Activity 03.1: Perform Ping Sweep Using `nmap`

Purpose:
During this activity you will perform a network scan in the form of a Ping sweep on your virtual system. This will familiarize you with one of the most common techniques to gather information about a target environment.

Objective:
Learn to use the ping sweep function of `nmap` – a program previously installed on your Linux virtual machine.
NOTE: Prior to beginning this lab you should have downloaded the CyberPatriot Fedora Core 12 virtual image.

Materials Required:
This exercise will require the following:

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

Estimated completion time: 5 – 10 minutes

Additional Information:

- None

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

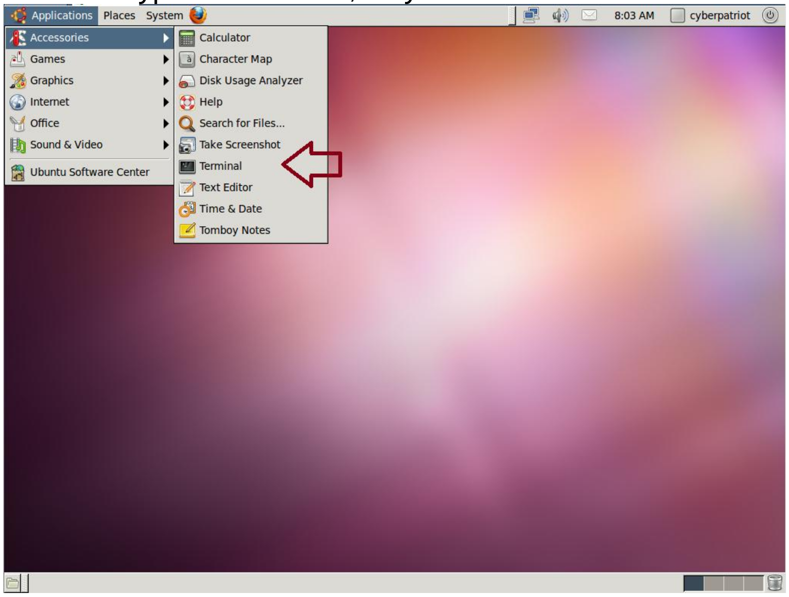
Step 1: Start the Ubuntu VM Image.
Step 2: Log onto the virtual machine using the “CyberPatriot” account.

- The password for this account is “cyberpatriot”

- **Note:** Please keep in mind that all commands in Unix/Linux are case sensitive. For example, “**student”** and “**Student”** are not the same.

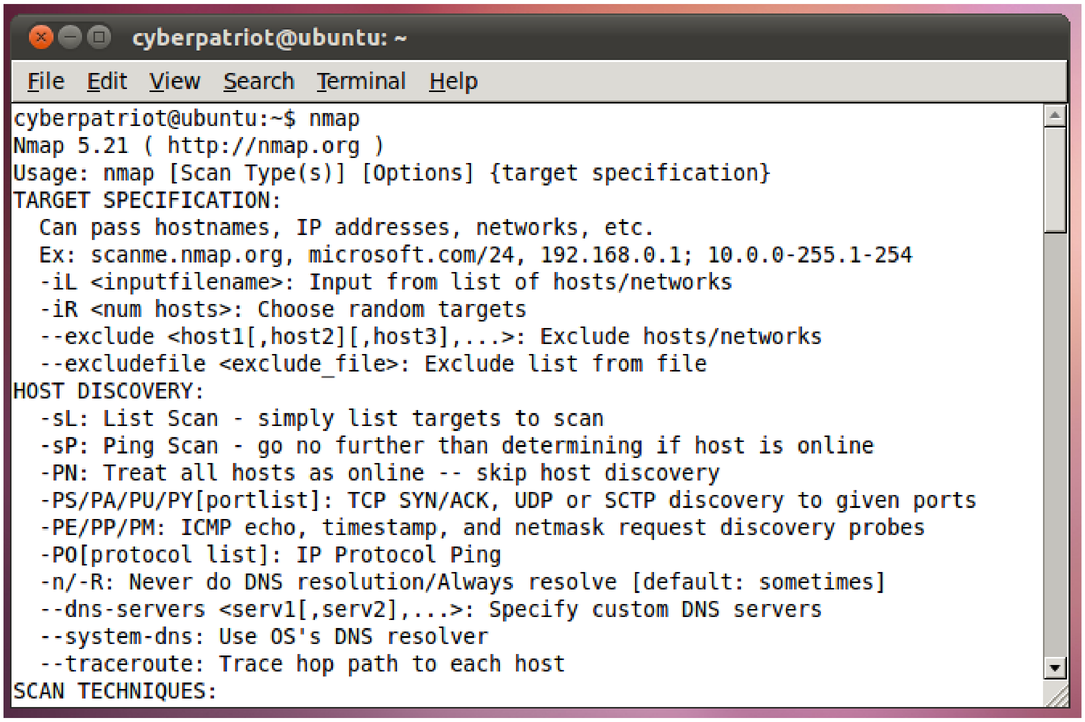
Step 3: Open up a **Terminal** Window (The terminal is known as a **Bash Shell**)

