COMP 3355 Cyber Security

Assignment 3 Tutorial

Disclaimer

"All lecture notes, handouts and discussions relating to technological means of hacking, virus attacks, denial of services or any other means of attacking a computer system are for the sole educational purpose of teaching COMP3355 (Cyber Security). Those are not intended to be adopted or applied to launch any attack on or to cause any damage to any computer system, and do not in any way encourage anyone to engage in such acts. By taking this course, you also agree not to adopt or apply any of the technological means discussed or otherwise disclosed in this course to engage in such acts."

Virtual machine

- In computing, a virtual machine (VM) is an emulation of a computer system. Virtual machines are based on computer architectures and provide functionality of a physical computer. Their implementations may involve specialized hardware, software, or a combination.

Install VMware

- Download VMware Workstation Pro 15:

https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html

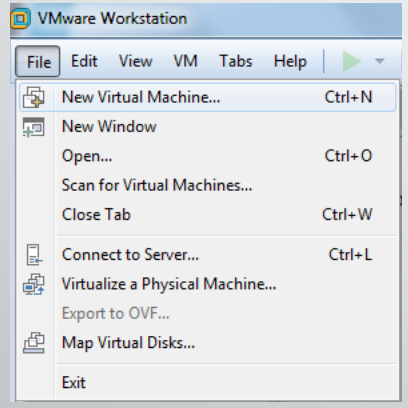
- Windows 10 image:

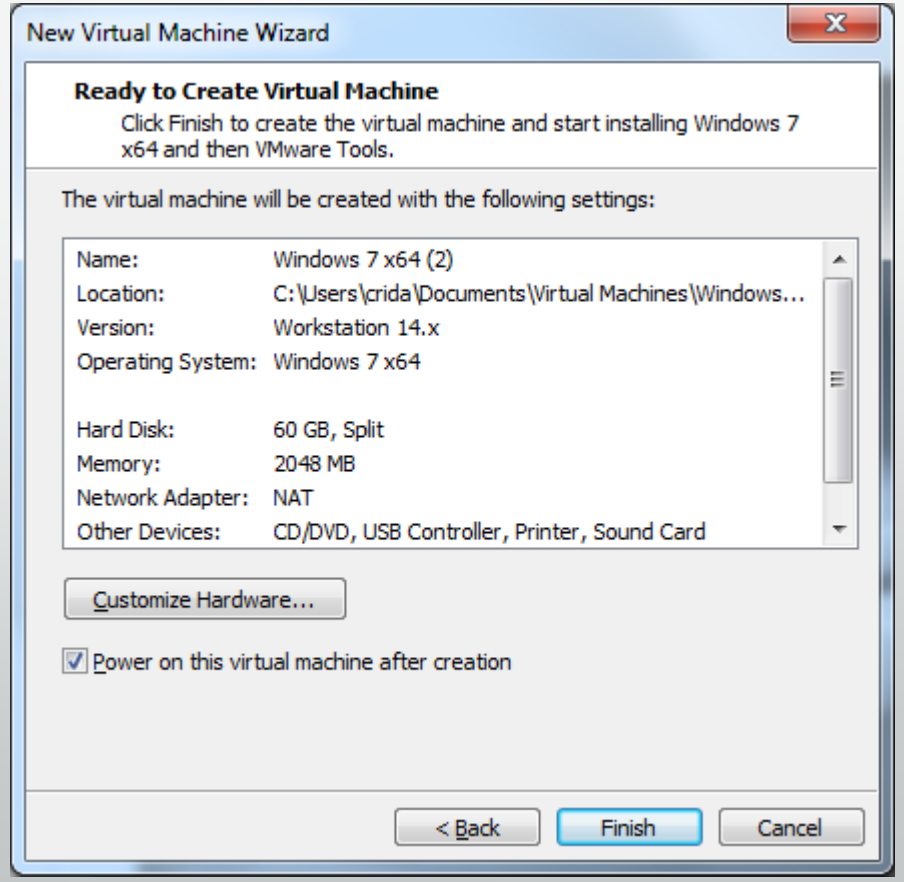
https://www.microsoft.com/en-hk/software-download/windows10ISO

Create Virtual Machine

- In this tutorial, we create a Windows virtual machine and set it to be the scanning target later.

