Lab 1 - Nmap (Network Scanning)

In this lab, we explore the basic services of one of the most widely used network scanning tools: nmap.

Nmap (Network Mapper) is a network scanner used to gather information about hosts or services running on machines that are part of an internal or external network.

For your information

- There are other scanning tools such as **Superscan** and **Angry IP Scanner**
- There is a graphical interface for nmap called **Zenmap**; however, in this lab we use nmap from the command line.
- Nmap has set up a server for testing domain scans. The domain is: scanme.nmap.org

Warning — you are not allowed to scan IP addresses and/or domains that do not belong to you.

Network Scanning

1. For each of the following commands, answer the following questions:
   - What does the command do?
   - How is the command useful for an attacker?

   The commands must be run from the root shell.

   - `nmap -sP <victim IP>`
   - `nmap -sP <another IP on the network>`
   - `nmap -sS <victim IP>`
   - `nmap -sV <victim IP>`
   - `nmap -p 80,443 <victim IP>`
   - `nmap -sV -p 80,443 <victim IP>`
   - `nmap -sV -p 80,443 <victim IP> -A`

2. What are the different port states returned by nmap?

3. Other commands
   - `nmap -sV -p 80,443 <victim IP> > scan.txt`
   - `nmap -6 <victim IPv6>`
   - `nmap -sC -p 80 <victim IP>`

You can scan more than one IP address using one of the following methods:
- `192.168.12.1-100`
- `192.168.12.*`
- `192.168.12.0/24`