

# Tugas Cyber Security

## Pertemuan 3

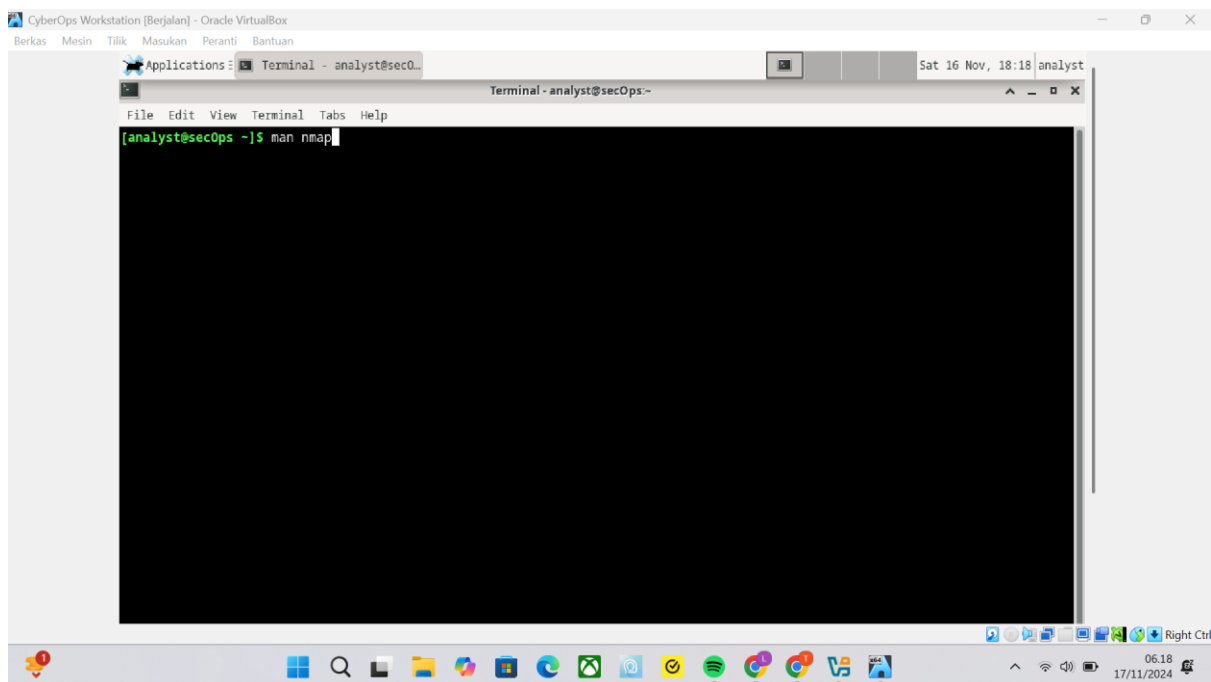
### *Sosial Engineering*

---

**Nama** : Lukas Febrian Laufra'  
**Kelas/Nim** : TI22J/20220040076  
**Dosen Pengajar** : Pak Ir. Somantri, S.T, M.Kom  
**Waktu Pengerjaan** : 07.41/Minggu, 17 November 2024

