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 *(unhas.co.id)*

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

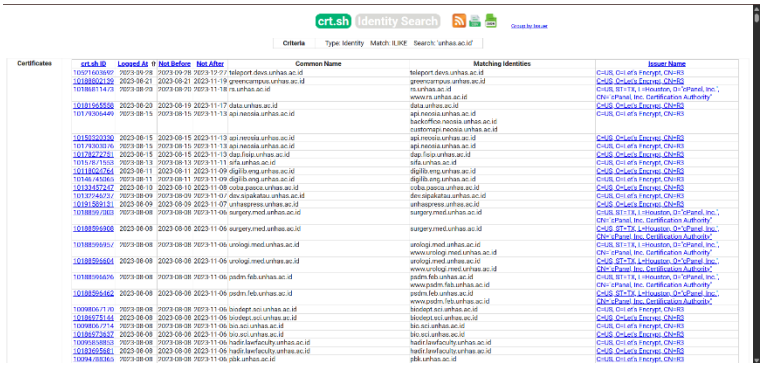
Tabel 1.3 Hasil Pengumpulan Informasi passive reconnaissance

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

Teknologi Website	Cloudflare React Cloudflare Web Analytics	BuiltWith https://builtwith.com/ unhas.ac.id	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

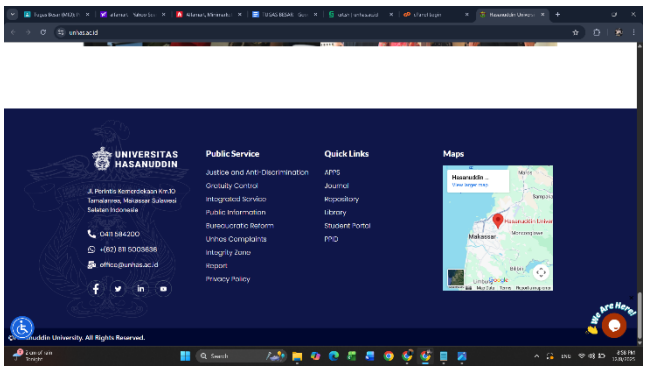


Gambar 1.1 Hasil Pencarian Subdomain menggunakan crt.sh

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

2. Informasi email dan karyawan

- Informasi email



Gambar 1.2 Identifikasi Kontak Publik pada Footer Website

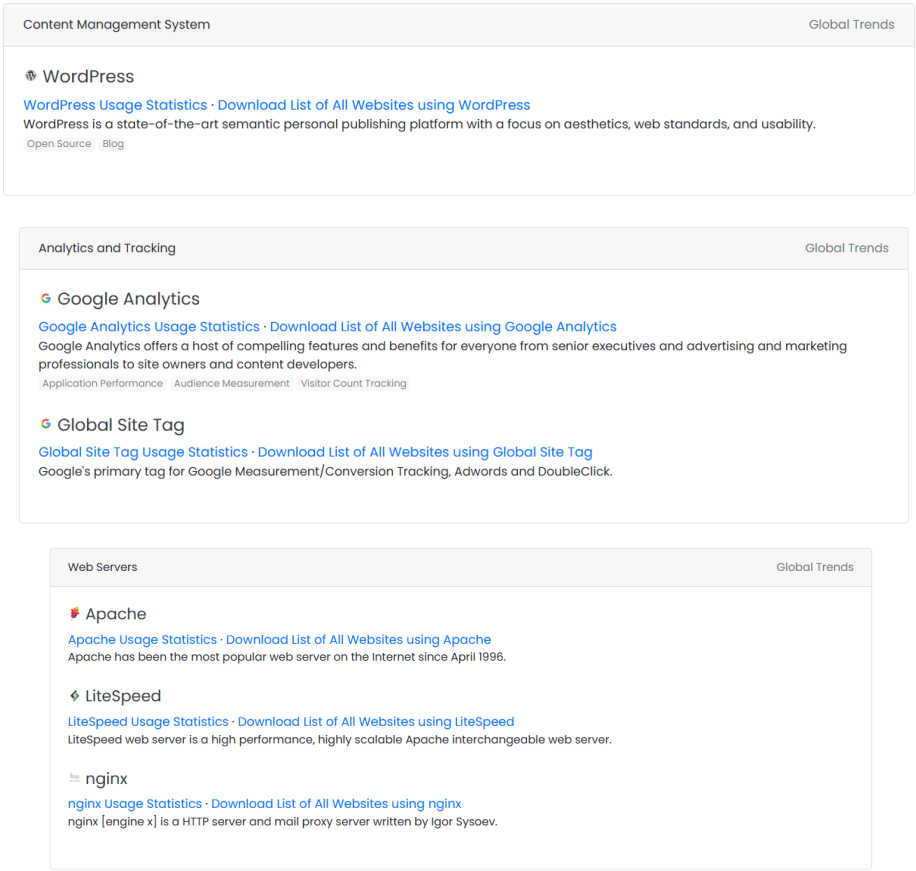
Penemuan alamat email generik (info@gowakab.go.id) yang memvalidasi format domain email organisasi.

- 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

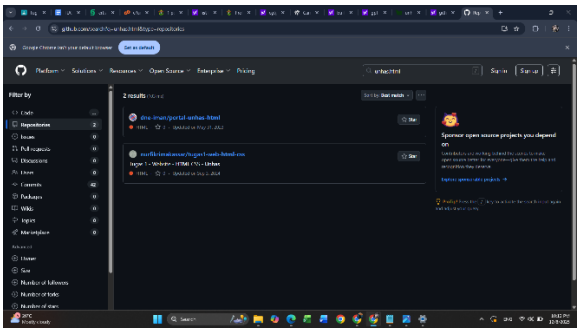
3. Teknologi yang digunakan



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.

