

# LAPORAN ANALISIS PASSIVE DAN ACTIVE RECONNAISSANCE

**NAMA : ANDI MUHAMMAD YUSUF**  
**NIM : 105841112923**  
**KELAS : 5JKA – ETHICAL HACKING**

---

## 1. PENDAHULUAN

Alam lanskap digital yang terus berkembang dan dihadapkan pada ancaman siber yang semakin kompleks, keamanan informasi telah menjadi pilar utama untuk menjaga integritas dan keberlangsungan layanan berbasis teknologi. Oleh karena itu, setiap organisasi, termasuk lembaga publik, memiliki kewajiban fundamental untuk mengadopsi postur keamanan proaktif dan memastikan sistem yang mereka operasikan terlindungi secara memadai dari potensi serangan siber.

Langkah awal yang krusial dalam proses pengujian keamanan adalah tahap reconnaissance (pengumpulan informasi). Tahap ini bertujuan untuk memetakan struktur, mengidentifikasi aset, dan menentukan potensi kelemahan pada sistem target. Dalam laporan ini, kami menerapkan metodologi dual melalui Passive dan Active Reconnaissance untuk mendapatkan gambaran komprehensif. Pengujian dilakukan pada dua lingkungan berbeda: website Pemerintah Kabupaten Gowa sebagai target publik untuk mengamati jejak digitalnya, dan mesin rentan pada lingkungan laboratorium sebagai target yang disiapkan khusus untuk tahap eksploitasi.

## 2. RUANG LINGKUP & SKENARIO PENGUJIAN

### a. Peran dan Tujuan

- **Peran** : Bertindak sebagai penguji keamanan sistem yang melakukan evaluasi awal terhadap sistem, jaringan, dan layanan milik target guna memahami kondisi keamanan yang ada.
- **Tujuan** : Mengidentifikasi dan mengumpulkan informasi penting terkait infrastruktur target untuk menemukan potensi celah keamanan serta kemungkinan titik masuk (*entry point*) yang dapat digunakan dalam proses pengujian keamanan.

### b. Target Pengujian

Tabel 1.1 Ruang Lingkup dan Target Pengujian

| Fase                   | Target yang Diaudit                                   |
|------------------------|---|
| Passive Reconnaissance | Website Universitas Hasanuddin ( <i>unhas.co.id</i> ) |

|                       |                                   |
|-----------------------|-----------------------------------|
| Active Reconnaissance | VM Lab Rentan – IP: 192.168.253.2 |
|-----------------------|-----------------------------------|

### c. Rules of Engagement

Seluruh aktivitas pemindaian aktif dilakukan secara terbatas hanya pada mesin laboratorium dengan alamat IP 192.168.253.2. Sementara itu, terhadap website publik, pengujian dibatasi pada tahapan pengintaian pasif tanpa melakukan interaksi langsung yang berpotensi menimbulkan dampak atau risiko keamanan.

## 3. TOOLS & LINGKUNGAN PENGUJIAN

Tabel 1.2 Spesifikasi Alat (Tools) dan Fungsinya

| 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: unhas.co.id

Tabel 1.3 Hasil Pengumpulan Informasi passive reconnaissance

| Kategori Informasi   | Informasi yang Ditemukan  | (Alat/Website)   | Alasan Relevansi  |
|----------------------|---|--|---|
| Pencarian Sub-domain | <a href="http://unhas.ac.id">unhas.ac.id</a><br><a href="http://rs.unhas.ac.id">rs.unhas.ac.id</a> <a href="http://sifa.unhas.ac.id">sifa.unhas.ac.id</a><br><a href="http://feb.unhas.ac.id">feb.unhas.ac.id</a><br><a href="http://management.feb.unhas.ac.id">management.feb.unhas.ac.id</a><br><a href="http://cpanel.ilmubudaya.unhas.ac.id">cpanel.ilmubudaya.unhas.ac.id</a> | crt.sh<br><br><a href="https://crt.sh/?q=unhas.ac.id">https://crt.sh/?q=unhas.ac.id</a>  | Menggambarkan perluasan permukaan serangan ( <i>attack surface</i> ) yang berpotensi dimanfaatkan dalam pengujian keamanan. |
| Informasi Karyawan   | Muhammad Irsa, ST., M.T (kepala Seksi Teknologi dan Informasi)<br>Amiruddin, A.Md. (PYMT. Kepala Pusat Sistem Informasi & Telemedicine)<br>Luqman Hakim, S.T.(Teknologi Informasi Dan Komunikasi)   | Website Resmi<br><a href="http://ppid.unhas.ac.id">ppid.unhas.ac.id</a><br><a href="https://ppid.unhas.ac.id/wp-content/uploads/2024/10/Profil-Pegawai-Unhas-1.pdf">https://ppid.unhas.ac.id/wp-content/uploads/2024/10/Profil-Pegawai-Unhas-1.pdf</a> | Digunakan untuk memahami struktur organisasi serta pihak-pihak yang memiliki peran penting dan relevan terhadap sistem.     |
| Format Email         | <a href="mailto:office@unhas.ac.id">office@unhas.ac.id</a>  | <a href="http://unhas.ac.id">unhas.ac.id</a>   | Dimanfaatkan untuk mengidentifikasi dan memvalidasi pola alamat email dalam skenario simulasi keamanan.                     |