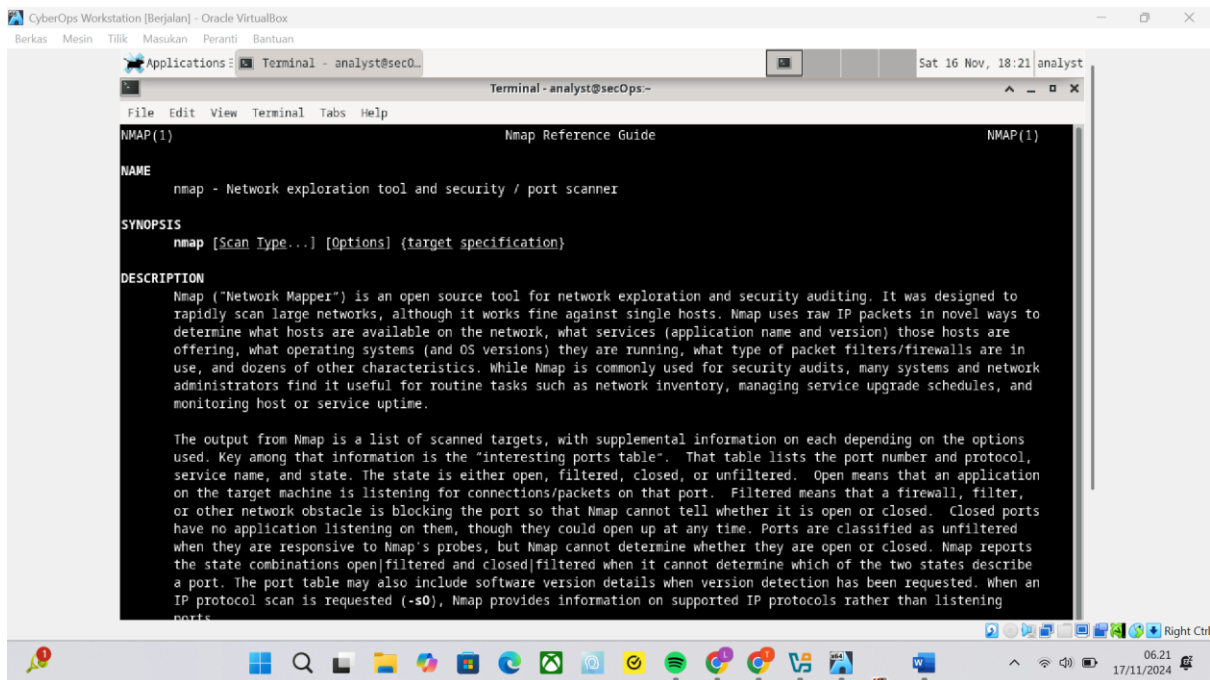
---

#### Part 1: Exploring Nmap



What is Nmap?

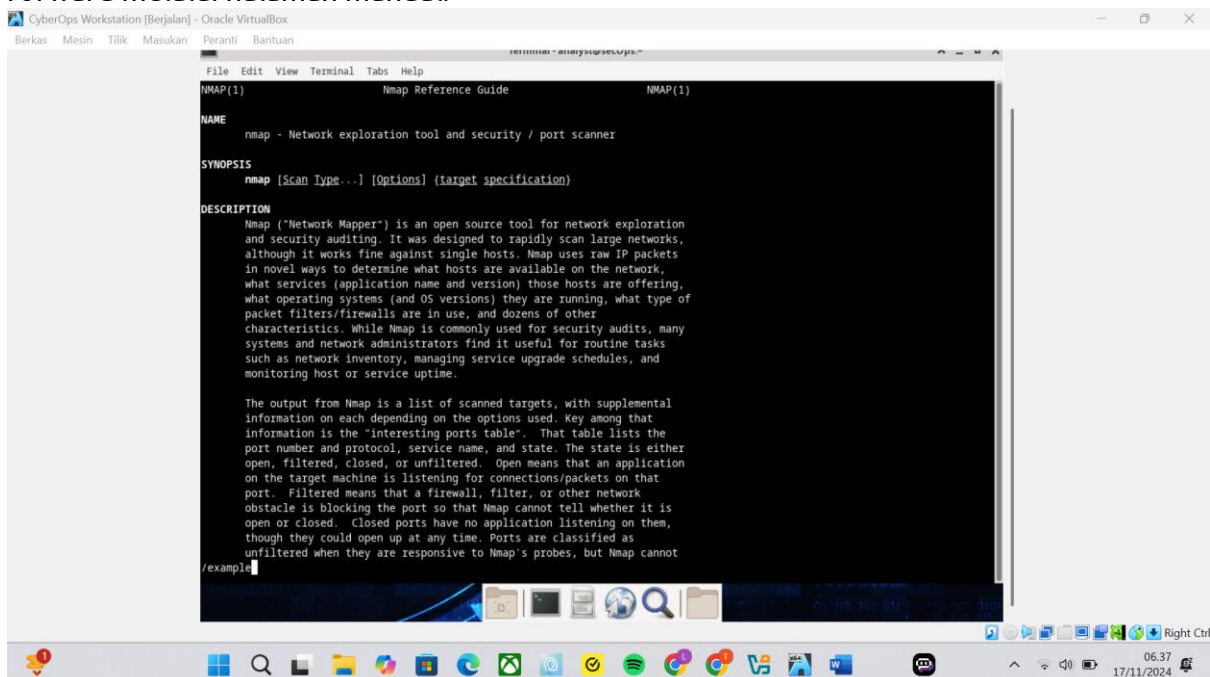
Nmap adalah alat pengekplorasi jaringan dan keamanan/pemindai port.



