NETWORK RECONNAISSANCE & SECURITY ASSESSMENT REPORT

Target: Home Network (192.168.1.0/24)

Environment: Personal Lab — Controlled Network

Tool: Nmap 7.98

Prepared by:

[ALIZHA TIARA SYAFAHIRA]

[102042330201 | Information Systems | Telkom University]

Date: 19 Februari 2026

⚠ DISCLAIMER: Seluruh aktivitas scanning dalam laporan ini dilakukan secara eksklusif terhadap jaringan pribadi milik penulis sendiri (home network). Tidak ada sistem, jaringan, atau perangkat milik pihak ketiga yang menjadi target. Laporan ini dibuat untuk keperluan edukasi dan portofolio semata.

1. Executive Summary

Laporan ini mendokumentasikan hasil network reconnaissance dan security assessment yang dilakukan terhadap jaringan pribadi (home network) dengan subnet 192.168.1.0/24 menggunakan Nmap versi 7.98. Tujuan assessment ini adalah mengidentifikasi host yang aktif, port yang terbuka, serta service yang berjalan pada jaringan tersebut, kemudian menganalisis potensi risiko keamanan yang ada.

Dari hasil scanning, ditemukan 2 host aktif dari total 256 IP address yang di-scan. Berikut ringkasan temuan:

Host	Device	Open Ports	Risk Level
192.168.1.1	Router (Cisco-Linksys E4200)	80, 49152	Medium
192.168.1.5	MacBook (Penguji)	80, 5000, 7000	Low

2. Scope & Metodologi

2.1 Scope

Item	Detail
Target Network	192.168.1.0/24 (Home Network Pribadi)
Hosts Aktif	2 dari 256 IP address
Tool Utama	Nmap 7.98
Tipe Scan	Service Version Detection (-sV) dan Aggressive Scan (-A)
OS Penguji	macOS (Apple MacBook Air, ARM)

2.2 Command yang Digunakan

Dua perintah Nmap dijalankan secara berurutan:

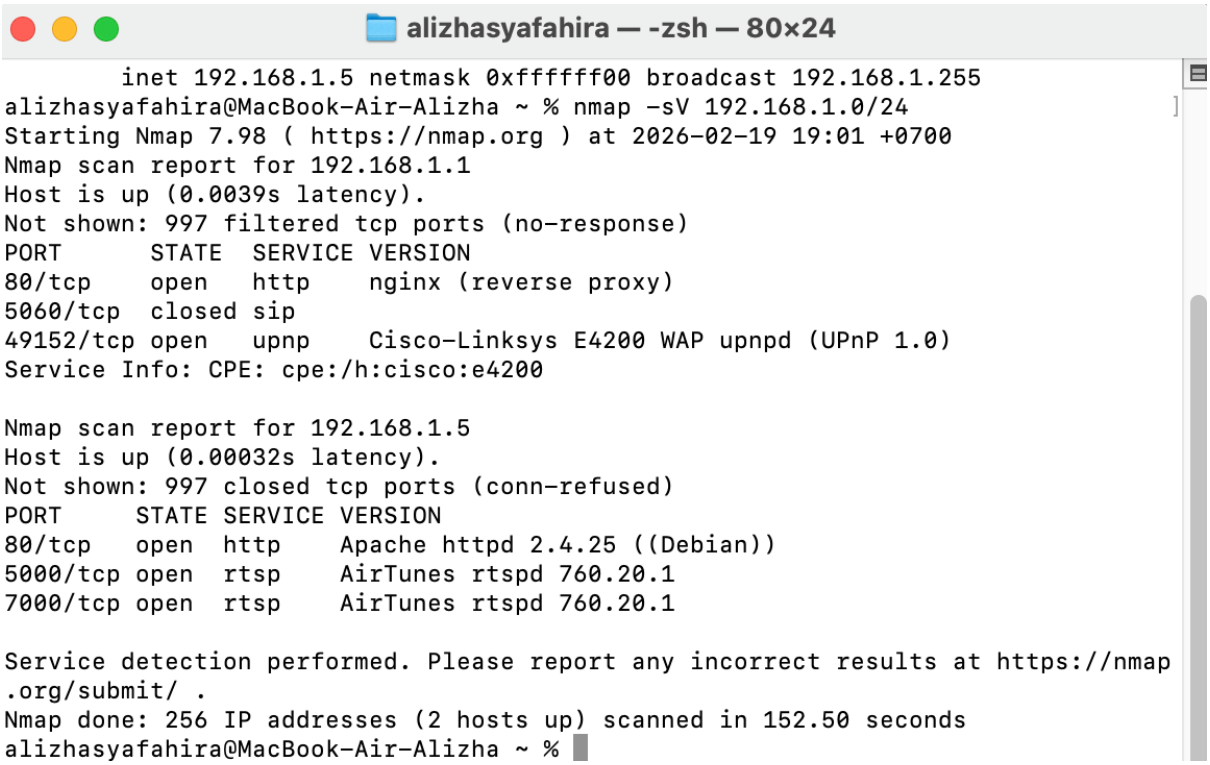
```
nmap -sV 192.168.1.0/24
```

Digunakan untuk mendeteksi semua host aktif beserta service dan versi yang berjalan pada seluruh subnet.

```
nmap -A 192.168.1.1
```

Digunakan untuk aggressive scan terhadap router — mencakup OS detection, version detection, script scanning, dan traceroute.

