

LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

NAMA : IRYAN TEGAR
NIM : 105841113023
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 eksploitasi. Hasil pengumpulan informasi ini akan menjadi dasar dalam tahap eksploitasi 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: 172.20.10.3

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:

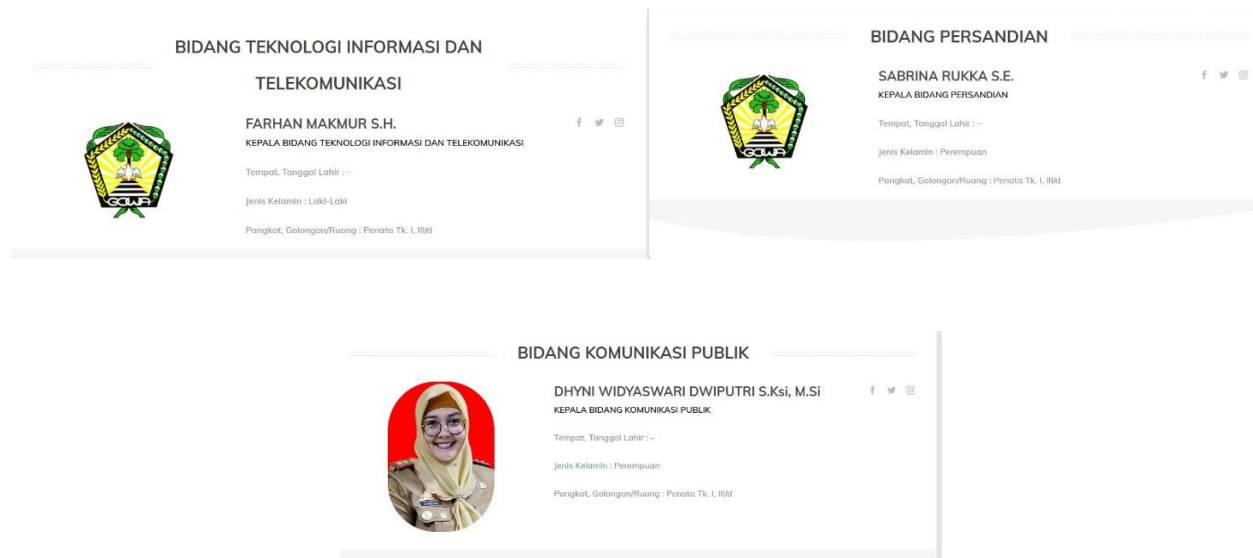
- a. Passive Reconnaissance
 - Mengumpulkan data melalui OSINT (Open Source Intelligence)
 - Tidak berinteraksi langsung dengan server
- b. Active Reconnaissance
 - Memindai IP target untuk menemukan port dan service terbuka
 - Mengidentifikasi OS dan protokol jaringan

5. PASSIVE RECONNAISSANCE (HASIL & ANALISIS)

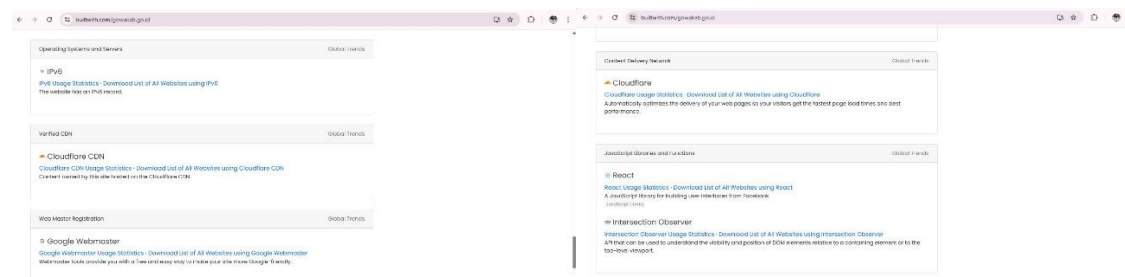
Target: wakab.go.id

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

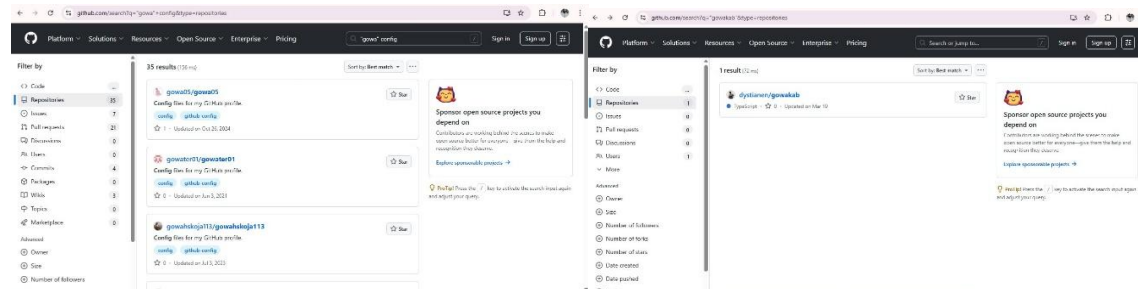
- Karyawan diskominfo



3. Teknologi yang digunakan



4. Informasi sensitive yang terpapar



4. ACTIVE RECONNAISSANCE (HASIL & ANALISIS)

ifconfig

```
(root@lryantergar) [/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:dbd0:f5ef:97e0 prefixlen 64 scopeid 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 scopeid 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	<code>sudo netdiscover -r 172.20.10.0/24</code>	Target ditemukan: 172.20.10.3	Memastikan host aktif di jaringan.
TCP SYN Scan	<code>sudo nmap -sS 172.20.10.3</code>	Port terbuka: 22, 80, 6667	Permukaan serangan layanan aktif.
UDP Scan	<code>sudo nmap -sU --top-ports 20 172.20.10.3</code>	Open/Filtered: 53, 67	DNS dan DHCP berpotensi menjadi target analisis.

a. Dokumentasi

- Host discovery

The image shows two screenshots from a Kali Linux environment. The top screenshot is a terminal window where the command `sudo netdiscover -r 172.20.10.0/24` has been executed. The bottom screenshot is the netdiscover graphical user interface (GUI) showing the results of the scan. It indicates that scanning is finished and displays a table of discovered hosts.

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)-[/home/kali]
# 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 scan

```
(root@iryantegar)-[/home/kali]
# 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 dhcpc
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)-[/home/kali]
# 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@iryanagar)-[/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
```

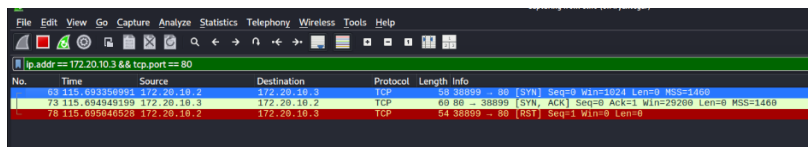
d. Network Protocol Analysis

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
63	115.693358991	172.20.10.2	172.20.10.3	TCP	60	38899 → 80 [SYN] Seq=0 Win=1824 Len=0 MSS=1460
73	115.694949199	172.20.10.3	172.20.10.2	TCP	60	80 80 → 38899 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1460
76	115.695846028	172.20.10.2	172.20.10.3	TCP	64	38899 → 80 [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