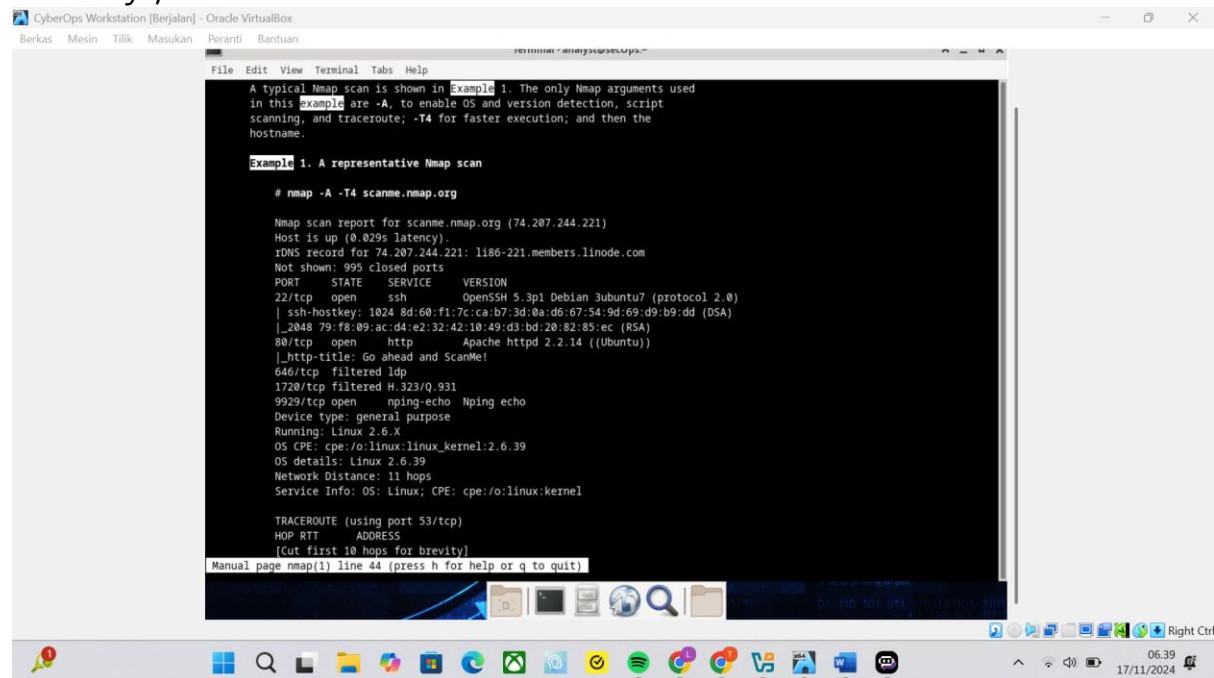
What is nmap used for?

**Nmap digunakan untuk memindai target jaringan untuk mengetahui informasi seperti host yang tersedia, layanan yang berjalan, dan jenis paket filter/firewall yang digunakan.**

Saat berada di halaman manual, Anda dapat menggunakan tombol panah atas dan bawah untuk menelusuri halaman. Anda juga dapat menekan bilah spasi untuk meneruskan halaman satu per satu. Untuk mencari istilah atau frasa tertentu, masukkan garis miring (/) atau tanda tanya (?) diikuti istilah atau frasa tersebut. Garis miring menelusuri dokumen ke depan, dan tanda tanya menelusuri dokumen ke belakang. Kunci n berpindah ke pertandingan berikutnya. Ketik /contoh dan tekan ENTER. Ini akan mencari kata example forward melalui halaman manual.



