Activity 03.1: Perform Ping Sweep Using `nmap`

Purpose:
During this activity you will perform a port scan on your virtual host using nmap. This will familiarize you with one of the most common techniques to gather information about services running on local and remote systems.

Objective:

Learn to use the port scanning functions of `nmap` – a program previously installed on your Linux virtual machine. By learning to identify services running on local and remote systems students can start to identify services that need to be disabled or secured from unauthorized access.

Materials Required:
This exercise will require the following:

- The lastest VMware Player (http://www.vmware.com/products/player/)
- CyberPatriot Ubuntu Image

Estimated completion time: 15 – 20 minutes

Additional Information:

- None

Instructor Notes:

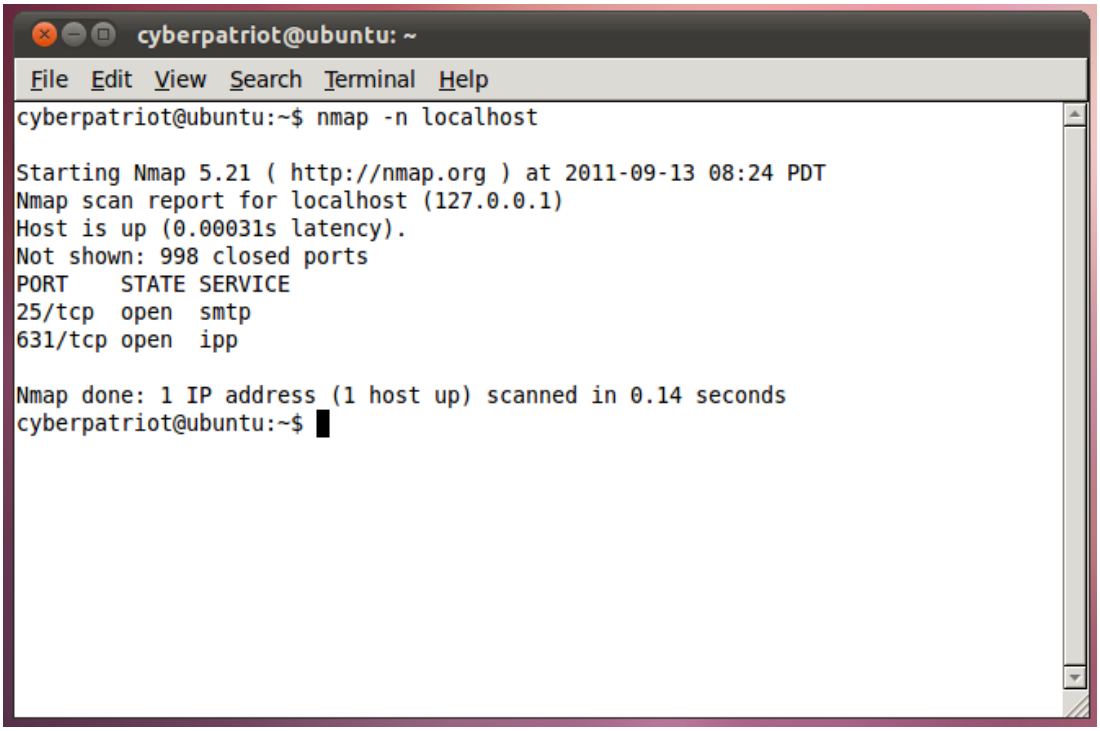
For this exercise, students will be using nmap to scan their local virtual system.

