025-11-25	2025-11-25	2026-02-23	mpp.maroskab.go.id	mpp.maroskab.go.id	C=US, 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
	22695639201	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
	22653081926	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=Secigo Limited, CN=Secigo Public Server Authentication CA OV E36
	22271058682	2025-11-07	2025-11-07	2026-02-05	maroskab.go.id	*.maroskab.go.id maroskab.go.id	C=GB, O=Secigo Limited, CN=Secigo Public Server Authentication CA OV 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	dpmpstp.maroskab.go.id	dpmpstp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21996705434	2025-10-25	2025-10-25	2026-01-23	dpmpstp.maroskab.go.id	dpmpstp.maroskab.go.id	C=US, O=Let's Encrypt, CN=R13
	21983981168	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	mnn.maroskab.go.id	mnn.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



Google search results for "email maroskab".

Mode AI **Semua** Gambar Berita Video Shopping Video singkat Lainnya ▾ Alat

Ringkasan AI

Dengarkan

Email untuk Pemerintah Kabupaten Maros bervariasi tergantung dinas atau bagiannya, contohnya **info@maroskab.go.id** untuk informasi umum, **kominfo@maroskab.go.id** untuk Dinas Komunikasi dan Informatika, **sekda@maroskab.go.id** untuk Sekretariat Daerah, serta email khusus OPD seperti **pariwisata@maroskab.go.id** atau **dispori@maroskab.go.id**. Anda dapat menemukan daftar lengkapnya di situs PPID Kabupaten Maros atau situs resmi maroskab.go.id.

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 Pelaporan
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

builtwith.com/maroskab.go.id

Widgets

Global Trends

CrUX Dataset

[CrUX Dataset Usage Statistics - Download List of All Websites using CrUX Dataset](#)

CrUX is a data collection system that gathers information about how real users interact with websites. This website is included in the user experiences data gathered from Google Chrome and thus considered sufficiently popular on the Internet.

CrUX Top 5m

[CrUX Top 5m Usage Statistics - Download List of All Websites using CrUX Top 5m](#)

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 5 million.

CrUX Top 10m

[CrUX Top 10m Usage Statistics - Download List of All Websites using CrUX Top 10m](#)

Relative measure of site popularity within the CrUX dataset, measured by the total number of navigations on the origin. This site is in the top 10 million.

Common Crawl

[Common Crawl Usage Statistics - Download List of All Websites using Common Crawl](#)

This website was found in the Common Crawl dataset. Data from this site was probably used to train AI LLMs.

CommonCrawl Top 5m

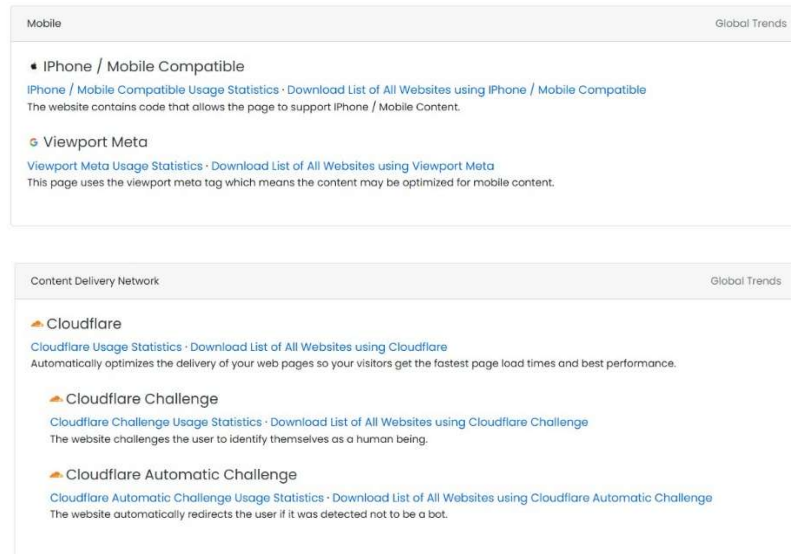
[CommonCrawl Top 5m Usage Statistics - Download List of All Websites using CommonCrawl Top 5m](#)

This website appears in the Common Crawl Page Rank top 5m websites.

Google Font API

[Google Font API Usage Statistics - Download List of All Websites using Google Font API](#)

The Google Font API helps you add web fonts to any web page.