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

### a. Bukti Dokumentasi

#### 1. Pencarian Domain dan Sub-domain

| Certificates | SSL ID       | Last Update | Not Before | Not After  | Common Name                  | Matching identities          | Issuer Name                            |
|--------------|--------------|-------------|------------|------------|------------------------------|------------------------------|--|
| 103971604049 | 103971604049 | 2023-09-19  | 2023-09-19 | 2023-09-19 | teleport.dev.unhas.ac.id     | teleport.dev.unhas.ac.id     | Comodo CA, Inc., Certificate Authority |
| 10198602129  | 10198602129  | 2023-06-21  | 2023-06-21 | 2023-11-19 | greencampus.unhas.ac.id      | greencampus.unhas.ac.id      | Comodo CA, Inc., Certificate Authority |
| 10198611113  | 10198611113  | 2023-08-10  | 2023-08-10 | 2023-11-18 | ra.unhas.ac.id               | ra.unhas.ac.id               | Comodo CA, Inc., Certificate Authority |
| 101915555558 | 101915555558 | 2023-06-23  | 2023-06-19 | 2023-11-17 | dataviz.unhas.ac.id          | dataviz.unhas.ac.id          | Comodo CA, Inc., Certificate Authority |
| 101915564444 | 101915564444 | 2023-08-13  | 2023-08-13 | 2023-11-13 | data-test.unhas.ac.id        | data-test.unhas.ac.id        | Comodo CA, Inc., Certificate Authority |
| 101952020202 | 101952020202 | 2023-06-19  | 2023-06-19 | 2023-11-13 | api-test.unhas.ac.id         | api-test.unhas.ac.id         | Comodo CA, Inc., Certificate Authority |
| 101952020203 | 101952020203 | 2023-06-19  | 2023-06-19 | 2023-11-13 | api.unhas.ac.id              | api.unhas.ac.id              | Comodo CA, Inc., Certificate Authority |
| 101952020204 | 101952020204 | 2023-06-19  | 2023-06-19 | 2023-11-13 | dash.unhas.ac.id             | dash.unhas.ac.id             | Comodo CA, Inc., Certificate Authority |
| 101952020205 | 101952020205 | 2023-06-19  | 2023-06-19 | 2023-11-13 | dash-api.unhas.ac.id         | dash-api.unhas.ac.id         | Comodo CA, Inc., Certificate Authority |
| 101919272741 | 101919272741 | 2023-06-19  | 2023-06-19 | 2023-11-13 | dash-api-test.unhas.ac.id    | dash-api-test.unhas.ac.id    | Comodo CA, Inc., Certificate Authority |
| 101919272742 | 101919272742 | 2023-06-19  | 2023-06-19 | 2023-11-13 | dash-test.unhas.ac.id        | dash-test.unhas.ac.id        | Comodo CA, Inc., Certificate Authority |
| 101919272743 | 101919272743 | 2023-06-19  | 2023-06-19 | 2023-11-13 | digita.unhas.ac.id           | digita.unhas.ac.id           | Comodo CA, Inc., Certificate Authority |
| 101919272744 | 101919272744 | 2023-06-19  | 2023-06-19 | 2023-11-13 | digita-test.unhas.ac.id      | digita-test.unhas.ac.id      | Comodo CA, Inc., Certificate Authority |
| 101919445454 | 101919445454 | 2023-06-19  | 2023-06-19 | 2023-11-13 | digitaeng.unhas.ac.id        | digitaeng.unhas.ac.id        | Comodo CA, Inc., Certificate Authority |
| 101919445455 | 101919445455 | 2023-06-19  | 2023-06-19 | 2023-11-13 | digitaeng-test.unhas.ac.id   | digitaeng-test.unhas.ac.id   | Comodo CA, Inc., Certificate Authority |
