**ITP 125 – Lab 03 – Basic Networking Commands**

**Due:**

1 minute before the next class lab

**Submission:**

1. Answer the questions at the end of this file, and name the document lab03.docx

You can directly add the screenshots into the word document.

1. 7zip the file with either 7zip (Windows) or Keka (OSX) and set a password for the decompression. The password should be dialupkid
2. Place the encrypted document into the repo and push to changes GitHub

**Procedure:**

In the steps ahead, **do not type the > symbol**. It is used to represent the command prompt. For OSX, start up terminal in order to do the commands. Look at the **OSX** section to see how to perform the commands.

1. Open a command prompt/terminal in by doing the following:

**Windows:**  
  
Right click the key on the *Desktop* and select *Command Prompt (Admin)*

**OSX:**

Either search for “*terminal*” or go to “*Applications 🡪 Utilities 🡪 Terminal*”

1. Let’s view the networking configuration by typing the following command:

**Windows:**

> ipconfig /all  
  
This command displays all the network configuration settings on the computer.   
  
For your lab, your network settings are under wherever you see an IP address.  
  
It shows the following

* + - All the network cards installed on the machine
    - All the IP address associated with each network card
    - The MAC address of each network card
    - The gateway/router for each network card

**Note:**

It is not always “Local Area Connection”, the lab is setup in a way that you will see a IP address similar to 192.168.1.\*. If you’re on the USC wireless, it may start with a 10 or 68

**OSX:**

*# ifconfig –a*

It shows the following

* + - All the network cards installed on the machine
    - All the IP address associated with each network card
    - The MAC address of each network card

Refer to the Windows steps to get some idea as to what is going on.

1. If you are ever having trouble with your Internet connection on the computer there are two things you can do to test it.  
     
   First test the connection between your computer and a DNS server that never goes down. In the command prompt type the following:

**Both:**

*ping 8.8.8.8*

Second, test the connection between your computer and a server on the Internet. In the command prompt type the following:

**Both:**

*ping www.usc.edu*

In each case, if you don’t get a reply from the machine you will see a “connection timeout” message. If you do get a reply, it means that everything is working up to that point.

1. One interesting way to see all the computers/routers between you and a server is using the traceroute command. In this case, the first hop/entry is considered the router/gateway of your network. In the command prompt, type the following.

**Windows:**

*> tracert www.google.com*

**OSX:**

*# traceroute www.google.com*

**Note:**

This takes advantage of the IP TTL field.

1. One way for a computer to keep track of the other machines on the network is by MAC address (layer 2 on the OSI model). Often the computer needs a way to translate IP address to MAC address. This is translation is called ARP (Address Resolution Protocol). To see some results of ARP, type the following in the command line:

**Both:**

*arp –a*  
  
This will display the MAC address to IP address that the machine discovered.

1. Using the procedure from step 2, get the MAC address of the network card with something similar to 192.168.1.## address (remember it can start with a 10, 68, or anything else). The MAC address is called Physical Address in Windows  
     
   Go to the following website:  
     
   <http://www.macvendorlookup.com>

Put the MAC address that you found inside the input box, and see the results. You can see the manufacture of the network card based on the MAC address.

1. One other thing that the computer needs to translate when connecting to the Internet is the domain name to IP address. Computers work better with numbers, but people work better with names. DNS (Domain Name System) was developed to do just this.  
     
   Using what you learned form step 3, get the IP address of Google, and put the numbers into your web browser. Notice that it should work.

For example:

128.125.253.136

1. Before DNS, network administrators needed to create a list of IP addresses to names. This list was stored in a file called ‘hosts’. Most if not all operating systems will check this ‘host’ file before it asks the DNS for the name to IP address translation. Do the following:  
     
   Hit the key and type *notepad*.   
     
   Note: Don’t press select the program yet  
     
   Right click on *Notepad* in the search results and select “Run as Administrator”  
     
   Goto File 🡪 Open 🡪 C:\Windows\System32\drivers\etc\  
     
   Select “All files” in the drop down menu on the bottom of the dialog window  
     
   Open the ‘hosts’ file.  
   In this file, you type in the IP address then the name. Try adding the following entry at the end of the file.   
     
   204.79.197.200 google.com

204.79.197.200 www.google.com

204.79.197.200 encrypted.google.com  
  
Note: Make sure there isn’t a # at the start of the line you just entered. The # represents a comment in the file.  
  
Try to go to Google in your web browser and see what happens.

**OSX:**

The file is actually in a different directory location. In order to do this you need to learn to use a text editor like vim, nano, or emacs. If you’re just starting out, I suggest to use nano as it is very easy to start off with. So you need to run the following commands:

*# sudo nano –wc /etc/hosts*

You will be prompted to enter the password for you account (assuming your account has administrator access). The format for the file is exactly the same.

**Questions:**

1. In step 3 of this lab you worked on the ping command. It is a great command for network administrators to see if a machine is responding on the network. Some cleaver people figured out how to use the command at an attack tool, and they call it the “Ping of death”. What is it and how does it work?

Ping of death of back then is a DOS attack. DOS stands for Denial of service attack that sends tons of packets of data to a specified IP address to theoretically over load it so It couldn’t handle any more.

1. In step 5 of this lab, you worked on a network command that shows the translation of MAC addresses to IP addresses. People who have studied ARP have figured out a way to use it to their advantage.   
     
   What is ARP spoofing and why is it dangerous? Try to explain to me how it works as if I was a 5 year old.

-ARP spoofing is cloning your mac address to be an actual IPV4 address. You can then spoof your IPV4 address broadcasting from your computer and then make the router think that you’re actually the router and then all traffic will be directed towards you.

-For 5 year old: Bad guy & good Guy. Good guy has a lot of friends. Bad guy takes good guys mask and puts it all. Now all good guys friends are going to bad guy. And he is taking all his friends.   
  
What can be done to prevent it?

There is no way.x  
  
Hint: Wikipedia is your friend.

1. In step 7 of this lab, you were (re)introduced to the concept of DNS. Basically every computer needs to ask the DNS server for the IP address of a domain name. For example:  
     
   google.com 🡪 74.125.224.221  
   usc.edu 🡪 128.125.253.136  
     
   Once again people were able to figure out how to take advantage of the system. Read the concept of “DNS spoofing”.   
     
   What can the attack do, and how does it affect regular people who are not experts in technology?  
     
   What can be done to prevent this attack?

-Keep resolver private and protected

- use a proxy XD  
  
Hint: See questions 1 and 2 hints.

1. At the beginning of this lab, it was mentioned that you would be working with layers 2, 3, 5, and 7 of the OSI model.   
     
   Looking back at each step in the procedure, label the corresponding layers of the OSI model they are working in.   
     
   Did we miss working in a layer?  
     
   Hint: Some steps may have more then one layer. Try to figure it out to the best of your knowledge.

Layer 2: The data-link layer

Layer 3: The network Layer

Layer 5: The Session Layer

Layer 7: The application model

OSI: Open system interconnection

1. Search up the term TTL. You did a traceroute that took advantage of this field in the IP header. What exactly is TTL and how does it work?

-A trace route is how your request is routed through all these different servers/firewalls to reach the end desination that is displaying the data. It send packets while you send your request that report back the current IP address of the machine that your data packet is on and then reports back to your machine and displays the information in front of you.