

# LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

**NAMA** : IRYAN TEGAR

**NIM** : 10584113023

**KELAS** : 5JKA – ETHICAL HACKING

---

## 1. PENDAHULUAN

Pada era digital saat ini, keamanan informasi menjadi bagian penting dalam menjaga keberlangsungan layanan berbasis teknologi. Setiap organisasi wajib memastikan bahwa sistem yang digunakan terlindungi dari potensi serangan siber. Salah satu langkah awal dalam proses pengujian keamanan adalah tahap reconnaissance, yaitu pengumpulan informasi untuk mengidentifikasi struktur dan potensi kelemahan pada sistem target.

Pada laporan ini dilakukan dua jenis reconnaissance yaitu Passive dan Active Reconnaissance, yang bertujuan untuk mengamati website Pemerintah Kabupaten Gowa sebagai target publik dan mesin rentan pada lingkungan lab sebagai target eksplorasi. Hasil pengumpulan informasi ini akan menjadi dasar dalam tahap eksplorasi berikutnya.

## 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

Fase	Target yang Diaudit
Passive Reconnaissance	Website Pemerintah Kabupaten Gowa ( <i>gowakab.go.id</i> )
Active Reconnaissance	VM Lab Rentan – IP: <b>172.20.10.3</b>

### c. Rules of Engagement

Semua aktivitas pemindaian **aktif** hanya dilakukan pada mesin lab dengan IP 172.20.10.3.

Pada website publik, hanya dilakukan **pengintaian pasif** tanpa interaksi langsung yang berbahaya.

## 3. TOOLS & LINGKUNGAN PENGUJIAN

Tools	Fungsi
Kali Linux	Sistem operasi pengujian keamanan
Netdiscover	Host discovery jaringan
Nmap	Port, service, dan OS scanning
Wireshark	Analisis protokol jaringan

crt.sh	Pemetaan domain & certificate transparency
BuiltWith	Identifikasi teknologi website
GitHub Search	Pencarian informasi sensitif dan kode publik

Lingkungan pengujian dilakukan pada jaringan lokal untuk memastikan legalitas.

#### 4. METODOLOGI RECONNAISSANCE

Tahapan yang digunakan sebagai berikut:

a. Passive Reconnaissance

- Mengumpulkan data melalui OSINT (Open Source Intelligence)
- Tidak berinteraksi langsung dengan server

b. Active Reconnaissance

- Memindai IP target untuk menemukan port dan service terbuka
- Mengidentifikasi OS dan protokol jaringan

## 5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

Target: wakab.go.id

Kategori Informasi	Informasi yang Ditemukan	(Alat/Website)	Alasan Relevansi
Pencarian Sub-domain	<a href="http://gowakab.go.id">gowakab.go.id</a> <a href="http://pariwisata.gowakab.go.id">pariwisata.gowakab.go.id</a> <a href="http://humas.gowakab.go.id">humas.gowakab.go.id</a> <a href="http://dinsos.gowakab.go.id">dinsos.gowakab.go.id</a> <a href="http://mpp.gowakab.go.id">mpp.gowakab.go.id</a> <a href="http://diskominfo.gowakab.go.id">diskominfo.gowakab.go.id</a>	crt.sh <a href="https://crt.sh/?q=gowakab.go.id">https://crt.sh/?q=gowakab.go.id</a>	Menunjukkan permukaan serangan (attack surface) yang lebih luas.
Informasi Karyawan	Farhan Makmur, S.H. (Kabid TI) Dhyni Widyawati D. (Kabid Komunikasi Publik) Sabrina Rukka, S.E. (Kabid Persandian)	Website Resmi Pemkab Gowa Diskomin <a href="https://diskominfo.gowakab.go.id/profil-pejabat/">https://diskominfo.gowakab.go.id/profil-pejabat/</a>	Untuk memahami struktur organisasi dan pihak yang relevan.
Format Email	<a href="mailto:info@gowakab.go.id">info@gowakab.go.id</a>	<a href="https://gowakab.go.id/site/">https://gowakab.go.id/site/</a>	Digunakan untuk validasi pola email dalam simulasi keamanan.

Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith <a href="https://builtwith.com/gowakab.go.id">https://builtwith.com/gowakab.go.id</a>	Menunjukkan penggunaan WAF dan potensi analisis keamanan sisi klien.
Informasi Sensitif Terpapar	Repository GitHub: dystianen/gowakab	GitHub Search (OSINT)	Potensi kebocoran source code atau kredensial.

a. Bukti Dokumentasi

## 1. Pencarian Domain dan Sub-domain

## 2. Informasi email dan karyawan

- Informasi email

 PORTAL GOWAKAB.GO.ID  Alamat Jl. Mesjid Raya No.30, Sungguminasa  Fax 0411 841141  Email info@gowakab.go.id

- Karyawan diskominfo

BIDANG TEKNOLOGI INFORMASI DAN TELEKOMUNIKASI



FARHAN MAKMUR S.H.  
KEPALA BIDANG TEKNOLOGI INFORMASI DAN TELEKOMUNIKASI

Tempat, Tanggal Lahir : -  
Jenis Kelamin : Laki-Laki  
Pangkat, Golongan/Ruang : Penata Tk. I, III/d

BIDANG PERSANDIAN



SABRINA RUKKA S.E.  
KEPALA BIDANG PERSANDIAN

Tempat, Tanggal Lahir : -  
Jenis Kelamin : Perempuan  
Pangkat, Golongan/Ruang : Penata Tk. I, III/d

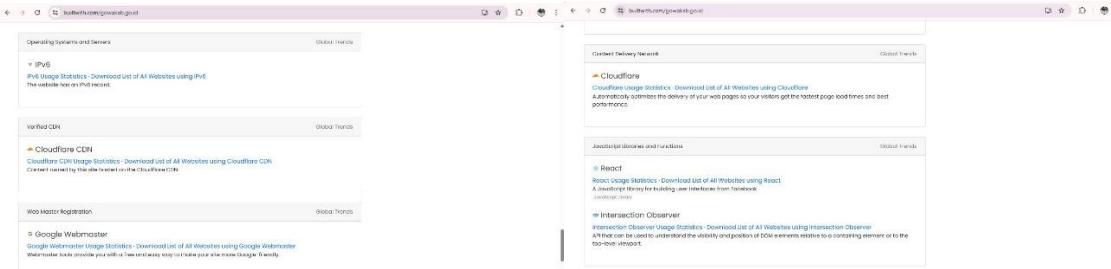
BIDANG KOMUNIKASI PUBLIK



DHYNI WIDAYAWATI DWIPUTRI S.Ksi, M.Si  
KEPALA BIDANG KOMUNIKASI PUBLIK

Tempat, Tanggal Lahir : -  
Jenis Kelamin : Perempuan  
Pangkat, Golongan/Ruang : Penata Tk. I, III/d

### 3. Teknologi yang digunakan



The screenshot shows a web browser with four tabs open, each displaying a different web-based tool or service:

- Operating Systems and Servers**: Shows a list of operating systems and servers, with "IPv6" highlighted.
- Cloudflare CDN**: Shows Cloudflare usage statistics and a link to Cloudflare's usage statistics page.
- Woo Master Registration**: Shows a registration form for Woo Master.
- Content Delivery Network**: Shows Cloudflare usage statistics and a link to Cloudflare's usage statistics page.
- React**: Shows React usage statistics and a link to Facebook's developer library.
- Intersection Observer**: Shows Intersection Observer usage statistics and a link to MDN's developer documentation.

#### 4. Informasi sensitive yang terpapar

The image shows two side-by-side screenshots of the GitHub search interface. The left screenshot shows the search results for 'goland' with 35 results. The right screenshot shows the search results for 'goland/goweb' with 1 result. Both results are for repositories named 'goland/goweb'. The repository details show it's a config file for a GitHub profile, updated on Oct 20, 2024, with 0 stars and 0 forks.

#### 4. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)

ifconfig

```
(root@iryantegar)-[~/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.10.2  netmask 255.255.255.240 broadcast 172.20.10.15
              inet6 fe80::f239:db00:f5ef:97e0  prefixlen 64  scopelid 0x20<link>
                ether 00:0c:29:a4:39:e3  txqueuelen 1000  (Ethernet)
                  RX packets 587  bytes 470824 (459.7 KiB)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 331  bytes 22772 (22.2 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  scopelid 0x10<host>
                loop  txqueuelen 1000  (Local Loopback)
                  RX packets 8  bytes 480 (480.0 B)
                  RX errors 0  dropped 0  overruns 0  frame 0
                  TX packets 8  bytes 480 (480.0 B)
                  TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Dilakukan hanya pada lingkungan lab IP 172.20.10.2 (vulonOS)

a. Host Discovery dan Port Scanning

Tugas	Command	Hasil	Potensi Dampak
Host Discovery	sudo netdiscover -r 172.20.10.0/24	Target ditemukan: 172.20.10.3	Memastikan host aktif di jaringan.
TCP SYN Scan	sudo nmap -sS 172.20.10.3	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	sudo nmap -sU --top-ports 20 172.20.10.3	Open/Filtered: 53, 67	DNS dan DHCP berpotensi menjadi target analisis.

a. Dokumentasi

- Host discovery