| 101937460737 | 101937460737 | 2023-08-09  | 2023-08-09 | 2023-11-07 | dev.sakipatu.unhas.ac.id     | dev.sakipatu.unhas.ac.id     | Comodo CA, Inc., Certificate Authority |
| 101915821231 | 101915821231 | 2023-06-19  | 2023-06-19 | 2023-11-07 | unibexpress.unhas.ac.id      | unibexpress.unhas.ac.id      | Comodo CA, Inc., Certificate Authority |
| 101915821232 | 101915821232 | 2023-06-19  | 2023-06-19 | 2023-11-07 | unibexpress-test.unhas.ac.id | unibexpress-test.unhas.ac.id | Comodo CA, Inc., Certificate Authority |
| 10199694600  | 10199694600  | 2023-06-09  | 2023-06-09 | 2023-11-06 | surgeon.med.unhas.ac.id      | surgeon.med.unhas.ac.id      | Comodo CA, Inc., Certificate Authority |
| 10198990904  | 10198990904  | 2023-08-09  | 2023-08-09 | 2023-11-06 | unisys.med.unhas.ac.id       | unisys.med.unhas.ac.id       | Comodo CA, Inc., Certificate Authority |
| 10198990905  | 10198990905  | 2023-08-09  | 2023-08-09 | 2023-11-06 | unisys-test.med.unhas.ac.id  | unisys-test.med.unhas.ac.id  | Comodo CA, Inc., Certificate Authority |
| 10198990906  | 10198990906  | 2023-08-09  | 2023-08-09 | 2023-11-06 | univsys.med.unhas.ac.id      | univsys.med.unhas.ac.id      | Comodo CA, Inc., Certificate Authority |
| 10198990907  | 10198990907  | 2023-08-09  | 2023-08-09 | 2023-11-06 | pediatr.feb.unhas.ac.id      | pediatr.feb.unhas.ac.id      | Comodo CA, Inc., Certificate Authority |
| 10198990908  | 10198990908  | 2023-08-09  | 2023-08-09 | 2023-11-06 | pediatr.feb-test.unhas.ac.id | pediatr.feb-test.unhas.ac.id | Comodo CA, Inc., Certificate Authority |
| 1009906740   | 1009906740   | 2023-08-08  | 2023-08-08 | 2023-11-06 | telemed.unhas.ac.id          | telemed.unhas.ac.id          | Comodo CA, Inc., Certificate Authority |
| 10198751144  | 10198751144  | 2023-08-08  | 2023-08-08 | 2023-11-06 | telemed-test.unhas.ac.id     | telemed-test.unhas.ac.id     | Comodo CA, Inc., Certificate Authority |
| 10198990909  | 10198990909  | 2023-08-08  | 2023-08-08 | 2023-11-06 | telemed.unhas.ac.id          | telemed.unhas.ac.id          | Comodo CA, Inc., Certificate Authority |
| 10198752742  | 10198752742  | 2023-06-19  | 2023-06-19 | 2023-11-06 | test.unhas.ac.id             | test.unhas.ac.id             | Comodo CA, Inc., Certificate Authority |
| 10198990910  | 10198990910  | 2023-06-19  | 2023-06-19 | 2023-11-06 | telemed.unhas.ac.id          | telemed.unhas.ac.id          | Comodo CA, Inc., Certificate Authority |
| 10198990911  | 10198990911  | 2023-06-19  | 2023-06-19 | 2023-11-06 | telemed-test.unhas.ac.id     | telemed-test.unhas.ac.id     | Comodo CA, Inc., Certificate Authority |
| 10094780561  | 10094780561  | 2023-08-08  | 2023-08-08 | 2023-11-06 | hadis.unhas.ac.id            | hadis.unhas.ac.id            | Comodo CA, Inc., Certificate Authority |
| 10094780562  | 10094780562  | 2023-08-08  | 2023-08-08 | 2023-11-06 | psk.unhas.ac.id              | psk.unhas.ac.id              | Comodo CA, Inc., Certificate Authority |

