Exercise: Nmap Scan of a Kubernetes Server on Ubuntu 24.04

Objective

By the end of this exercise, you will:

- Understand which services Kubernetes exposes by default
- Use Nmap to discover open ports and service versions
- Identify security-relevant information from the scan

🛠️ Prerequisites

- A **Kubernetes cluster** running (even a single-node cluster like `minikube` or `k3s`)
- A second **Ubuntu 24.04** server to act as the scanning machine
- Root or sudo access on both
- Nmap installed on the scanning machine

🧩 Part 1: Install Nmap

On the Ubuntu scanning machine

```
sudo apt update
sudo apt install -y nmap
```

🧩 Part 2: Identify Target Information

1. Get the IP of the Kubernetes master node

On the Kubernetes server:

```
ip a
```

> Note the IP address (e.g., `192.168.122.10`) to scan from the other machine.

🧩 Part 3: Perform Nmap Scans

1. Basic port scan (top 1000 ports)

```
nmap 192.168.122.10
```

Nothing should happen, because it´s just the top 1000 ports

2. Full port scan (much slower)

```
sudo nmap -p- 192.168.122.10
```

Expected open ports (for Kubernetes):

- **6443**: Kubernetes API server (HTTPS)
- **10250**: Kubelet API
- **10255**: (deprecated, read-only Kubelet API)
- **10257/10259**: Controller/Manager
- **2379–2380**: etcd ports

---

3. Service version detection

```
sudo nmap -sV -p 6443,10250,2379,2380 192.168.122.10
```

This reveals software versions, e.g.:

```
PORT     STATE SERVICE  VERSION
6443/tcp open  https     Kubernetes API server 1.28.2
```

---

4. OS detection (optional)

```
sudo nmap -O 192.168.122.10
```

---

5. Scan with Nmap NSE scripts for SSL/TLS

```
sudo nmap --script ssl-cert,ssl-enum-ciphers -p 6443 192.168.122.10
```

This checks for:

- TLS version support
- Certificate details
- Weak ciphers

🧩 Part 4: Interpreting Results

Answer the following:

1. What Kubernetes-related ports were open?
2. Was the Kubernetes API secured (HTTPS/TLS)?
3. Did any services reveal their version info?
4. Was etcd exposed externally (risk!)?

🧩 Part 5: Hardening Suggestions (Optional)

If etcd or the kubelet API is exposed:

- Restrict access via firewall
- Use authentication on exposed APIs

- Verify TLS configurations

Example:

```
sudo ufw allow from 192.168.122.0/24 to any port 6443 proto tcp
```

🧾 Summary

Scan Type	Command	Purpose
Basic Scan	`nmap <IP>`	Quick overview
Full Port Scan	`nmap -p- <IP>`	All 65535 ports
Version Scan	`nmap -sV -p <ports> <IP>`	Get service versions
TLS Analysis	`nmap --script ssl-* -p <port> <IP>`	Analyze certificate + TLS support

August 22, 2025