💣 [Hasil terminal nmap -sV 192.168.1.0/24]



💣 [Hasil terminal nmap -A 192.168.1.1]

```
alizhasyafahira@MacBook-Air-Alizha ~ % nmap -A 192.168.1.1
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-19 19:07 +0700
Nmap scan report for 192.168.1.1
Host is up (0.0042s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE  SERVICE VERSION
80/tcp    open   http    nginx (reverse proxy)
|_http-title: Site doesn't have a title (text/html; charset=utf-8).
5060/tcp  closed sip
49152/tcp open   upnp    Cisco-Linksys E4200 WAP upnpd (UPnP 1.0)
Service Info: CPE: cpe:/h:cisco:e4200

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 127.27 seconds
alizhasyafahira@MacBook-Air-Alizha ~ %
```

3. Temuan Detail

3.1 Host: 192.168.1.1 — Router Cisco-Linksys E4200

Port	State	Service	Keterangan
80/tcp	Open	HTTP (nginx)	Admin panel router dapat diakses via browser. Risiko: akses tidak sah jika password default belum diubah.
5060/tcp	Closed	SIP	Port VoIP tertutup. Tidak ada risiko aktif.
49152/tcp	Open	UPnP	Universal Plug and Play aktif. Risiko: dapat dieksploitasi untuk NAT traversal atau port forwarding tidak sah.

Analisis Risiko:

- Port 80 terbuka mengekspos admin panel router ke seluruh perangkat dalam jaringan. Jika kredensial default (admin/admin) belum diubah, penyerang dalam jaringan yang sama dapat mengakses panel administrasi penuh.
- UPnP pada port 49152 merupakan protokol yang dikenal rentan terhadap serangan SSRF (Server-Side Request Forgery) dan dapat dimanfaatkan untuk memodifikasi konfigurasi firewall secara otomatis tanpa autentikasi.

Rekomendasi:

- Ganti password default admin panel router segera
- Nonaktifkan UPnP jika tidak digunakan — akses Settings router → Advanced → UPnP → Disable
- Batasi akses admin panel hanya dari perangkat tertentu menggunakan MAC filtering

3.2 Host: 192.168.1.5 — MacBook (Perangkat Penguji)

Port	State	Service	Keterangan
80/tcp	Open	HTTP (Apache 2.4.25)	DVWA berjalan di Docker container. Sengaja aktif sebagai lab environment.
5000/tcp	Open	AirTunes (rtspd)	Fitur AirPlay macOS. Normal dan tidak berbahaya dalam jaringan pribadi.
7000/tcp	Open	AirTunes (rtspd)	Fitur AirPlay macOS. Normal dan tidak berbahaya dalam jaringan pribadi.

Catatan:

Port 80 pada perangkat ini adalah DVWA yang sengaja dijalankan sebagai lab environment untuk keperluan penetration testing (lihat laporan terpisah: Web Application Vulnerability Assessment Report — DVWA). Port AirTunes merupakan service bawaan macOS untuk fitur AirPlay dan tidak menimbulkan risiko dalam jaringan pribadi yang terkontrol.

4. Kesimpulan & Rekomendasi

Hasil network reconnaissance terhadap jaringan 192.168.1.0/24 menunjukkan bahwa jaringan ini relatif bersih dengan hanya 2 host aktif yang terdeteksi. Tidak ditemukan port berbahaya yang terbuka secara tidak wajar, namun terdapat dua area yang perlu diperhatikan pada router, yaitu admin panel yang dapat diakses tanpa enkripsi (HTTP) dan layanan UPnP yang aktif.

Rekomendasi Umum:

- Segera ubah kredensial default router dan aktifkan HTTPS untuk akses admin panel
- Nonaktifkan layanan yang tidak digunakan, khususnya UPnP, untuk memperkecil attack surface
- Lakukan network scanning secara berkala untuk mendeteksi perangkat atau port baru yang tidak dikenal
- Aktifkan firewall pada semua perangkat dalam jaringan
- Gunakan network segmentation jika terdapat perangkat IoT dalam jaringan yang sama

5. Referensi

- Nmap Official Documentation — https://nmap.org/docs.html
- OWASP Top 10 2021 — https://owasp.org/Top10/
- SANS Institute — Network Reconnaissance Techniques
- CVE Database UPnP Vulnerabilities — https://cve.mitre.org