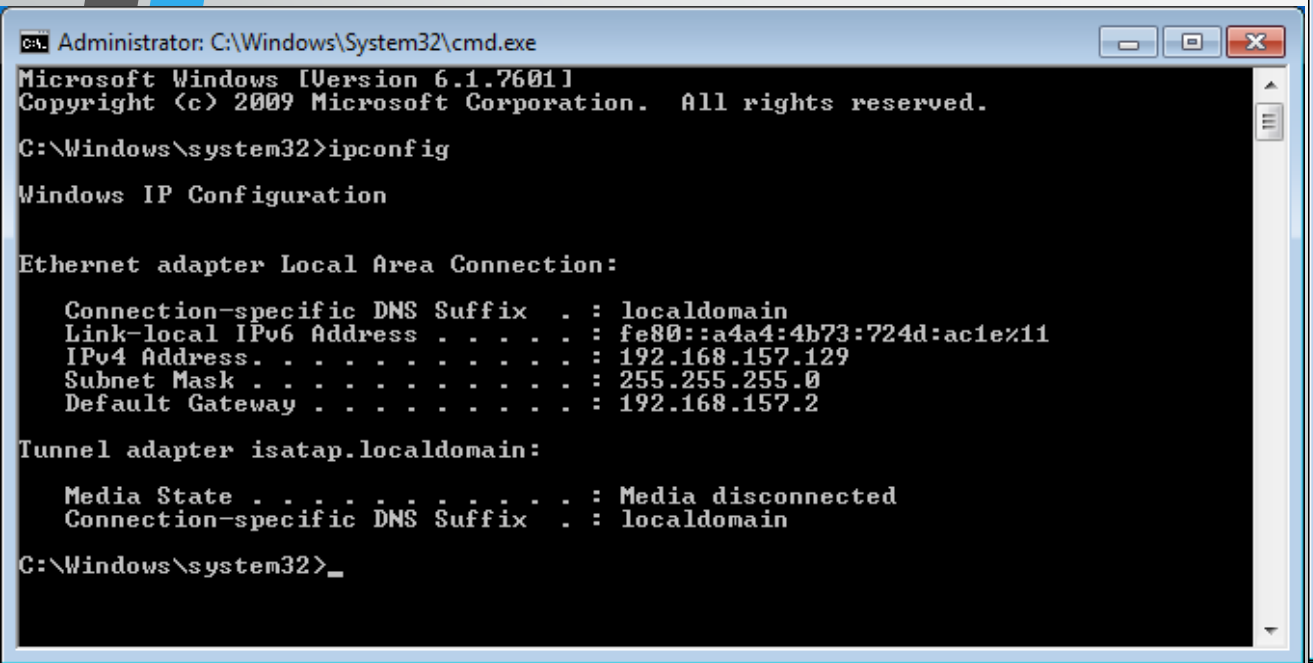
File→ New Virtual Machine