Pada contoh pertama, Anda melihat tiga kecocokan. Untuk pindah ke pertandingan berikutnya, tekan n.



```
File Edit View Terminal Tabs Help
A typical Nmap scan is shown in Example 1. The only Nmap arguments used
in this example are -A, to enable OS and version detection, script
scanning, and traceroute; -T4 for faster execution; and then the
hostname.

Example 1. A representative Nmap scan

# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
IDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
|_ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_2048 79:fb:09:ac:d4:e2:32:42:10:49:d3:b4:20:82:85:ee (RSA)
80/tcp    open  http      Apache httpd 2.2.14 ((Ubuntu))
|_http-title: Go ahead and ScanMe!
646/tcp   filtered ldg
1720/tcp   filtered H.323/Q.931
9929/tcp   open  nping-echo Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT ADDRESS
[Cut first 10 hops for brevity]
Manual page nmap(1) line 44 (press h for help or q to quit)
```

What is the nmap command used?

**Nmap command yang digunakan dalam contoh ini adalah:  
"# nmap -A -T4 scanme.nmap.org"**

Use the search function to answer the following questions.

Questions: What does the switch -A do?

**Switch -A pada nmap memungkinkan OS dan versi deteksi, script scanning, dan traceroute.**

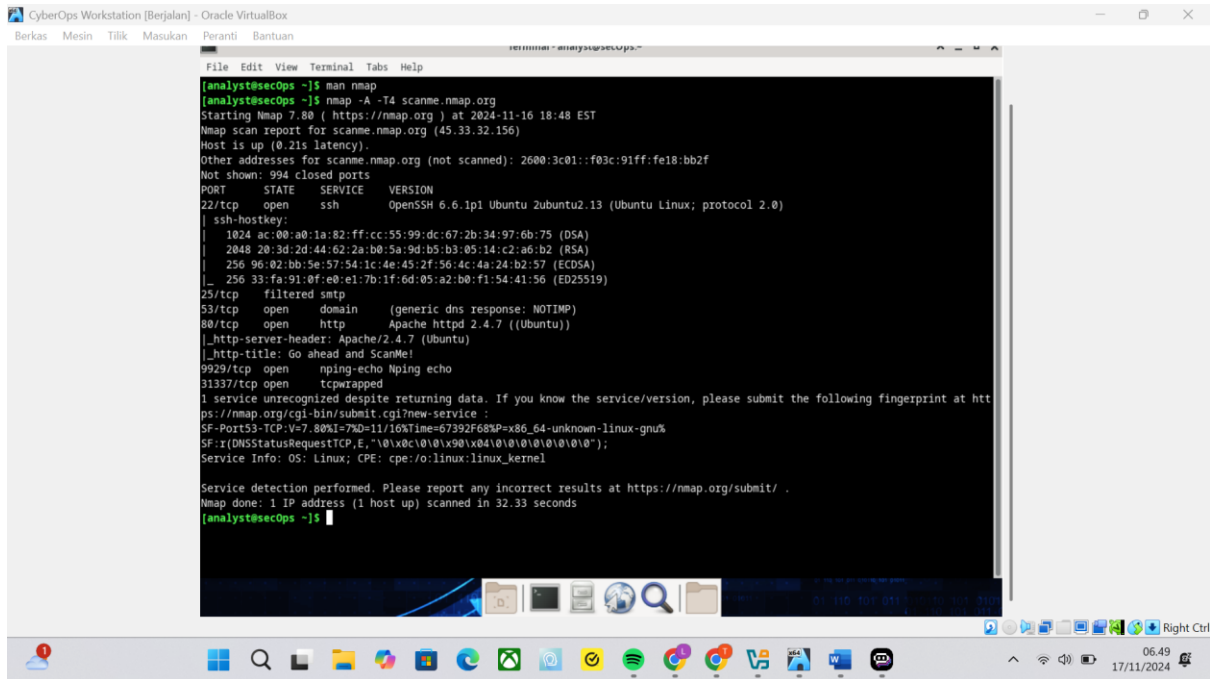
What does the switch -T4 do?

**Switch -T4 pada nmap digunakan untuk eksekusi yang lebih cepat, dengan mengatur tingkat waktu tunggu yang lebih rendah (lebih agresif).**

Type your answers here. f. Scroll through the page to learn more about nmap. Type q when finished.

