**Worksheet Pertemuan 22 SJK: Port Scanner & Wireshark Analysis**

Kelompok: An-naml

Anggota hadir: Zikri Dwi Andika 17523226

Rizqi Kartika Safitri 17523153

Natasya Ulfha Nabilla 17523184

-------------------------------------------------------------------------------------------------------------------------

**Part 1 - Port Scanning - scanme.nmap**

1. Install NMAP, <https://nmap.org/download.html>

2. Buka Command Prompt, masuk ke folder di mana NMAP terinstall

3. Buka aplikasi Wireshark, capture paket yang melalui WiFi (atau koneksi yang Anda pakai untuk terhubung ke internet)

4. Buka lagi Command Prompt, masukkan perintah **nmap -T4 -A -v scanme.nmap.org**

5. Jika proses scan selesai (“Nmap done”), stop capturing packets di Wireshark

6. Amati hasil scan di Command Prompt.

Isi tabel dan isian di bawah ini dengan status port yang ditemukan:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No.  Port | Protokol  (transport layer) | Status | Layanan | Versi |
| 22 | TCP | open | ssh | OpenSSH 6.6.1p1 Ubuntu 2Ubuntu2.11(Ubuntu Linux; protocol 2.0) |
| 25 | TCP | filtered | smtp |  |
| 53 | TCP | filtered | domain |  |
| 80 | TCP | open | http | Apche httpd 2.4.7 ((Ubuntu)) |

Alamat IP dari scanme.nmap.org:45.33.32.156

Sistem operasi yang digunakan scanme.nmap.org: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jarak dari perangkat Anda ke scanme.nmap.org: \_\_\_\_\_\_\_\_ hops

7. Amati paket-paket yang telah berhasil di-*capture* di Wireshark

a. Mengamati paket-paket yang membuktikan bahwa status port “**open**”

i. Filter daftar captured packets di Wireshark dengan:

(ip.addr eq <alamat IP scanme.nmap.org>) and (tcp.port eq <salah satu no.port di tabel atas, dengan status **open**>)

contoh: (ip.addr eq 123.123.123.123) and (tcp.port eq 99)

ii. Pilih salah satu paket, klik kanan → Conversation Filter → TCP

iii. Tampilkan hasil screenshot Anda di sini:

iv. Berdasarkan tampilan di poin iii, mengapa NMAP bisa menyatakan bahwa port tersebut terbuka (status: **open**)?

Jawab:

b. Mengamati paket-paket yang membuktikan bahwa status port “**filtered**”

i. Filter daftar captured packets di Wireshark dengan:

(ip.addr eq <alamat IP scanme.nmap.org>) and (tcp.port eq <salah satu no.port di tabel atas, dengan status **filtered**>)

ii. Tampilkan hasil screenshot Anda di sini:

iii. Berdasarkan tampilan di poin ii, mengapa NMAP bisa menyatakan bahwa port tersebut berstatus **filtered**?

Jawab:

**Part 2 - Port Scanning-VM Server**

1. Nyalakan VM Server dan VM Router
2. Buka Command Prompt, pastikan lokasi berada di folder di mana terdapat aplikasi nmap.
3. Masukkan perintah **nmap -T4 -A -v (alamat IP VM server)**Contoh: **nmap -T4 -A -v 192.168.1.2**
4. Amati hasil scan di Command Prompt.  
   Isi tabel dan isian di bawah ini dengan status port yang ditemukan:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| No.  Port | Protokol  (transport layer) | Status | Layanan | Versi |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. Alamat MAC dari interface VM Server: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. Sistem operasi yang digunakan VM Server, menurut hasil scan NMAP: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Jarak dari host ke VM Server: \_\_\_\_\_\_\_\_ hops