FIT3173 Software Security
Week 8 Tutorial: Penetration testing I

This tutorial will give you some experience in using penetration testing tools to scan target hosts. In particular, you are expected to use a widely-used tool called "Nmap" (https://nmap.org) to perform this task. Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It uses raw IP packets in ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts.

Note that nmap is already installed in SeedVM.

Task 1:
The basic nmap syntax is nmap scantype options target. The simplest way to run nmap is to provide the target host address after nmap. Address can be supplied as an ip address or as a domain name.

Type command in your terminal

```
nmap 127.0.0.1
```

Then,

```
nmap www.google.com
```

What can you learn from the output?

Task 2: Determine the operating system running on the target

```
sudo nmap -O 127.0.0.1
```

```
sudo nmap -O www.google.com
```

```
sudo nmap -O www.monash.edu
```

Observe the outputs.

Task 3: Obtain more details about the port information and services running on the host.

```
nmap -v -sV 127.0.0.1
```

Task 4: Check whether a port is open or not.

```
nmap -p ssh 127.0.0.1
```

Task 5: Check whether a host is alive or not.

```
nmap -sn 127.0.0.1
```

Task 6: Check whether a host is alive or not.

```
nmap -sn 127.0.0.1
```

Task 6: Scan a range of hosts (e.g., hosts in a subnet)

Find out the ip address of your host:

```
ifconfig
```

Assume that ip: 10.0.2.15 mask:255.255.255.0. Perform range scan (reference for subnet: https://www.tldp.org/HOWTO/archived/IP-Subnetworking/IP-Subnetworking-6.html)

```
nmap 10.0.2.15/24
```