## PART 2: Scanning for Open Ports

Step 1: Scan your localhost:



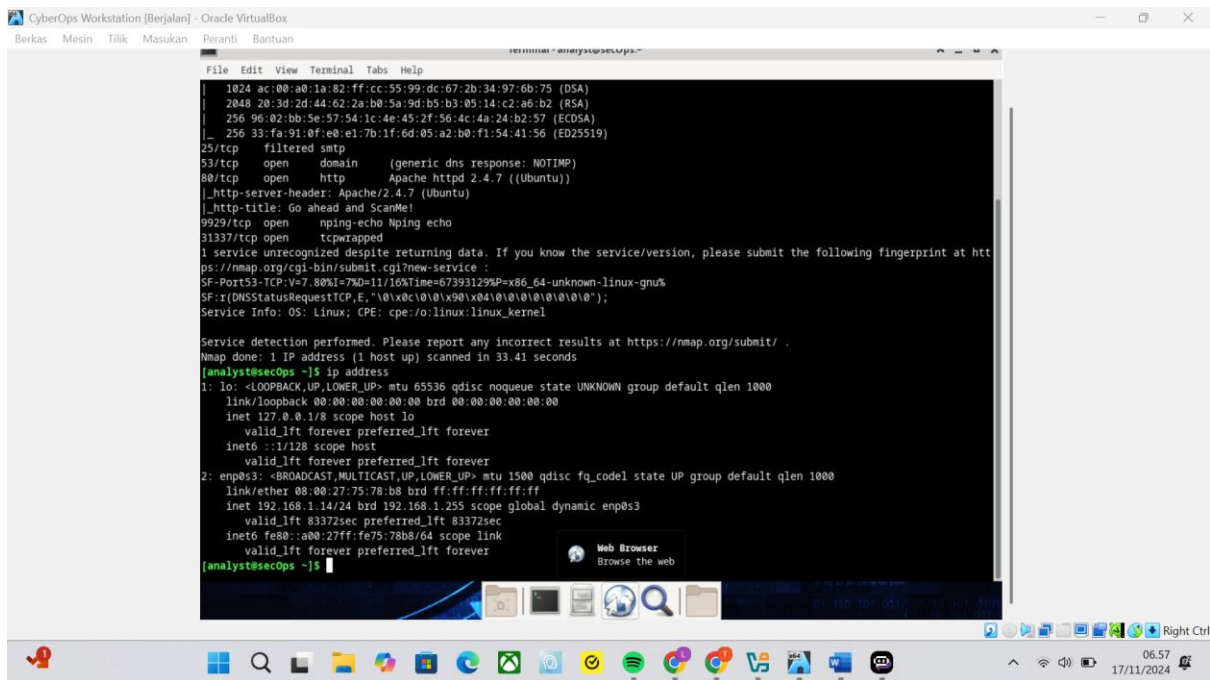
Review the results and answer the following questions. Questions: Which ports and services are opened?

- Port 22/tcp terbuka dengan layanan SSH
- Port 53/tcp terbuka dengan layanan domain (generic DNS response: NOTIME)
- Port 80/tcp terbuka dengan layanan http (Apache httpd 2.4.7 (Ubuntu))
- Port 9929/tcp terbuka dengan layanan nping-echo/Nping echo
- Port 31337/tcp terbuka dengan layanan tcpwrapped

Type your answers here. For each of the open ports, record the software that is providing the services.

Step 2: : Scan your network.

Warning: Before using Nmap on any network, please gain the permission of the network owners before proceeding.



Record the IP address and subnet mask for your VM. Question:

Which network does your VM belong to?

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
```

Dari informasi tersebut, dapat disimpulkan bahwa VM ini berada di jaringan loopback (localhost) dengan subnet mask 255.0.0.0. Jaringan loopback digunakan untuk komunikasi internal pada perangkat itu sendiri.

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:75:78:b8 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.14/24 brd 192.168.1.255 scope global dynamic enp0s3
        valid_lft 8337sec preferred_lft 8337sec
    inet6 fe80::a00:27ff:fe75:78b8/64 scope link
        valid_lft forever preferred_lft forever
```

Berdasarkan informasi tersebut, VM ini juga memiliki antarmuka jaringan enp0s3 yang terhubung ke jaringan 192.168.1.0/24. Ini menunjukkan bahwa VM ini terhubung ke jaringan lokal dengan subnet mask 255.255.255.0.