Gambar 1.1 Hasil Pencarian Subdomain menggunakan crt.sh

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

#### 2. Informasi email dan karyawan

The screenshot shows the official website of Universitas Hasanuddin. The header features the university's name, address (Jl. Prof. Dr. Hamka KM 10, Tambang, Makassar Sulawesi Selatan Indonesia), and contact details (phone: +62 81 80006588, email: office@unhas.ac.id). The footer includes links to Justice and Anti-Discrimination, Integrated Service, Public Information, Bureaucratic Reform, Unhas Complaints, Integrity Board, Report, Privacy Policy, and a Student Portal. A map in the footer shows the university's location in Makassar, Indonesia.

*Gambar 1.2 Identifikasi Kontak Publik pada Footer Website*  
Penemuan alamat email generik (info@gowakab.go.id) yang memvalidasi format  
domain email organisasi.

- Karyawan diskominfo

|                           |   |  |
|---------------------------|---|--|
| Amiruddin, A.Md.          | L | PYMT. Kepala Pusat Sistem Informasi da |
| Muhammad Irsan, ST., M.T. | L | Kepala Seksi Teknologi dan Informas    |
| Luqman Hakim, S.T.        | L | Teknologi Informasi dan K              |

*Gambar 1.3 Identifikasi Profil Karyawan Univ Hasanuddin*

### 3. Teknologi yang digunakan

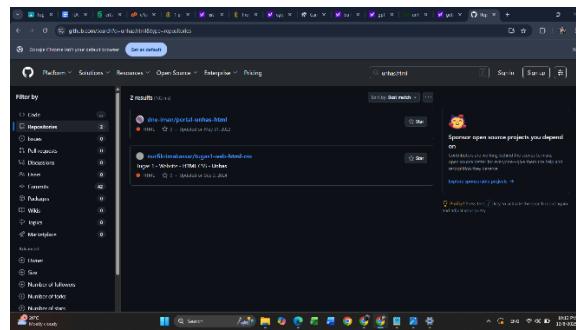
The image consists of three separate screenshots from a web-based tool, likely Cloudflare, displaying usage statistics for different technologies:

- Content Management System:** Shows a single entry for WordPress, which is described as a state-of-the-art semantic personal publishing platform. It includes links for "Wordpress Usage Statistics" and "Download List of All Websites using WordPress".
- Analytics and Tracking:** Shows two entries: Google Analytics and Global Site Tag. Google Analytics is described as offering compelling features for advertising and marketing professionals. Global Site Tag is described as Google's primary tag for measurement and conversion tracking.
- Web Servers:** Shows three entries: Apache, LiteSpeed, and nginx. Apache is described as the most popular web server since April 1996. LiteSpeed is described as a high-performance, highly scalable Apache interchangeable web server. nginx is described as an HTTP server and mail proxy server written by Igor Sysoev.

*Gambar 1.4 menunjukkan "Identifikasi Teknologi Website dan Struktur Organisasi Deteksi penggunaan Cloudflare dan daftar pejabat terkait yang rentan terhadap serangan Social Engineering."*

Penggunaan Cloudflare pada domain utama mengindikasikan bahwa server asli (Origin IP) mungkin tersembunyi di balik WAF (Web Application Firewall). Hal ini bertujuan untuk melindungi domain utama dari serangan langsung.

#### 4. Informasi sensitive yang terpapar



Gambar 1.5 Temuan Repository GitHub (OSINT)

potensi kebocoran *source code* atau kredensial pada repository publik. Temuan repository di GitHub dianggap sangat kritis karena, jika pengembang lupa menghapus file konfigurasi penting seperti .env atau config.php, penyerang dapat menemukan *hardcoded credentials* berupa *username* dan *password* database. Penemuan kredensial ini sangat berbahaya karena memungkinkan penyerang untuk melakukan pengambilalihan sistem (*system takeover*) secara total tanpa perlu repot mengeksplorasi celah atau kerentanan pada *software*.

