ITP 125 - Lab 03

Deadline

1 minute before the next scheduled lecture.

Objective

Learn to work with layers the networking layers in the OSI model.

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.

* Open a command prompt in Windows by doing the following:  
    
  Right click the key on the *Desktop* and select *Command Prompt (Admin)*
* When a command prompt opens type the following command:  
    
  > ipconfig /all  
    
  This command displays all the network configuration settings on the computer.   
    
  For your lab, your network settings are under “Local Area Connection 2”, you may need to scroll up to find it.  
    
  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 2”, the lab is setup in a way that you will see a 192.168.1.\* address. So look for the network configuration with that address.

**OSX:** In order to pull the same command on OSX/\*nix you need to run the following in terminal. You can find Terminal in Applications Utilities Terminal

*# ifconfig –a*

* 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 the gateway/router. In the command prompt type the following:  
    
  > ping 192.168.1.1  
    
  Second, test the connection between your computer and a server on the Internet. In the command prompt type the following:  
    
  > ping [www.usc.edu](http://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.
* One interesting way to see all the computers/routers between you and a server is using the traceroute command. In the command prompt, type the following.  
    
  > tracert [www.google.com](http://www.google.com/)  
    
  **Note:** This takes advantage of the IP TTL field.

**OSX:** Type in the following command instead:

# traceroute [www.google.com](http://www.google.com/)

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

**OSX:** No changes

* Using the procedure from step 2, get the MAC address of the network card with the 192.168.1.## address. The MAC address is called Physical Address in Windows  
    
  Goto 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.
* 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.
* 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](http://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

* 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?   
    
  Hint: Google search it.  
    
  Note: This attack doesn’t work on new systems. Only really old ones.

A ping packet is usually 56 bytes in size (exlcuding the header), however in the IPv4 protocol, a packet can be as large as 65,535 bytes is size. A Ping of Death is a packet with the size of 65,535 in size, however disguised as a ping packet. When the destination computer tries to unpack the Ping of Death packet, it will cause a buffer overflow due to the unexpected size and cause the system to crash

* 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.

Let's say you have a map, and the map shows you how to get to the places you want. When you ARP spoof, you're redrawing the map so that the path to get to your destination is changed to get to a destination you didn't know about. This allows the person using the map to end up in dangerous places without them knowing that they are going to these dangerous places.

What can be done to prevent it?

Well you can always type the actual IP address instead of the we address, but that's rather silly. We can always encrypt our file, or just be careful no one every touches our computer to change our ARP file.

Hint: Wikipedia is your friend.

* 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?

If someone is able to alter the DNS database of a particular router (or anywhere) and change the dictionary of DNS to IP addresses, they can effectively create an ARP spoof without even accessing someone's computer physically or via hacking and also affect a larger number of people in one go.

What can be done to prevent this attack?

Have higher security for DNS databases or make the DNS entries immutable.

Hint: See questions 1 and 2 hints.

* 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.

Ping Packet: Layer 3 (IP Address), Layer 4 (transport protocol), Layer 5 (establish session)

Trace Routing: Layer 3(IP Address), Layer 4(transport protocol), Layer 5(establish session)

MAC Addresses: Layer 2

IP Addresses: Layer 3

ipconfig: Layer 1 (looking at the physical connections)

DNS: Layer 3 (routing packets via DNS lookups)

ARP: Layer 6 & 7 (resolution of a name to an address)

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.

* 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?

TTL stands for "Time To Live", essentially if a packet exceeds this TTL value on its way to its destination, it will kill itself and disappear. This avoid the problem of having packets get really congested in a network if it keeps getting re-routed forever without ever reaching its destination.

FAQ

* **Question:** I have no idea what I'm doing.

**Answer:** Before you leave the class make sure you take with the TA, Instructor, or fellow students for help. Do not leave the room before you understand what is going on. You can always use the power of Google/Yahoo/Bing to figure it out.

* **Question:** How do I prove that I did the course?

**Answer:** That’s up to you to figure out. There are some obvious ways.

* **Question:** I uploaded the files, but they don’t show up on the website.

**Answer:** Looks like a permission issue again, refer to lab 01 to see how to fix that. You’ll need to SSH into aludra to fix it.

Submission

After you are done with Code Academy, name the file **lab03.docx,** then encrypt the file using **7zip or Keka**, and. Upload the file to your **itp125 folder** on the web hosting.

Set the password to the all the files to be: **dialupkid**

Make sure you can see the file by publicly accessing the URL using any web browser of your choosing.