Laboration 5 - Port Scanning

Contents

1. Install the Nmap:

sudo apt-get install nmap

2. Scan the entire network 172.16.0.0/24 to find out which TCP ports are open inside the network:

Scan using TCP connect:

nmap -sT 172.16.0.0/24

Here are some other options with a slight descrption for each command

Scan a network and find out which servers and devices are up and running

nmap -sP 172.16.0.0/24

Laboration 5 - Port Scanning

Fast Nmap Scanning for a Network range

```
nmap -F 172.16.0.0/24
```

Sacn all Ports Using Nmap

```
nmap -p "*" 172.16.0.0/24
```

3. Scan for UDP ports

Scan UDP ports

```
nmap -sU 172.16.0.0/24
```

4. Selecting one of the computers i found that have port # 80 open and trying to find out a bit closer to :

- Detect OS and Services for the chosen computer.
- Application protocol running on the port
- Version of software running on the port

Detect OS and Services

```
sudo nmap –A 172.16.0.1
```

Using version scan to detect the OS

```
sudo nmap -sV -O –v
```

Simple usage of version detection

```
sudo nmap -sV -T4 -F 172.16.0.230
```

Laboration 5 - Port Scanning

To get version detection, you need to include the -sV flag to nmap. Alternatively, if you want the whole kitchen sink of options, you can use the -A argument, which will enable OS detection and everything else you could possibly want.

```
sudo nmap -A -T4 -F 172.16.0.230
```

```
sudo nmap -A -p 1-65535 172.16.0.230
```

To get hardware information use lshw command:

```
sudo lshw -short
```