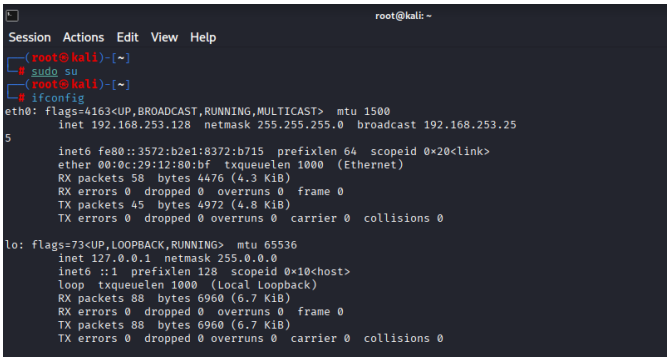
4. Informasi sensitive yang terpapar



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 mengeksploitasi celah atau kerentanan pada *software*.

4. ACTIVE RECONNAISSANCE (HASIL & ANALISIS) ifconfig



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 konektivitas 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."

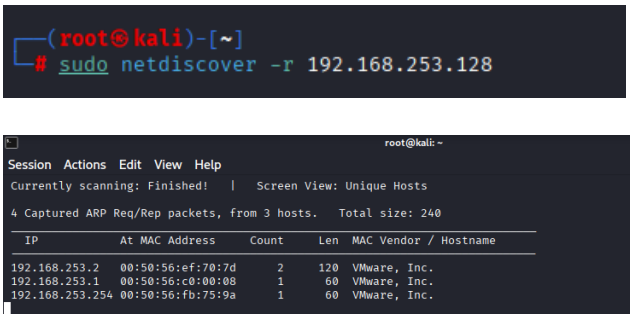
a. Host Discovery dan Port Scanning

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: 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, 67	DNS dan DHCP berpotensi menjadi target analisis.

a. Dokumentasi

- Host discovery



Gambar 1.7 Hasil Host Discovery dengan Netdiscover

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

- 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 dhcps
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

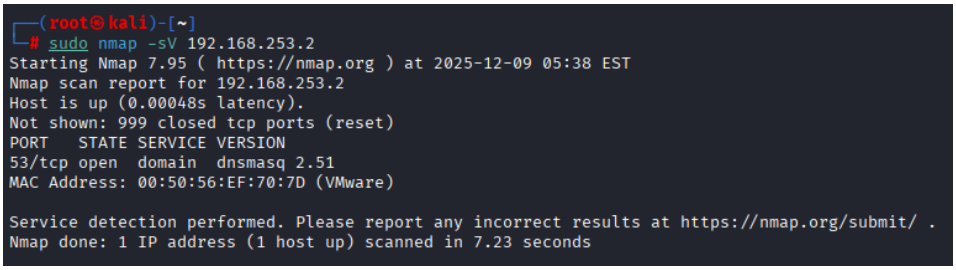
b. Service and Version Detection sudo

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



Gambar 1.10 Deteksi Versi Layanan dan Sistem Operasi

Target teridentifikasi menggunakan Ubuntu Linux lawas dengan layanan Open Domain Dnsmasq 2.51

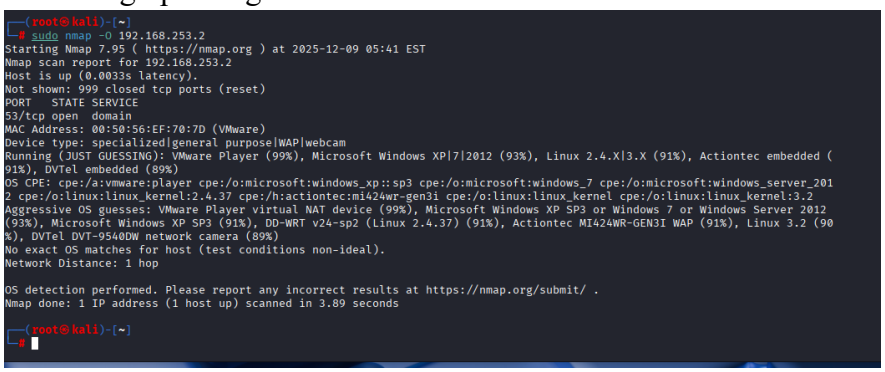
c. OS Fingerprinting sudo

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 *kernel* yang lawas ini membawa beban ribuan celah keamanan (*CVE*) 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 (*Privilege Escalation*) menjadi root melalui eksploitasi pada *networking stack* atau *system call* yang sudah usang.

- Bukti OS fingerprinting



Gambar 1.11 Hasil Identifikasi Sistem Operasi (OS Fingerprinting)

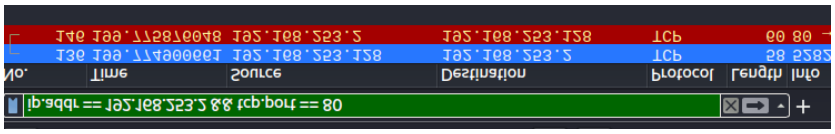
Deteksi kernel Linux versi 2.4.x|3.x menggunakan opsi -O pada Nmap, mengindikasikan target menggunakan sistem operasi yang sudah usang (End-of-Life).

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 eksploitasi 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.