```
(root@iryantegar)-[/home/kali]
# sudo netdiscover -r 172.20.10.0/24

Session Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
IP At MAC Address Count Len MAC Vendor / Hostname
172.20.10.3 00:0c:29:93:5c:58 1 60 VMware, Inc.
172.20.10.7 d4:e9:8a:32:bf:a4 1 60 Intel Corporate
172.20.10.1 96:0c:98:60:18:64 1 60 Unknown vendor
```

- TCP SYN scan

```
[root@iryantegar ~]# sudo nmap -sS -p- 172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 09:36 EST
Nmap scan report for 172.20.10.3
Host is up (0.00060s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
6667/tcp  open  irc
MAC Address: 00:0C:29:93:5C:58 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.56 seconds
```

- UDP scn

```
[root@iryantegar ~]# sudo nmap -sU --top-ports 20 172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 09:39 EST
Nmap scan report for 172.20.10.3
Host is up (0.0035s latency).

PORT      STATE      SERVICE
53/udp    open|filtered domain
67/udp    open|filtered dhcps
68/udp    open|filtered dhcpc
69/udp    open|filtered tftp
123/udp   open|filtered ntp
135/udp   closed     msrpc
137/udp   open|filtered 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  open|filtered ms-sql-m
1900/udp  closed     upnp
4500/udp  closed     nat-t-ike
49152/udp open|filtered unknown
MAC Address: 00:0C:29:93:5C:58 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 8.26 seconds
```

## b. Service and Version Detection

```
sudo nmap -sV 172.20.10.3
```

Port	Service	Version	Analisis Risiko
22	SSH	OpenSSH 6.6.1p1	Versi lama → potensi brute force & enumeration.
80	HTTP	Apache 2.4.7	Banyak CVE publik untuk versi lama.
6667	IRC	ngircd	Layanan tidak umum untuk server produksi.

- Bukti service detection

```
[root@iryantegar ~]# sudo nmap -sV 172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 09:41 EST
Nmap scan report for 172.20.10.3
Host is up (0.00033s 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)
Service Info: Host: irc.example.net; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.71 seconds
```

## c. OS Fingerprinting

```
sudo nmap -O 172.20.10.3
```

Hasil	Detail OS	Analisis
OS Terdeteksi	Linux Kernel 3.x – 4.x	Menunjukkan OS lawas yang berpotensi memiliki celah keamanan.

- Bukti OS fingerprinting

```
(root@iryantegar)-[~/home/kali]
# sudo nmap -O 172.20.10.3
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-07 09:42 EST
Nmap scan report for 172.20.10.3
Host is up (0.0020s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
6667/tcp  open  irc
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

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

#### d. Network Protocol Analysis

Tool: Wireshark

Analisis:

Ditemukan pola SYN → SYN/ACK → RST saat proses pemindaian Nmap, menunjukkan penggunaan metode SYN Scan (-sS).

- Bukti network protocol analysis

No.	Time	Source	Destination	Protocol	Length	Info
03	115.693356995	172.20.10.2	172.20.10.3	TCP	58	38899 → 88 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
1	73.115.694045199	172.20.10.3	172.20.10.2	TCP	60	88 → 38899 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
2	78.115.695846928	172.20.10.2	172.20.10.3	TCP	54	38899 → 88 [RST] Seq=1 Win=0 Len=0

## 5. KESIMPULAN DAN SARAN

### a. Kesimpulan

- Passive recon menunjukkan **potensi kebocoran informasi publik**
- Active recon menunjukkan **port & layanan rentan** yang dapat menjadi titik serangan
- Tahap reconnaissance berhasil memberikan gambaran permukaan serangan sistem

### b. Saran

- Update layanan SSH & Apache
- Audit kembali subdomain dan hapus yang tidak relevan
- Tutup port yang tidak digunakan & perkuat firewall
- Kontrol akses terhadap repository GitHub
- Monitoring login & brute force turut diaktifkan