- On the top right corner, there is am Applications tab.
- Click Applications -> Accessories -> Terminal
- Note: when a command is started with a $, this means the command is run as a normal user. If it is started with a #, this means the command is run as the root, or admin, user. Do not type in the $ or #, only what is after



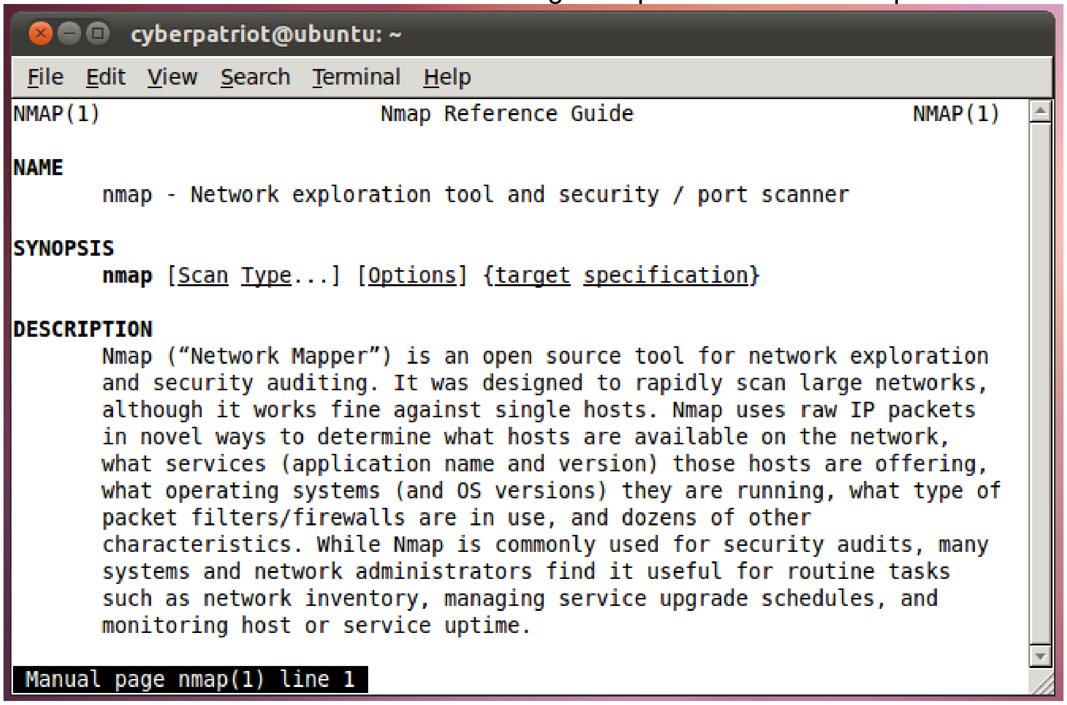
Step 4: type:

- $nmap
  - Since we did not give it any arguments, it presents us with how to run nmap.



```
cyberpatriot@ubuntu:~$ nmap
Nmap 5.21 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -PN: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

- $man nmap
    - This command presents us with the man pages of nmap. This will help you in how to run it.
    - Pressing ‘q’ will get you out of the man page, and pressing enter or the down button will scroll down. Pressing the up button will scroll up.

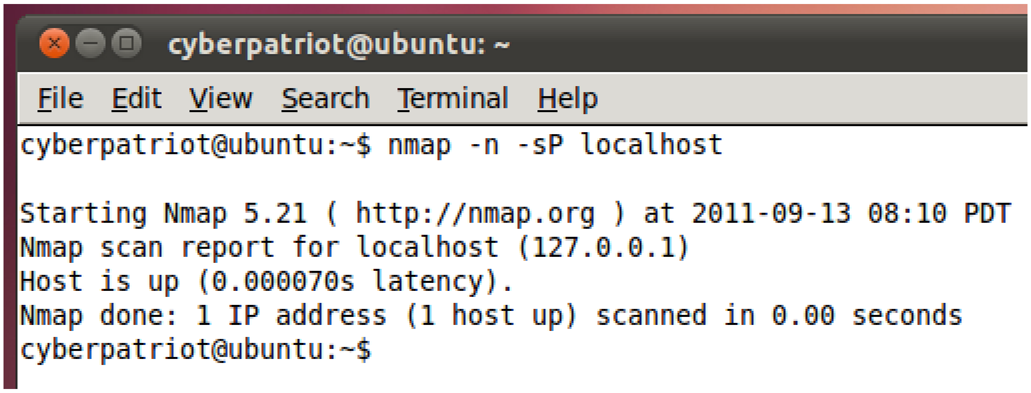


```
NMAP(1)                       Nmap Reference Guide                     NMAP(1)

NAME
       nmap - Network exploration tool and security / port scanner

SYNOPSIS
       nmap [Scan Type...] [Options] {target specification}

DESCRIPTION
       Nmap (“Network Mapper”) is an open source tool for network exploration
       and security auditing. It was designed to rapidly scan large networks,
       although it works fine against single hosts. Nmap uses raw IP packets
       in novel 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. While Nmap is commonly used for security audits, many
       systems and network administrators find it useful for routine tasks
       such as network inventory, managing service upgrade schedules, and
       monitoring host or service uptime.