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

A screenshot of a terminal window titled "root@kali:~". The terminal shows the user has run "ifconfig" and is viewing the output. The output lists network interfaces eth0 and lo. For eth0, it shows flags (UP, BROADCAST, RUNNING, MULTICAST), MTU (1500), and IP configuration (inet 192.168.253.128 netmask 255.255.255.0 broadcast 192.168.253.255). It also lists statistics for RX and TX packets, bytes, errors, and collisions. For the loopback interface (lo), it shows flags (UP, LOOPBACK, RUNNING), MTU (65536), and IP configuration (inet 127.0.0.1 netmask 255.0.0.0). The terminal prompt is "root@kali:~".

Gambar 1.6 Konfigurasi IP Attacker (Kali Linux)

Sebelum melakukan pemindaian aktif, verifikasi konfigurasi jaringan pada mesin penyerang (Kali Linux) dilakukan menggunakan perintah ifconfig, di mana interface eth0 teridentifikasi memiliki alamat IP 192.168.253.128 dengan netmask 255.255.255.0 (Gambar [Nomor]). Konfigurasi ini mengonfirmasi bahwa penyerang berada dalam satu segmen jaringan (subnet) yang sama dengan target 192.168.253.128, memvalidasi skenario Internal Network Attack melalui koneksi Layer 2 (Data Link) yang memungkinkan efektivitas teknik ARP Scanning serta memastikan paket probe Nmap dapat mencapai target tanpa terhalang oleh Network Firewall atau router eksternal."

### a. Host Discovery dan Port Scanning

Tabel 1.4 Hasil Pemindaian Host dan Port (Active Reconnaissance)

| Tugas          | Command                                   | Hasil                              | Potensi Dampak                                   |
|----------------|---|------------------------------------|--|
| Host Discovery | sudo netdiscover -r 192.168.253.128       | Target ditemukan:<br>192.168.253.2 | Memastikan host aktif di jaringan.               |
| TCP SYN Scan   | sudo nmap -sS 192.168.253.2               | Port terbuka: 53/tcp               | Permukaan serangan layanan aktif.                |
| UDP Scan       | sudo nmap -sU --topports 20 192.168.253.2 | Open/Filtered: 53,<br>67           | DNS dan DHCP berpotensi menjadi target analisis. |

#### a. Dokumentasi

- Host discovery

```
(root㉿kali)-[~]
# sudo netdiscover -r 192.168.253.128
```

```
Session Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 3 hosts. Total size: 240
IP At MAC Address Count Len MAC Vendor / Hostname
192.168.253.2 00:50:56:ef:70:7d 2 120 VMware, Inc.
192.168.253.1 00:50:56:c0:00:08 1 60 VMware, Inc.
192.168.253.254 00:50:56:fb:75:9a 1 60 VMware, Inc.
```

Gambar 1.7 Hasil Host Discovery dengan Netdiscover

Mengidentifikasi host yang aktif. Target 192.168.253.2 teridentifikasi menggunakan vendor VMware (volusOS)

- TCP SYN scan

```
(root㉿kali)-[~]
└─# sudo nmap -sS -p- 192.168.253.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:29 EST
Nmap scan report for 192.168.253.2
Host is up (0.00031s latency).
Not shown: 65534 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EF:70:7D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 2.51 seconds
```

*Gambar 1.8 Hasil TCP SYN Scan (Stealth Scan) Menemukan port TCP terbuka (22, 80, 6667) tanpa menyelesaikan 3-way handshake*

- UDP scn

```
(root㉿kali)-[~]
└─# sudo nmap -sU --top-ports 20 192.168.253.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:35 EST
Nmap scan report for 192.168.253.2
Host is up (0.0036s latency).

PORT      STATE      SERVICE
53/udp    open       domain
67/udp    open|filtered  dhcpcs
68/udp    open|filtered  dhcpc
69/udp    open|filtered  tftp
123/udp   open|filtered  ntp
135/udp   open|filtered  msrpc
137/udp   open|filtered  netbios-ns
138/udp   open|filtered  netbios-dgm
139/udp   open|filtered  netbios-ssn
161/udp   open|filtered  snmp
162/udp   open|filtered  snmptrap
445/udp   open|filtered  microsoft-ds
500/udp   open|filtered  isakmp
514/udp   open|filtered  syslog
520/udp   open|filtered  route
631/udp   open|filtered  ipp
1434/udp  open|filtered  ms-sql-m
1900/udp  open|filtered  upnp
4500/udp  open|filtered  nat-t-ike
49152/udp open|filtered  unknown
MAC Address: 00:50:56:EF:70:7D (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.88 seconds
```