Step 1: Start up the Ubuntu VM and open up a terminal

- If you are unsure of how to do this, refer back to Lesson 3, Activity 1

Step 2: Type

- $nmap –n localhost



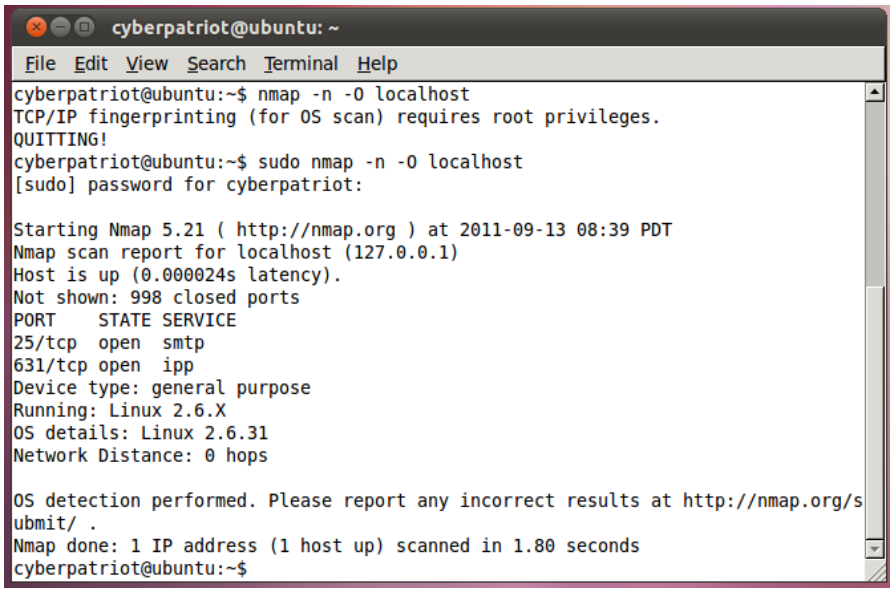
- nmap will perform a basic TCP port scan and report back any services answering.
- The port scan sends a packet to every single common port on the system being examined. If a service is running on that port – the system being examined will respond indicating that there is a service running on that port.
- If we were to change “localhost” to a network range such as “10.10.10.1-254” then nmap would perform a port scan on all the systems in that range. This technique can be used to discover which systems are active on a specific network or what services are active on those systems. **Make sure you do not perform a port scan against a system or network where you do not have permission to do so!** A port scan is considered potentially harmful traffic by some system administrators and security professionals when it is performed by people without permission to do so.
- On the results, there are Ports, States, and Services
    - The port can be listening for TCP/UDP traffic
    - The state is whether the port is open or closed
    - The service is what service nmap believes is running on there

Step 3: Do a search of what each of these services mean and do.

- Should these services be running on your computer?
- Are they critical to the operation of your computer?
- What programs are listening on these ports?

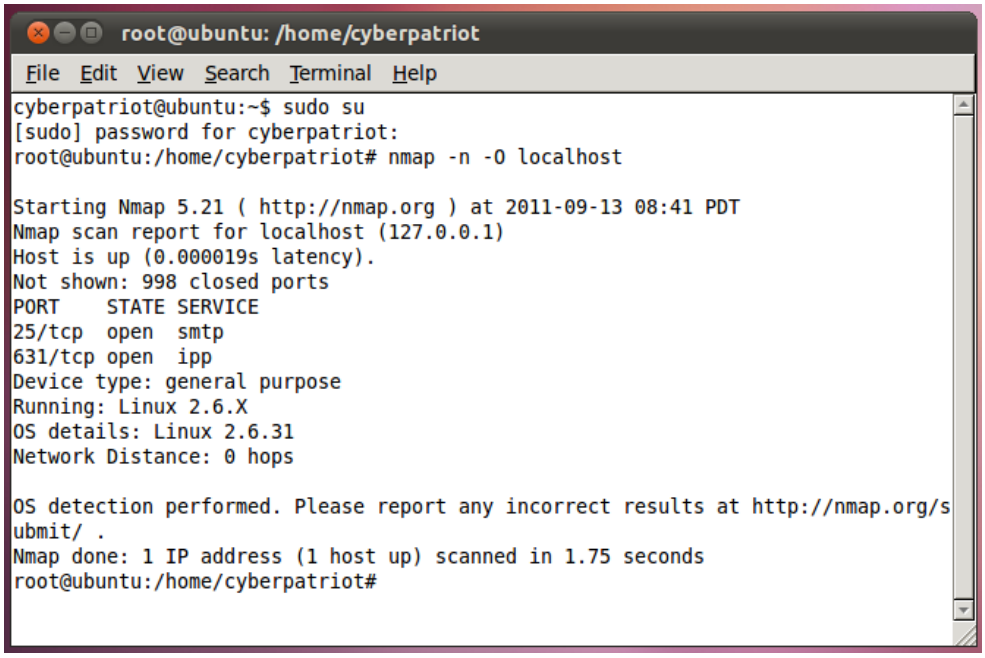
Step 4: Type

- $nmap -n -O localhost
    - It will respond that it requires root privileges. To accomplish this, you can type
        - $sudo nmap -n -O localhost
            - This tells Ubuntu that if you are allowed root privileges, run this command as root



