SEC 250 Network Scanning

One of the primary methods used to attack and defend networks is network scanning. This involves finding devices that are alive on a network and services being run on devices. For attackers, this information provides the basis to plan an attack. This information can also be used to secure a network as unneeded services can be shut down, firewall rules put in place, etc.

The common tool used for this is nmap/zenmap. Zenmap is a GUI-based nmap.

1. **Setup**

   Start up your Win10VM.

We want to make sure there are some services running to scan.

Make sure the webserver you set up on there is running (http://localhost will give you the MS IIS default web page, and then to the page you set up in a previous lab: http://localhost/web1.htm

Turn **all** firewalls off, and make sure others can see your webserver.

Download the Latest Stable Release nmap installer from https://nmap.org/download.html#windows

This installs nmap (command line) and zenmap (GUI) into the C:\Program Files (x86)\nmap directory.

Use the default installation selections.

2. **Find devices on the network**

   The first basic step in network scanning is to find what devices are running by doing a ping scan

   Start zenmap

   Target 192.168.1.1-254
   Profile: ping scan
   Click **scan**

   You should get a list of devices that are responding

   List 5 of them here 192.168.__. ___, ___, ____, _____, _____

3. Find open ports on a host.

   Choose a target range than includes 3 hosts

What IP range did you use? _____

Chose then Quick scan plus profile.

!= Notice in the command window that this issues an nmap command with options.

Copy the command to here and describe what the options do (except –version-light).
To find out what the options are, select Profile > Edit Selected Profile tab. In the scan tab, some of the options are checked. Look through the tabs to find all the options.

Command with options: _____

Options descriptions: _____

Now launch the scan.

Fill out the following for the host with the most services running.

What is the IP? _____

What ports were open? _____

What services were running that had open ports? _____

What is the OS guess? _____

How many filtered ports were there? _____

How many closed ports? _____

Now use the same targets, but use a Intense Scan plus UDP profile.

What additional information did you find out about the hosts regarding services running? -
_____

4. Start a new service, and see if it shows up

Start an ncat session to listen on a port (under s:\Spring2017Software if you need to recopy it).

SEC 250 Network Scanning

C:\program files (x86)\nmap\ncat -l port number (pick a port number above 1024)

What port number did you use? _____

Can your neighbor see it in a scan? _____
Provide Snip!