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

6. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)

```
(kali@Andini)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.20.10.3 netmask 255.255.255.240 broadcast 172.20.10.15
    inet6 fe80::f239:dbd0:f5ef:97e0 prefixlen 64 scopeid 0x20<link>
    ether 00:10:c2:9a:44:39:ea txqueuelen 1000 (Ethernet)
    RX packets 2078 bytes 1583005 (1.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 314 bytes 21048 (20.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 10 bytes 580 (580.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10 bytes 580 (580.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Sebelum melanjutkan ke tahap pemindaian aktif (Active Reconnaissance), verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah `ip` 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	<code>sudo netdiscover -r 172.20.10.0/24</code>	Target ditemukan: 172.20.10.4	Memastikan host aktif di jaringan.
TCP SYN Scan	<code>sudo nmap -sS 172.20.10.4</code>	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	<code>sudo nmap -sU --top ports 20 172.20.10.4</code>	Open/Filtered: 53, 67,68	DNS dan DHCP berpotensi menjadi target analisis.

• Dokumentasi

– Host discovery

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
172.20.10.2	d4:e9:8a:32:bf:a4	11	660	Intel Corporate
172.20.10.1	16:f2:87:de:a5:64	2	120	Unknown vendor
172.20.10.4	00:0c:29:93:5c:58	1	60	VMware, Inc.

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

- TCP SYN scan

```
(kali@Andini)-[~]
$ sudo nmap -sV -O 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:50 EST
Nmap scan report for 172.20.10.4
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
6667/tcp  open  irc      ngircd
MAC Address: 00:0C:29:93:5C:58 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 12.90 seconds

(kali@Andini)-[~]
$ sudo nmap -sV -O 172.20.10.4
```

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

- UDP scn

```
(kali@Andini)-[~]
$ sudo nmap -sU --top-ports 20 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:46 EST
Nmap scan report for 172.20.10.4
Host is up (0.0022s latency).
PORT      STATE SERVICE
53/udp    closed domain
67/udp    closed dhcp
68/udp    open|filtered dhcp
69/udp    closed tftp
123/udp   closed ntp
135/udp   closed msrpc
137/udp   closed netbios-ns
138/udp   closed netbios-dgm
139/udp   closed netbios-ssn
161/udp   closed snmp
162/udp   closed snmptrap
445/udp   closed microsoft-ds
500/udp   closed isakmp
514/udp   closed syslog
520/udp   closed route
631/udp   closed ipp
1434/udp  closed ms-sql-m
1900/udp  closed upnp
4500/udp  closed nat-t-lke
49152/udp closed unknown
MAC Address: 00:0C:29:93:5C:58 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 19.45 seconds

(kali@Andini)-[~]
```

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 <i>brute force</i> , <i>enumeration</i> nama pengguna, atau

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

- Bukti service detection

```
(kali@Andini)-[~]
$ sudo nmap -sV -O 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:50 EST
Nmap scan report for 172.20.10.4
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
6667/tcp  open  irc      ngircd
MAC Address: 00:0C:29:93:5C:58 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 12.90 seconds

(kali@Andini)-[~]
$ sudo nmap -sV -O 172.20.10.4
```

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 <i>End-of-Life (EOL)</i> tidak lagi menerima pembaruan keamanan, sehingga sangat rentan terhadap serangan <i>Kernel Exploit</i> lokal (misalnya kerentanan <i>Dirty COW</i> - CVE-2016-5195) yang memungkinkan penyerang menaikkan hak akses (<i>Privilege Escalation</i>) menjadi <i>root</i> .
--	--	--

- Bukti Dokumentasi

```
(kali@Andini)-[~]
$ sudo nmap -sV -O 172.20.10.4
sudo: unable to resolve host Andini: Name or service not known
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 08:50 EST
Nmap scan report for 172.20.10.4
Host is up (0.0032s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.6 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
6667/tcp  open  irc       ngircd
MAC Address: 00:0C:29:93:5C:58 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.14, Linux 3.8 - 3.16
Network Distance: 1 hop
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

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 12.90 seconds

(kali@Andini)-[~]
$ sudo nmap -sV -O 172.20.10.4
```

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.

- Host Target merespons dengan paket SYN-ACK (Synchronize-Acknowledge), yang mengindikasikan bahwa port tersebut berstatus Open (terbuka) dan siap untuk handshake penuh.
- 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

No.	Time	Source	Destination	Protocol	Length	Info
5798	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5799	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5800	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5801	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5802	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5803	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5804	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5805	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5806	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5807	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5808	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5809	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5810	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5811	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5812	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5813	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5814	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5815	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5816	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5817	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5818	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5819	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5820	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5821	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5822	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5823	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5824	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5825	0.42	172.20.10.3	172.20.10.4	TCP	60	80 → 33358 [FIN, ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111
5826	0.42	172.20.10.4	172.20.10.3	TCP	60	33358 → 80 [ACK] Seq=5174 Win=65535 Len=0 TSV=425243 TSecr=4113908111

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.

- 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