

Discussion: It's hard to imagine an operating system that exists today without a network interface. Certainly all of the major desktop and server OS's that we are familiar with do, and even most so-called "embedded" systems like DVD's, TV's, TIVO's, (even refrigerators) nowadays have a network interface, thus the world's ever expanding challenge of cyber security. The physical network interface is often implemented with a "card" inserted into the computer, so you will often hear the name "network interface card" or "NIC." Somehow, however, the computer has to incorporate that card into the operating system so that it can be used as a communications device. The NIC handles all of the layer 1 (physical) and most of the layer 2 (data link) functionality for the computer. Today we will explore this network interface in detail.

Reading Assignment: Frenzel pp. 459-463.

Setup: Open your personal Ubuntu Virtual Machine (VM) using VSphere Client and be sure you are at a CLI with the "Midshipman" user prompt. You will have sudo NOPASSWD privileges on your machine, so be careful! Note: The options for sudo are changed using the "sudo visudo" command, which edits the /etc/sudoers file and tells the system who gets those rights and sets options like "NOPASSWD." Type in "cat /etc/sudoers" if you are curious to see.

1. In the CLI, type this command and write down the output (three lines):

```
$ dmesg | grep vmx
```

This will print out a filtered list of kernel messages that were logged at bootup. The "kernel" is the part of the OS that does the heavy lifting of making all the parts of the computer work together, so it has to recognize and install a "driver" for the NIC if it's going to be used. The kernel does this step for every bit of hardware in your computer when it starts up (it basically queries everything and looks for a response). The NIC we are using is made by VMWare, since they are the vendor of our virtual machine. It's really a "virtual NIC," but don't let that bother you.

2. Now type this command:

```
$ ifconfig -a
```

You will see a list of multiple groups, listed on the left. Write down the names of those groups. These are a listing of all the network interfaces available on your computer.

3. We are first going to concentrate on the one titled “lo,” which stands for “local loopback.” So many modern software programs use a network interface that we have to have some method of providing an interface even if there is no actual NIC in the computer. The “lo” interface is an internal NIC that all computers have, and it is used whenever a program needs to talk to the host computer itself, or if a program needs to be tricked into thinking that it is using a network. It is sometimes also called the “dummy” interface or the “local **home**” interface, but these are not quite accurate, technically. There is an “`inet addr:`” field in that listing – write it down and we’ll come back to that when we get to IP addresses. This address is a standard used by all computers for this purpose. Note: I once saw a geek’s bumper sticker that said, “There’s no place like _____” (fill in your answer from below).
4. In the Ubuntu GUI, left click on the network icon on the top right of the display and then select “manual configuration.” Explore the options and tabs in this window. Does what you see in the GUI reflect what you see in the CLI?
5. Now close the settings window and focus on the top interface on the CLI (eth1). Write down the entire top line and see if you can guess what each element means. If you need help, you can type “`man ifconfig`”.
6. On the second line, there is a field called “MTU.” What is this and what does the value represent?

7. The next several lines contain overall stats about receive and transmit. What can you infer from these?

8. The final line might look a touch familiar. What do you think the hex value is?

We're going to ignore the second grouping for now, since we have more to learn about IP addresses. We'll dive into that next lab. For now, type in the following:

```
sudo ifconfig eth1 down
```

and hit enter. Then do both "ifconfig" and "ifconfig -a". What is different? Why is eth1 still there?

9. From step 4, you wrote down a "HWAddr." What is that also known as? Which digits would tell you the vendor of the NIC? Look it up on the internet and write down what you find. With minimal searching you should be able to find the answer.

10. How many possible numbers can be formed with one of these addresses?

11. How many addresses does each vendor have in each group (assume they have only one group – in reality major vendors have many).

Conclusion and Results:

Your typed lab report will consist of two paragraphs, in the first paragraph:

- Briefly describe what you did in the lab in your own words.
- Discuss something new that you learned.

In the second paragraph, answer the questions:

- How could an adversary use this knowledge or these tools for malicious purposes?
- How could you use your new understanding to protect your systems and personnel from attack?

Staple the completed report to the back of your original lab and turn it in to your instructor at the beginning of the next class.