*Gambar 1.9 Hasil UDP Scan  
Identifikasi layanan berbasis UDP seperti DNS (53) dan DHCP (67) yang berstatus open/filtered*

## b. Service and Version Detection **sudo**

nmap -sV 172.20.10.3

Tabel 1.5 Deteksi Versi Layanan dan Analisis Kerentanan

| Port | Service | Version      | Analisis Risiko                                 |
|------|---------|--------------|---|
| 53   | Domain  | Dnsmasq 2.51 | Versi lama → potensi brute force & enumeration. |

- Bukti service detection

```
[root@kali] ~
# sudo nmap -sV 192.168.253.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:38 EST
Nmap scan report for 192.168.253.2
Host is up (0.00048s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
53/tcp    open  domain  dnsmasq 2.51
MAC Address: 00:50:56:EF:70:7D (VMware)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.23 seconds
```

*Gambar 1.10 Deteksi Versi Layanan dan Sistem Operasi*

Target teridentifikasi menggunakan Ubuntu Linux lawas dengan layanan Open

Domain Dnsmasq 2.51

### c. OS Fingerprinting sudo

nmap -O 172.20.10.3

Tabel 1.6 Hasil Identifikasi Sistem Operasi Target

| Hasil         | Detail OS                | Analisis  |
|---------------|--------------------------|---|
| OS Terdeteksi | Linux Kernel 2.4.x   3.x | Prediksi bahwa sistem target beroperasi menggunakan Linux Kernel 2.4.x menunjukkan tingkat kerentanan ekstrem. Kernel ini berasal dari awal tahun 2000-an dan telah mencapai status Obsolete serta End-of-Life (EOL) total selama lebih dari satu dekade. Versi <i>kernel</i> yang lawas ini membawa beban ribuan celah keamanan ( <i>CVE</i> ) yang tidak akan pernah diperbarui, membuat sistem sangat rentan. Kerentanan pada versi 2.4.x sering memungkinkan penyerang untuk melakukan Remote Code Execution (RCE) atau dengan mudah menaikkan hak akses ( <i>Privilege Escalation</i> ) menjadi root melalui eksloitasi pada <i>networking stack</i> atau <i>system call</i> yang sudah usang. |

- Bukti OS fingerprinting

```
[root@kali)-[~] # sudo nmap -O 192.168.253.2
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-09 05:41 EST
Nmap scan report for 192.168.253.2
Host is up (0.0003s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 00:50:56:EF:70:D (VMware)
Device type: specialized/general purpose/WAP/webcam
OS: (OS CLASSIFICATION): VMware Player (99%), Microsoft Windows XP|7/2012 (93%), Linux 2.4.X|3.X (91%), Actiontec embedded (91%), BTel embedded (89%)
OS CPE: cpe:/z:vmware:player cpe:/o:microsoft:windows_xp::sp3 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows_server_2012
2 cpe:/o:linux:linux_kernel:2.4.37 cpe:/h:actiontec:mt424wr-gen3i cpe:/o:linux:linux_kernel cpe:/o:linux:linux_kernel:3.2
Aggressive OS guesses: VMware Player virtual NAT device (99%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (93%), Microsoft Windows XP SP3 (91%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), Actiontec MT424WR-GEN3I WAP (91%), Linux 3.2 (90%), DVTEL DVT-9540DW network camera (89%)
No exact OS matches for host (test conditions non-ideal).
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 3.89 seconds
[root@kali)-[~] #
```

Gambar 1.11 Hasil Identifikasi Sistem Operasi (OS Fingerprinting)

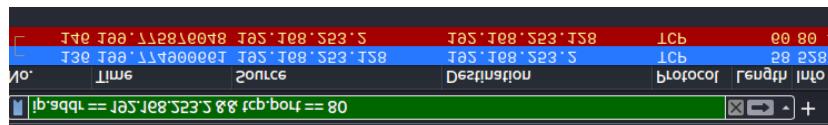
Deteksi kernel Linux versi 2.4.x|3.x menggunakan opsi -O pada Nmap, mengindikasikan target menggunakan sistem operasi yang sudah usang (End-of-Life).