### 3. Layanan yang terdeteksi pada host 192.168.1.5 adalah:

- FTP: Versi 2.0 atau lebih baru (FTP code 230)
- SSH: Versi 0

Jadi, dari hasil nmap, terdapat 1 host lain yang Up dalam jaringan LAN yang sama dengan VM Anda, yaitu 192.168.1.5 yang menjalankan layanan FTP dan SSH.

From your Nmap results, list the IP addresses of the hosts that are on the same LAN as your VM. List some of the services that are available on the detected hosts.

### Step 3: Scan a remote server.

Open a web browser and navigate to [scanme.nmap.org](https://scanme.nmap.org). Please read the message posted.

Question: What is the purpose of this site?

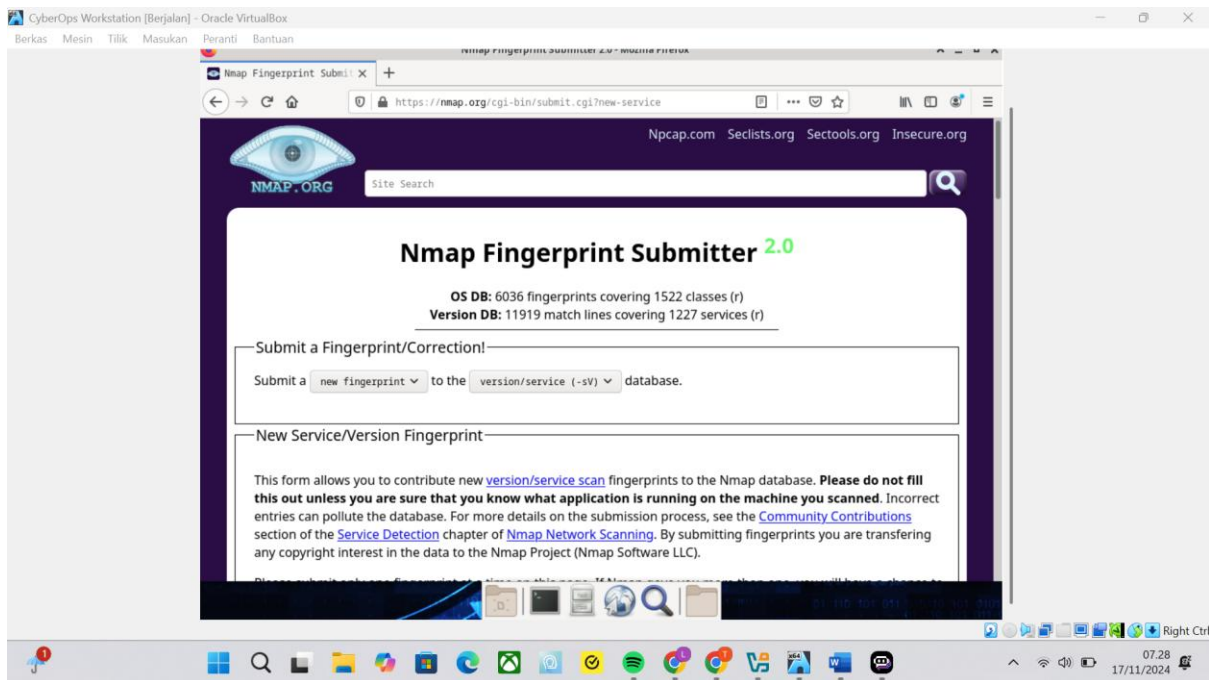
Setelah membuka web browser dan navigasi ke situs [scanme.nmap.org](https://scanme.nmap.org), saya menemukan pesan yang menjelaskan tujuan dari situs tersebut:

**"This is a test server operated by Nmap. Feel free to scan it, but please do not abuse it. You can read more about it at <https://www.insecure.org/news/Nmap-test-host-story.html>".**

Jadi, tujuan dari situs [scanme.nmap.org](https://scanme.nmap.org) adalah sebagai server uji coba yang dioperasikan oleh Nmap. Pengguna diperbolehkan untuk memindai (scan) server tersebut, namun diminta untuk tidak menyalahgunakan akses tersebut.