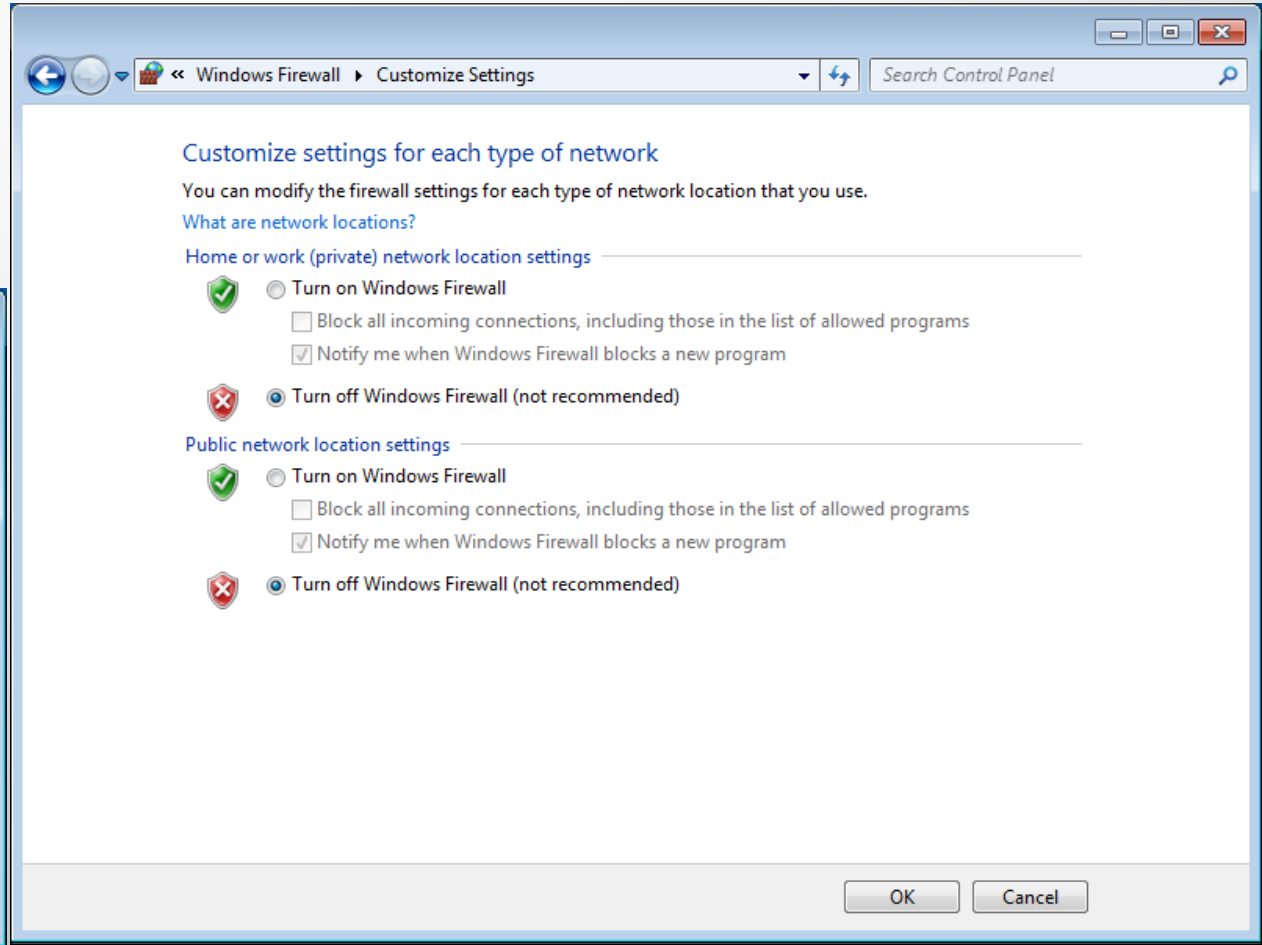




Preparation for scanning (Demo)