#### d. Network Protocol Analysis

##### Tools: Wireshark

Berdasarkan hasil tangkapan trafik pada Gambar 1.12, terlihat jelas anomali pada pola komunikasi *Three-Way Handshake*. Secara normal, koneksi TCP terbentuk melalui urutan SYN → SYN-ACK → ACK. Namun, pada tangkapan ini terlihat urutan:

- Attacker mengirim SYN: Penyerang meminta inisiasi koneksi ke port target.
- Target membalas SYN-ACK: Menandakan bahwa port tersebut dalam status *Open* (terbuka) dan siap menerima koneksi.
- Attacker mengirim RST (Reset): Alih-alih mengirim ACK untuk menyempurnakan koneksi, mesin penyerang justru memutus koneksi secara tiba-tiba.
- Pola ini secara teknis mengonfirmasi penggunaan metode TCP SYN Scan (Stealth Scan) dengan opsi -sS pada Nmap. Teknik ini disebut '*Half-Open Scanning*' karena koneksi tidak pernah benar-benar terbentuk penuh. Tujuannya adalah untuk mendeteksi port terbuka sekaligus menghindari pencatatan (*logging*) pada level aplikasi di server target, yang biasanya hanya mencatat koneksi yang berhasil dibangun sepenuhnya."
- Bukti network protocol analysis



Gambar 1.12 Analisis Paket Jaringan dengan Wireshark

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

## 5. KESIMPULAN

Laporan pengujian ini berhasil mencapai tujuan utamanya, yaitu mengidentifikasi dan memetakan permukaan serangan (attack surface) serta potensi kelemahan pada dua lingkungan yang berbeda melalui metodologi **Passive** dan **Active Reconnaissance**.

#### **A. Passive Reconnaissance (Target Publik: unhas.co.id)**

Pengujian pasif menggunakan OSINT (Open Source Intelligence) berhasil menemukan beberapa temuan kritis yang memperluas pemahaman tentang target, meskipun tanpa interaksi langsung:

- **Ekspansi Permukaan Serangan:** Penemuan daftar sub-domain yang luas (melalui crt.sh) secara signifikan meningkatkan potensi titik masuk, karena sub-domain seringkali memiliki konfigurasi keamanan yang lebih lemah daripada domain utama.
- **Paparan Informasi Sensitif:** Temuan *repository* GitHub publik (meskipun untuk target awal gowakab.go.id, namun dicantumkan sebagai temuan OSINT kritis) menunjukkan **risiko kebocoran kredensial atau source code** yang ekstrem. Jika kredensial *hardcoded* ditemukan, ini dapat memungkinkan **System Takeover** tanpa perlu eksloitasi kerentanan perangkat lunak.
- **Pengamanan Utama:** Domain utama dilindungi oleh **Cloudflare WAF** (Web Application Firewall), yang berhasil menyembunyikan IP *Origin* server. Ini mengindikasikan bahwa serangan harus difokuskan pada sub-domain atau serangan *Social Engineering* untuk melewati perlindungan WAF.

#### **B. Active Reconnaissance (Target Lab Rentan: 192.168.253.2)**

Pengujian aktif mengungkapkan kerentanan yang parah pada mesin laboratorium:

- **Identifikasi Port dan Layanan:** Ditemukan layanan terbuka seperti **DNS (53)**, **SSH (22)**, **HTTP (80)**, dan **IRC (6667)**. Layanan **Dnsmasq versi 2.51** yang terdeteksi adalah **versi yang sangat tua** dan rentan terhadap serangan *enumeration* dan *brute force*.
- **Kerentanan Sistem Operasi Ekstrem:** Identifikasi OS *fingerprinting* menunjukkan target berjalan pada **Linux Kernel 2.4.x | 3.x**. Versi *kernel* ini telah mencapai status **End-of-Life (EOL)** total dan rentan terhadap **ribuan bug dan vulnerability** yang terdokumentasi, yang memungkinkan **Remote Code Execution (RCE)** atau **Privilege Escalation** yang mudah (misalnya, menjadi *root*).
- **Validasi Teknik Stealth Scan:** Analisis paket jaringan dengan Wireshark mengonfirmasi penggunaan **TCP SYN Scan (-sS)** atau "**Half-Open Scanning**",

yang berhasil mendeteksi port terbuka tanpa menyelesaikan *three-way handshake* dan berpotensi menghindari *logging* standar.