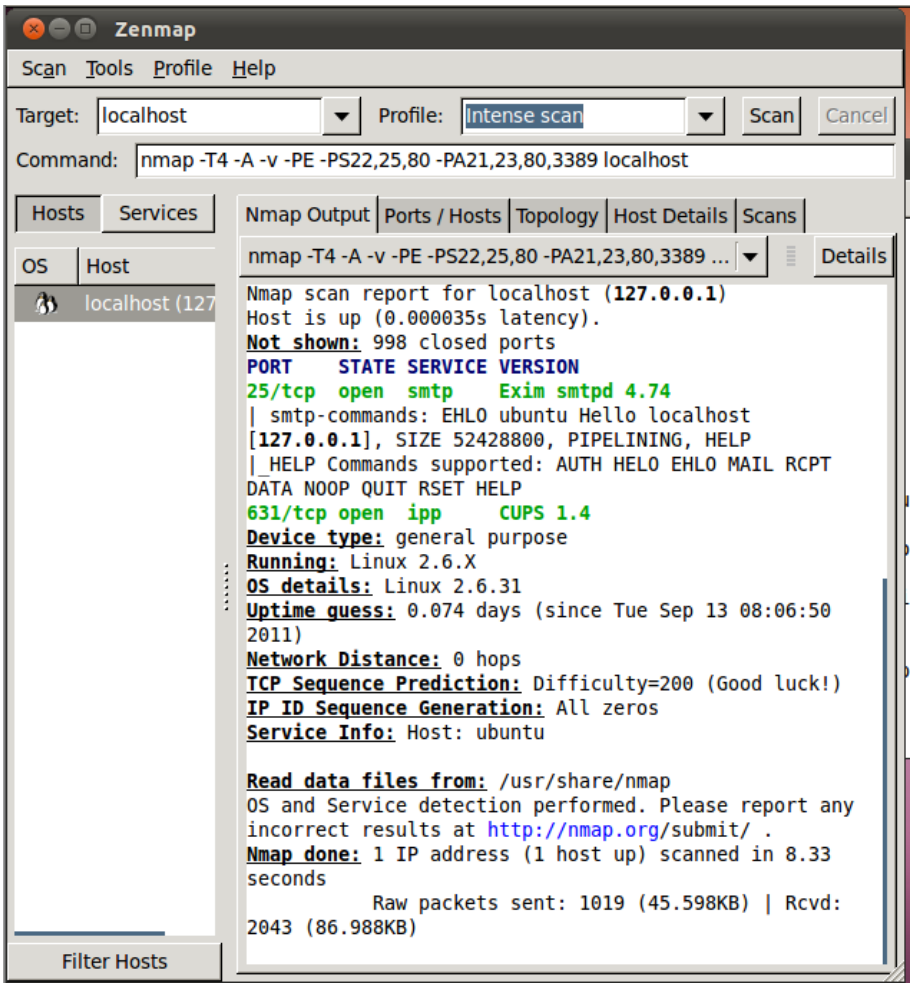
            - You can also type
                - $sudo su
                    - This tells ubuntu that you wish to switch to the root user (if the current user is allowed to)
                - #nmap –n –O localhost
    - With this command, nmap will try to identify the Operating Systeem (OS) it is scanning, along with the normal scan

*NOTE: “sudo …” and “sudo su” then “#...” do the same thing. But if you use “sudo” you must type it in front of every command you want to run as root.



Step 5: Type

- #zenmap
    - In the Zenmap GUI, type “localhost” in Target: and use “Intense scan” in Profile:
    - This scan can take a couple of minutes.
    - Take note of all of the details this give you to view.



Zenmap/nmap are very powerful programs. If you want to learn more about it, read through http://nmap.org/book/man.html