ITP 125 - Lab 04

Deadline

1 minute before the next scheduled lecture.

Objective

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

Learn a bit more about TCP and network commands available on Windows

Procedure

Now before we can practice the steps below in the lab, we need to startup the Windows 8.1 virtual machine. You should see an icon on the desktop saying Win 8.1 or something similar. Double click on that and work within the virtual machine.

1. Open a command prompt in Windows by doing the following:  
     
   Press key 🡪 “Search Programs and files” 🡪 type in: cmd.exe

**OSX:** In order to do something similar you need to open up Terminal from the following location Applications 🡪 Utilities 🡪 Terminal

1. When a command prompts opens type the following command:  
     
   > netstat -aon  
     
   This command will show you all the ports that the operating system is currently using. This is a great way to see if anything is opening a connection to the network that you’re not familiar with.

**OSX:** No changes

1. Open a web browser and check out a video on Youtube. Rereun step 2, and see if you can see connection being made to Youtube.
2. Let’s change the TTL settings for TCP in Windows.  
     
   Press key 🡪 “Search Programs and files” 🡪 type in: regedit  
     
   In the left panel of the windows, open the following folders:  
     
   HKEY\_LOCAL\_MACHINE 🡪  
   System 🡪  
   CurrentControlSet 🡪  
   Services 🡪  
   Tcpip 🡪  
   Parameters 🡪  
     
   Right click on the Parameters folder and select: New 🡪 DWORD (32-bit Value)  
     
   Name the new key the following: DefaultTTL  
     
   Double click on the new key: and type the following:  
     
   Value Date: 64  
   Base: Decimal  
     
   Open up a command prompt, and “ping 127.0.0.1”. Note the TTL that the commands says.  
     
   Reboot the machine, and redo a ping. See if you notice a change in the TTL.  
     
   If you ping different servers you can find their TTL values. With these values, you can guess the operating system the machine is running on.  
     
   If you want to play a dirty trick, try to change the TTL to 1 and see if you can access the Internet.

**OSX:** In order to change the network settings you need to open up Terminal and run the following commands:

*# sudo sysctl net.inet.ip.ttl=1*

It will ask you for the password of the account (assuming you have administrative rights). Remember that the default TTL value of OSX is 64. You can easily reverse this process.

Questions

1. Watch the video:  
     
   <http://youtu.be/PBWhzz_Gn10?hd=1>  
     
   Did this help in your understanding of the Internet and networking? Explain.

**Well I’ve studied networking before, so it was mostly review for me**

Would you recommend this video to someone who doesn’t understand computer networking?

**I guess this is a good video for someone who has no knowledge of computer science or of any tech background, however I would have preferred something more succinct and clean**

1. Using step 2 from this lab, you were able to see the ports that were opened for your computer. Open a browser to Hulu and start a video. Run netstat again and see if you can see what protocol Hulu is using to send you the video (TCP or UDP). Does it make sense to you why they are using this protocol?

**Yes, since Hulu would want seamless video streaming, they’ll want UDP, the occasional wrong packet containing a pixel is too hard for the human eye to detect, so it’s worth the tradeoff**

In addition, notice the port number that is opened. Is it a well-known, registered, or dynamic port? Who assigned the ports, and does it make sense why it assigned the port number?

**I don’t have a Hulu account, so I’m going to guess Registered since they are an established company and will need their packets on this port type.**

1. In step 5, we were able to play with the TCP settings to make it impossible for the computer to access the Internet. Check out the following link:  
     
   <http://support.microsoft.com/kb/314053>  
     
   Look for the information regarding “TcpWindowSize”. If you were to play a joke on a friend’s computer, what values would you set this key to be?

**You can set the window size to 0 so no packets can be transferred. That might be an invalid value, so setting it to 1 can cause all connection speeds to slow down**

Does it really change anything when you change the window size on the computer?

**Do you mean the computer communicating within itself? If so, then no, since the communication is almost instantaneous.**

1. When you ran the netstat command in step 2, you will notice there were some ports that were opened/listening that you didn't interact with.  
     
   As a person wanting to learn more about security, the first thing is to question everything. So look up what programs are associated with these ports, and why should they be running? Use “the Google”, and look up what these ports are for.

**TCP Port 135: Remote procedure call, a port for other computers to control this one  
TCP Port 445: Allows access without the need for a NetBIOS layer, letting the outside direct access into your hardware  
TCP Port 5357: Used for Microsoft Network Discovery, allows you to see other connections from other devices**

**These are usually blocked by a firewall.**

1. Review the slides from lecture. Do the conversion and fill in the following table:

|  |  |  |
| --- | --- | --- |
| **Decimal** | **Binary** | **Hex** |
| 161 | 1010 0001 | A1 |
| 47258 | 1011 1000 1001 1010 | B8 9A |
| 232 | 1110 1000 | E8 |
| 15 | 1111 | F |

You may use a calculator to add up the base 2 values. If you want to get some good practice try this by hand. May also use the calculator to verify your answers.

FAQ

1. **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.

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

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

1. **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 **lab04.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: **00100100**

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