Network Reconnaissance and Port Scanning using Nmap

Jonathan Jethro

May 3, 2025

1. Ringkasan

Laporan ini menjelaskan proses scanning jaringan lokal menggunakan **Nmap**. Target adalah jaringan 10.10.150.42/24 untuk mengidentifikasi perangkat aktif, port terbuka, dan layanan berjalan.

2. Tujuan

- Melatih keterampilan dasar dalam network reconnaissance.
- Mengidentifikasi potensi celah keamanan melalui port terbuka.
- Membuat dokumentasi keamanan sebagai latihan pentesting.

3. Tools dan Lingkungan

- OS: Parrot Security OS (Live USB)
- Tools: Nmap v7.94, Wireshark (untuk validasi)
- Target: 10.10.150.42/24

4. Metodologi

4.1 Host Discovery

```
nmap -sn 10.10.150.42/24
```

4.2 Port Scanning

```
nmap -sS -v 10.10.150.42
```

4.3 Service and Version Detection

```
nmap -sV -sC 10.10.150.42
```

4.4 Hostname Scanning

```
nmap -R 10.10.150.42
```

4.4 OS Detection

```
nmap -O 10.10.150.42
```

5. Hasil dan Temuan

5.1 Ringkasan Host Aktif

IP Address	Hostname	Status
10.10.150.1	Router	Online
10.10.150.38	Target Device	Online
10.10.150.64	Printer	Online

5.2 Scan Port 192.168.1.10

```
PORT     STATE SERVICE     VERSION
22/tcp   open  ssh         OpenSSH 7.6p1 Ubuntu 4
80/tcp   open  http        Apache httpd 2.4.29
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X
445/tcp  open  microsoft-ds Samba smbd 4.7.6-Ubuntu
```

6. Rekomendasi

- SSH (port 22): Batasi akses menggunakan firewall.
- HTTP (port 80): Periksa potensi kerentanan web server.
- Samba (port 139/445): Hanya aktifkan jika diperlukan.

7. Screenshot dan Bukti

(Sisipkan gambar hasil scanning)

8. Kesimpulan

Scanning berhasil mengidentifikasi perangkat dan layanan aktif. Data ini bermanfaat untuk langkah selanjutnya dalam hardening sistem.

9. Referensi

- https://nmap.org/book/
- https://nmap.org/man/
- https://www.sans.org/media/score/checklists/Nmap_Reference_Guide.pdf