INFOTC 3001 - Advanced Cyber Security
Laboratory # 2 - Footprinting

I. Objectives

1) Enable a local virtual environment.
2) Perform network configuration using different commands.
3) Discover hosts and open ports on remote systems.
4) Scan ports and services remotely.

II. Material Required

Kali Linux, Kali Linux Clone, and WS2K3(TW3P0) hosts.

III. Activity

1. Clone your Kali system to KaliClone.
2. Download (from Canvas) the WS2K3(TW3P0) host and include it in your virtual environment.
3. Connect all VMs to VMnet2.

IV. Review Questions

1. Respond to the following questions:
   i. Which protocol uses the `netdiscover` command to find out IP addresses in a network?
   ii. How many UDP, TCP ports exist in total?
   iii. The port 22 is the port assigned to the SSH service, would be possible to assign a different port number to the SSH?
   iv. How many bits has a MAC address?
2. Assign the 192.168.166.201/24 to Kali host by using the `ifconfig` command. Show screenshot.
3. Assign the 192.168.166.202/24 to KaliClone host by using the `ip` command. Show screenshot.
4. Attach a screenshot of the `netdiscover` command specifying the network adapter and the 192.168.166.0 network (make sure all three systems are connected to VMnet2). The screenshot should show the IP addresses of KaliClone and the WS2K3(TW3P0) hosts.
5. Select 5 ports showed with `nmap` command over the WS2K3(TW3P0) host and explain the purposes.
6. Is there any way to use `nmap` on a Windows system or other Linux distributions besides Kali? If so, what would be the installation process in Windows and Linux systems? Check nmap.org for more information.

7. Open FTP port on ‘Kali Clone’ host (you might need to connect to the internet to install the service), from ‘Kali’ host execute:

   ```
   # nmap 192.168.166.202
   ```

   Which port number is assigned to the FTP service? Submit screenshot.

8. Use the ‘-F’ option to obtain similar results as the previous question. Compare the execution time. Which one was executed faster, why? Provide a screenshot showing clearly the execution time for both commands.