Lab 03: Enumerating Hosts using Wireshark, Windows, and Linux Commands

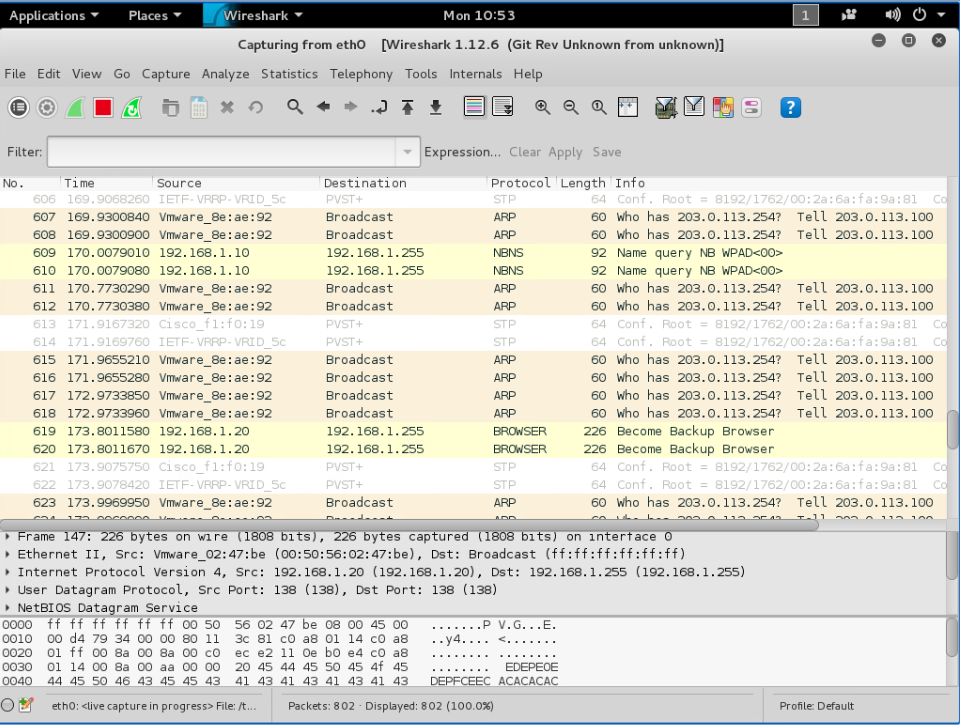
Lab report template Name: Kevin Ubilla

This Lab is required for Unit 2. It is worth 15 points. The Challenge exercises is worth 2.5 Extra Credit points.

1. **Passive Scanning, Step 10:** In your own words, please explain why you wish to suppress your IP address while scanning? (Just a sentence or two, please.)

**→ It can alert other hackers of my presence. With my IP address, they can follow my every move, or worse. ←**

1. **Passive Scanning, Step 18:** Please capture a portion of the Wireshark screen that displays captured packets from 192.168.1.10, 192.168.1.20, and 192.168.1.254 and paste it in here **(I am asking for all three in one capture, but two captures will do)**:

**→ ←**

1. **Passive Scanning, Step 18:** In your own words, please tell us if 192.168.1.101 was visible as an address in any packets during the scan. Why should it have been (in)visible?

**→ It is not because we suppressed it using ifconfig in a previous step, setting it to 0.0.0.0 ←**

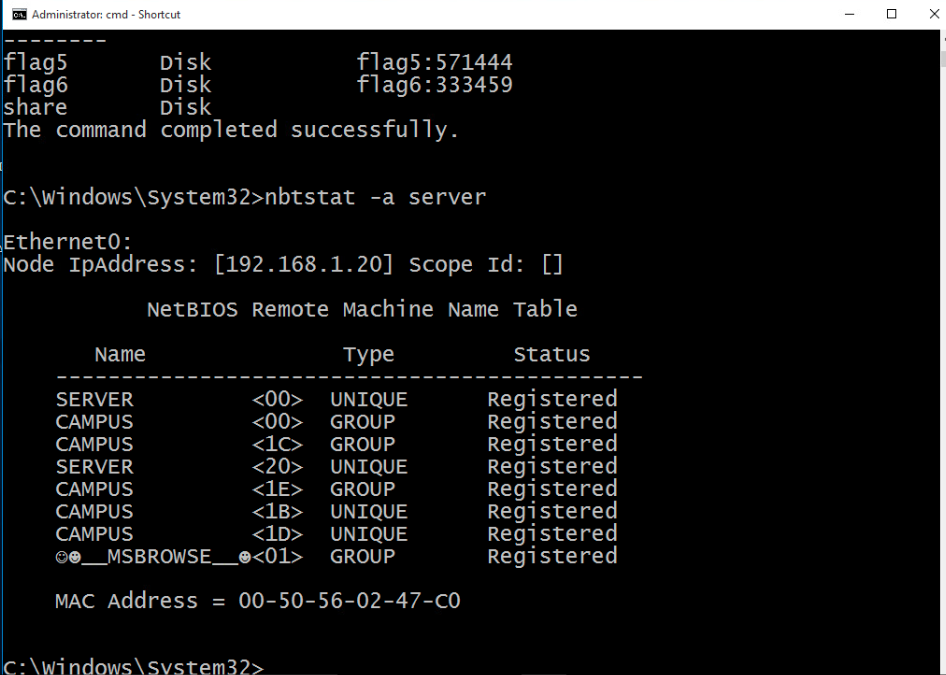
1. **Passive Scanning, Discussion Questions:** In your own words, please tell us what ifconfig is.

**→ ifconfig is a command line tool that we can use to display and configure all the interfaces on a Linux system ←**

1. **Active Scanning with Commands, Step 10:** Please capture the command prompt screen showing your command "**net view \\server**" and the response to it, down to the line that tells you it has completed successfully and paste it here **(please paste it as “in line with text”)**:

**→  ←**

1. **Active Scanning with Commands, Step 12:** Please capture the command prompt screen showing your command "**nbtstat -a server**" from your command down to include the line with the MAC address and paste it here **(please paste it as “in line with text”)**:

**→  ←**

1. **The entire Lab exercise:** At this point, you have used a number of “switches” with the nmap command (“-T4”, “-A”, “-v”, “-O”), please write, in your own words, what each of at least four of these switches does:

**→**

**-O: detects the operating system**

**-v: increases verbose level, which prints more info about scan in progress**

**-A: detects OS, version, script scanning, and tracer route**

**-T4: makes nmap work faster by prohibiting dynamic scan delay from exceeding 10 ms for TCP ports**

**←**

1. **Active Scanning with Tools, Step 7:** Please capture the command prompt screen from where you typed the command “**hosts**” down to the line detailing the fourth host **(please paste it as “in line with text”)**:

**→ Graphical user interface, text

Description automatically generated←**

1. **Active Scanning with Tools, Step 12:** Please capture the Armitage screen that shows all four systems you “fingerprinted” with the graphic depicted the OS for each on the depiction of the system monitor **(please crop it to optimize the text for reading and and paste it as “in line with text”)**:

**→ Graphical user interface, website

Description automatically generated ←**

**If you encountered any issues, either positive or negative, with this Lab, please let me know by commenting here. (This IS an experiment, after all.) I am tuning this according to what you say.**

**→ ←**