Activity 11 : Network Scanner with NMAP

Instructors : Krerk Piromsopa, Ph.D

Overview

We will use NMAP ("Network Mapper") to extract various information about host and environment information. Please install nmap. You may install it from the package in your system distribution. Alternatively, you may get it from https://nmap.org/book/install.html. If preferred, you may install the GUI version (zenmap).

Exercise

1. Please connect to your university network (e.g ChulaWIFI or eduroam).
   We will use a simple ping scan to identify online hosts.
   eg.
   ```
   nmap -v -sn 10.201.3.0/24
   ```

   Don't forget to substitute 10.201.3.0 with your network address.
   Please explain the parameters (-sn).

2. Pick an ip address from the list in exercise 1 (maybe get the ip address of your friend). We will try to detect OS from the network footprint.
   eg.
   ```
   nmap -v --osscan-guess 10.201.3.250
   ```

   Experiment with several operating systems (Windows, Linux, Mac OS X, iPhone, Android Phone, etc.)
   Explain how nmap identifies the operating system.
   You may use -A (Aggressive scan options) to get the result as well.

3. Assuming that you are asked to identify all web servers on a campus, which command will you use to obtain the information. Please explain with an explicit example.

There are several things that can be done with nmap. Please refer to https://nmap.org/book/man.html for more information.

Enjoy!