Situs ini digunakan Nmap sebagai server tes untuk mendemonstrasikan kemampuan alat Nmap dalam mengidentifikasi dan memindai sistem. Pengguna dapat berinteraksi dengan situs ini untuk mempelajari dan mempraktikkan penggunaan Nmap secara aman dan bertanggung jawab.

[illegible]



Review the results and answer the following questions.

Questions:

- Which ports and services are opened?

**1. Ports dan layanan yang terbuka:**

- Port 22/tcp: OpenSSH 6.6.1p1 (Ubuntu 2ubuntu2.13)
- Port 53/tcp: domain (generic DNS response: NOTIME)
- Port 80/tcp: Apache httpd 2.4.7 ((Ubuntu))
- Port 9929/tcp: nping-echo Nping echo
- Port 31337/tcp: tcpwrapped

- Which ports and services are filtered?

**2. Port yang terfilter:**

- Port 25/tcp: filtered smtp

- Type your answers here. What is the IP address of the server?

**3. IP address server: 45.33.32.156**

- Type your answers here. What is the operating system?

**4. Sistem operasi: OS: Linux; CPE:/o:linux:linux\_kernel**

Jadi, berdasarkan hasil nmap scan, server yang dipindai memiliki beberapa port terbuka seperti SSH, DNS, HTTP, serta layanan Nping echo dan tcpwrapped. Port SMTP terfilter. Server menggunakan sistem operasi Linux.



## Reflection Question

Nmap is a powerful tool for network exploration and management. How can Nmap help with network security? How can Nmap be used by a threat actor as a nefarious tool?

Nmap adalah alat yang sangat kuat untuk eksplorasi dan manajemen jaringan. Penggunaan Nmap dapat memberikan manfaat maupun risiko tergantung pada tujuan dan cara penggunaannya.

### **Manfaat Nmap untuk Keamanan Jaringan:**

- 1. Identifikasi sistem dan layanan yang aktif:** Nmap dapat mengidentifikasi host aktif, port terbuka, dan layanan yang berjalan pada jaringan. Informasi ini membantu administrator jaringan memahami infrastruktur mereka dan mengidentifikasi titik-titik kelemahan.
- 2. Deteksi kerentanan:** Nmap dapat digunakan untuk memindai jaringan, mendeteksi layanan yang rentan, dan mengidentifikasi titik-titik masuk potensial bagi penyerang.
- 3. Validasi konfigurasi keamanan:** Nmap dapat membantu memverifikasi bahwa kontrol keamanan, seperti firewall dan aturan ACL, berfungsi sesuai yang diharapkan.
- 4. Pengujian rencana pemulihan:** Nmap dapat digunakan untuk menguji rencana pemulihan setelah insiden, memastikan bahwa layanan penting dapat dipulihkan dengan cepat.

### **Penggunaan Nmap oleh Aktor Ancaman:**

- 1. Pemetaan target:** Penyerang dapat menggunakan Nmap untuk mengidentifikasi host, port, dan layanan yang aktif pada jaringan target, sehingga dapat merencanakan serangan yang lebih terstruktur.
- 2. Penembusan awal:** Informasi yang dikumpulkan melalui Nmap dapat digunakan oleh penyerang untuk mengidentifikasi kerentanan dan menyusup ke dalam sistem.
- 3. Eskalasi hak akses:** Penyerang dapat memanfaatkan informasi yang diperoleh dari Nmap untuk memperluas akses dan pergerakan di dalam jaringan yang dikompromikan.
- 4. Penyebaran malware:** Penyerang dapat menggunakan Nmap untuk mengidentifikasi sistem yang lemah dan menyebarkan malware ke dalamnya.

Oleh karena itu, Nmap merupakan alat yang sangat powerful, yang dapat membawa manfaat jika digunakan secara bertanggung jawab oleh administrator jaringan, namun juga dapat disalahgunakan oleh penyerang untuk melakukan aktivitas ilegal dan berbahaya.