- Turn off the firewall on your VM
- Get your IP address
  - ipconfig

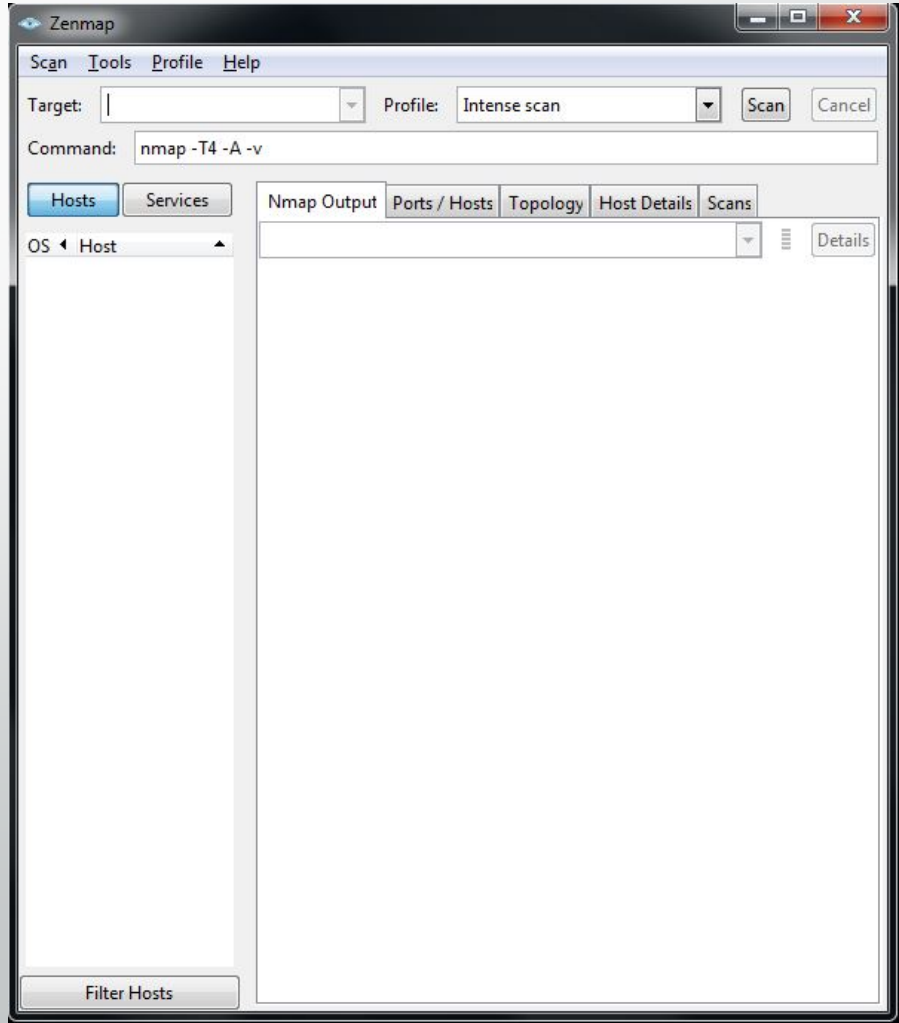




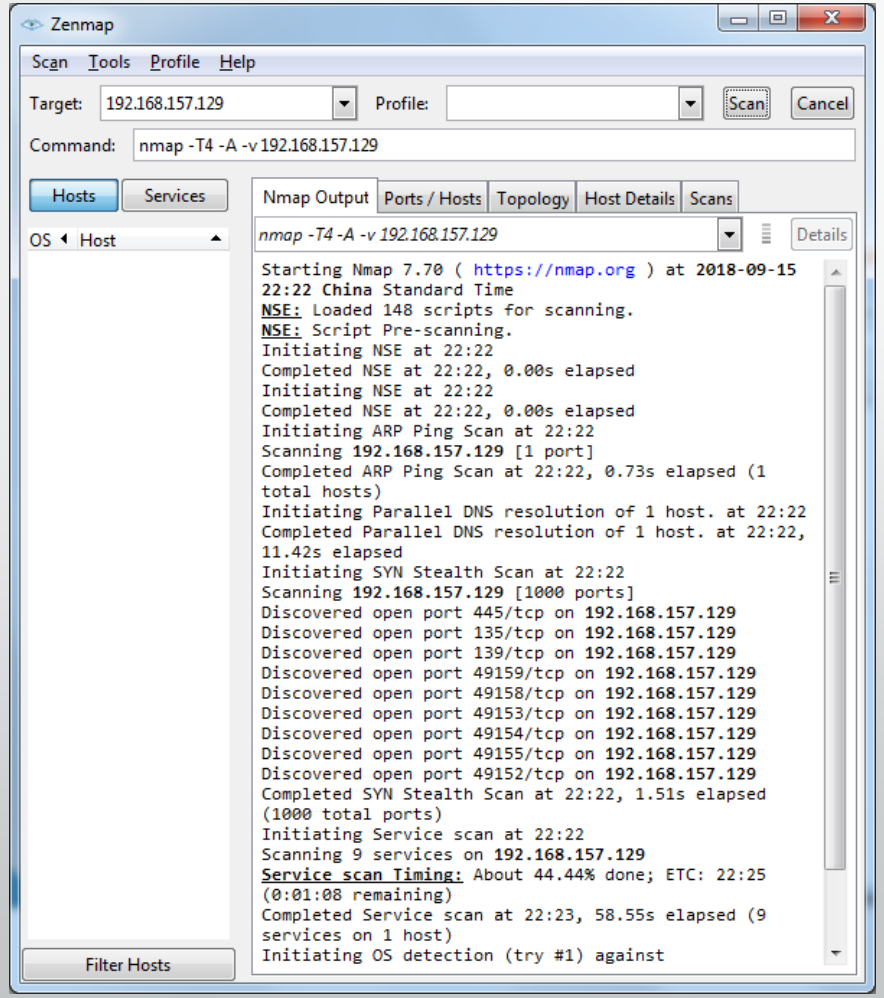
Install Nmap

- Download Nmap:

https://nmap.org/download.html



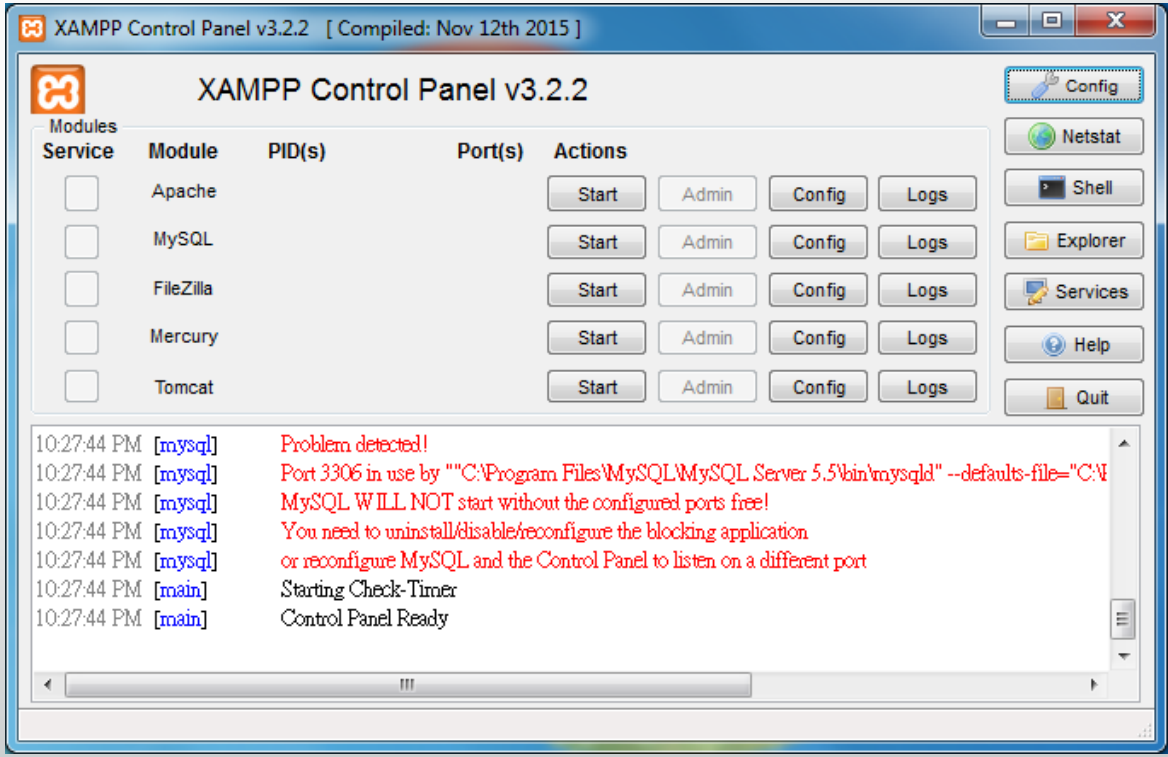
Nmap scan


Zenmap
Scan Tools Profile Help
Target: 192.168.157.129
Profile:
Scan
Cancel
Command: nmap -T4 -A -v 192.168.157.129
Hosts
Services
OS
Host
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 192.168.157.129
Details
Starting Nmap 7.70 (https://nmap.org) at 2018-09-15 22:22 China Standard Time
NSE: Loaded 148 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating NSE at 22:22
Completed NSE at 22:22, 0.00s elapsed
Initiating ARP Ping Scan at 22:22
Scanning 192.168.157.129 [1 port]
Completed ARP Ping Scan at 22:22, 0.73s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 22:22
Completed Parallel DNS resolution of 1 host. at 22:22, 11.42s elapsed
Initiating SYN Stealth Scan at 22:22
Scanning 192.168.157.129 [1000 ports]
Discovered open port 445/tcp on 192.168.157.129
Discovered open port 135/tcp on 192.168.157.129
Discovered open port 139/tcp on 192.168.157.129
Discovered open port 49159/tcp on 192.168.157.129
Discovered open port 49158/tcp on 192.168.157.129
Discovered open port 49153/tcp on 192.168.157.129
Discovered open port 49154/tcp on 192.168.157.129
Discovered open port 49155/tcp on 192.168.157.129
Discovered open port 49152/tcp on 192.168.157.129
Completed SYN Stealth Scan at 22:22, 1.51s elapsed (1000 total ports)
Initiating Service scan at 22:22
Scanning 9 services on 192.168.157.129
Service scan Timing: About 44.44% done; ETC: 22:25 (0:01:08 remaining)
Completed Service scan at 22:23, 58.55s elapsed (9 services on 1 host)
Initiating OS detection (try #1) against

Set up Web Server & FTP Server

- Download XAMPP:

https://sourceforge.net/projects/xampp/



Assignment 3

Due Date: Oct.28, 23:55

Objectives

- After completing this assignment, you should be able to:

1) Install and set up your own virtual machine on your physical machine.

2) Use Nmap to scan and enumerate the ports and services available on your VM.

3) Set up SSH Server on your VM.

Tasks

- Step 1. Install VMware on your machine and download the VM shared with Google Drive .
- Step 2. Open the VM (Windows 10 x64.vmx).
- Step 3. Take a look at XAMPP and get familiar with it . Will use it during the assignment.
- Step 4. Use Nmap to find out the open ports of the Windows VM. Take note of the result.

➢ Using appropriate options in **Nmap**, find out the **port numbers**, **service name** and **versions** of the SSH service you've set up.

Thanks!

Q&A