 Manual page nmap(1) line 1
```

Step 5: Type

- $nmap -n –sP localhost

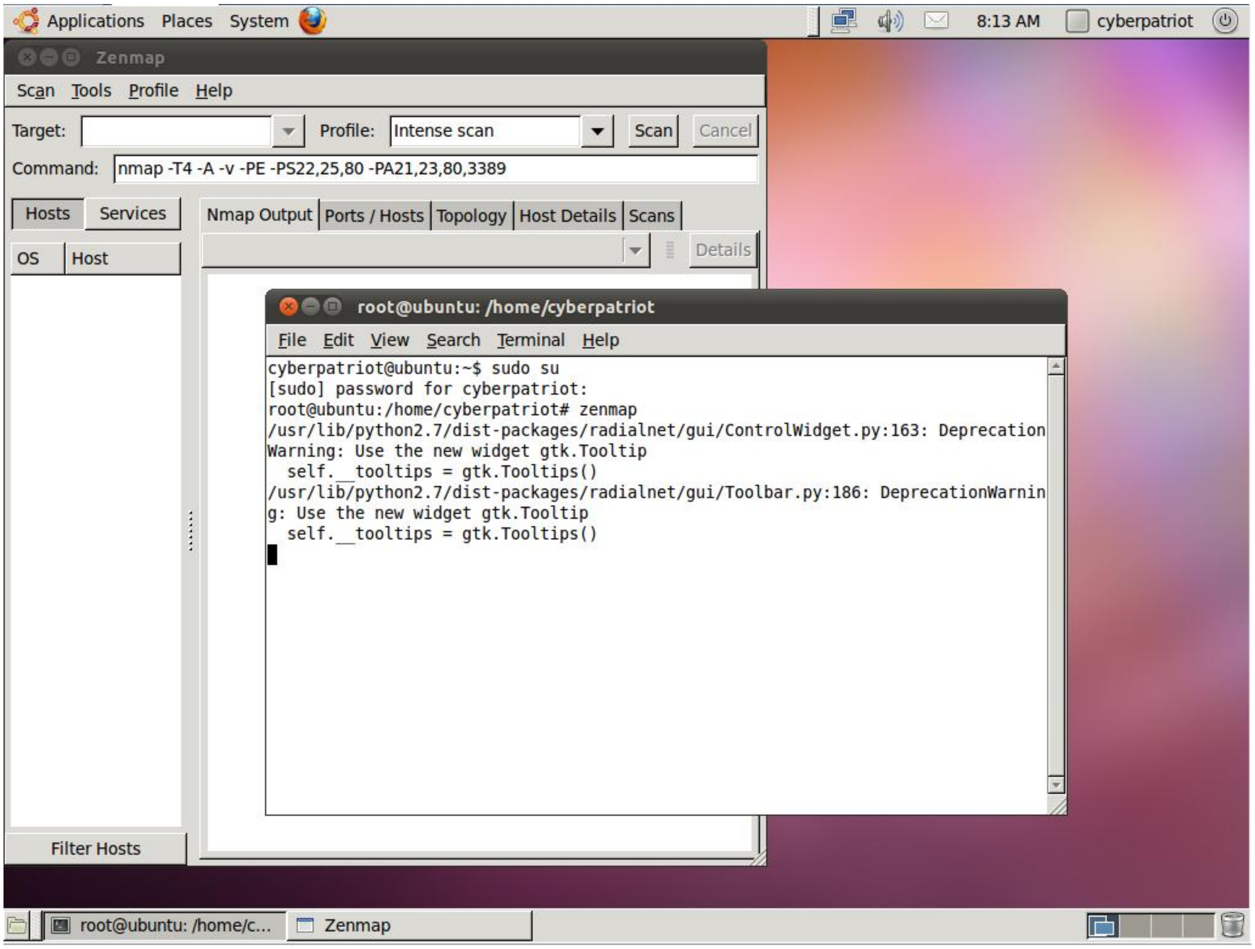
- –n, -sP, and localhost are all known as arguments. They tell nmap what specifically to do.
- –n tells nmap not to resolve localhost with DNS
- –sP tells nmap to ping the host to see if it is online
- localhost tells nmap to scan localhost, or the machine it is running on
- The "-sP" option send an ICMP ECHO_REQUEST packet to every system you've told it to – in this case we only asked nmap to send a single packet to our local system (the virtual image itself). When a system is "pinged" like this it will typically respond with an ICMP ECHO_RESPONSE packet. If nmap receives an echo response from one of the systems it "pinged" it will report that system as being "up". In our example screenshot above we see the words "Host is up" and "1 host up". This indicates that our system is active and accepting ICMP packets.
- If we were to change "localhost" to a network range such as "10.10.10.1-254" then nmap would send a packet to every system in that range and report back which systems responded. This technique can be used to discover which systems are active on a specific network or whether or not a specific system is active. However, these results should be viewed carefully – not all systems or networks respond to ICMP packets even when they are up and running. Many organizations do not allow ICMP packets through their firewalls.



```
cyberpatriot@ubuntu:~$ nmap -n -sP localhost

Starting Nmap 5.21 ( http://nmap.org ) at 2011-09-13 08:10 PDT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000070s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.00 seconds
cyberpatriot@ubuntu:~$
```

Step 6: Zenmap

- Type
  - $sudo su
    - You will be presented with a password prompt. Enter in "cyberpatriot"
  - #zenmap
    - You will then get the program zenmap. This is a Graphical User Interface (GUI) for nmap



Target:

Profile: Intense scan

Command: nmap -T4 -A -v -PE -PS22,25,80 -PA21,23,80,3389

root@ubuntu: /home/cyberpatriot

```
cyberpatriot@ubuntu:~$ sudo su
[sudo] password for cyberpatriot:
root@ubuntu:/home/cyberpatriot# zenmap
/usr/lib/python2.7/dist-packages/radialnet/gui/ControlWidget.py:163: Deprecation
Warning: Use the new widget gtk.Tooltip
  self.__tooltips = gtk.Tooltips()
/usr/lib/python2.7/dist-packages/radialnet/gui/Toolbar.py:186: DeprecationWarnin
g: Use the new widget gtk.Tooltip
  self.__tooltips = gtk.Tooltips()
```

Step 7: Using Zenmap

- In target, type “localhost”
- In Profile: You can pick any of the scans. In the screenshot, I chose “Intense scan”
    - Note: these scans can take a few minutes. Quick Scan will only take 20-30 seconds.

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