**CPS3498 Computers Security**

**Lab 2: Network Configuration and Connectivity**

**Description:**

This lab introduces some basic commands and tools that enable you to manipulate and monitor the network setting on a computer. You will need these skills later to perform functions that are necessary to secure a network from attacks. Note that you may encounter difficulty in observing some data if you are not performing the lab procedures on campus.

**Procedure:**

**Lab 2.1 Name Resolution in Windows**

**Lab A localhost**

1. Long on to a Windows PC with the administrator account, or an account that has administrator privilege.
2. Open the command prompt. For Windows XP, choose Start 🡪 Run, and type **cmd** in the Open field. For Windows 7, click on Start, enter **cmd** in “Search program and file, and choose “cmd.exe” from search result. For Windows 8, press “Start” key on your keyboard and type **cmd** (ignore the GUI menu on screen). For Mac OS, open “Finder,” select “applications,” choose “utilites,” and double click “Terminal.”
3. At the command prompt
   * Type **ipconfig /all** (**ifconfig -a** For Mac OS) and press Enter. Note the result.
   * Type **ping 127.0.0.1** (for local loopback address) and press ENTER. Observe the information displayed.
4. At the command prompt type **ping localhost** and press ENTER. Observe the information displayed. How does the computer know that localhost defaults to 127.0.0.1?
5. For Windows XP, choose Start 🡪 Run, and type **notepad c:\windows\system32\drivers\etc\hosts** in the Open field. For Windows 7, click on Start, enter **notepad c:\windows\system32\drivers\etc\hosts** in “Search program and file, and choose it from search result. For Windows 8, press “Start” key on your keyboard and type **notepad c:\windows\system32\drivers\etc\hosts**. For Mac OS, type **sudo nano /private/etc/hosts**.
   * Observe the information displayed. What entries are already there?
   * Why are there some instructions commented out?
6. Add the following lines to the end of the host file:

xxx.xxx.xxx.xxx winserv (where xxx.xxx.xxx.xxx is the IP address of your Default Gateway)

yyy.yyy.yyy.yyy me (where yyy.yyy.yyy.yyy is the IP address of your computer)

1. Click on File 🡪 Save and close Notepad.
2. At the command prompt type **ping me** and press ENTER. Observe the information displayed.
3. At the command prompt type **ping winserv** and press ENTER. Observe the information displayed.
4. Can you think of a way that this file could be exploited without administrator privilege?
5. To show to contents of the DNS cache, at the command prompt type **ipconfig /displaydns** and press ENTER. For Mac OS, type **sudo killall –INFO mDNSResponder**. The summary of DNS internal state is in **/var/log/system.log**

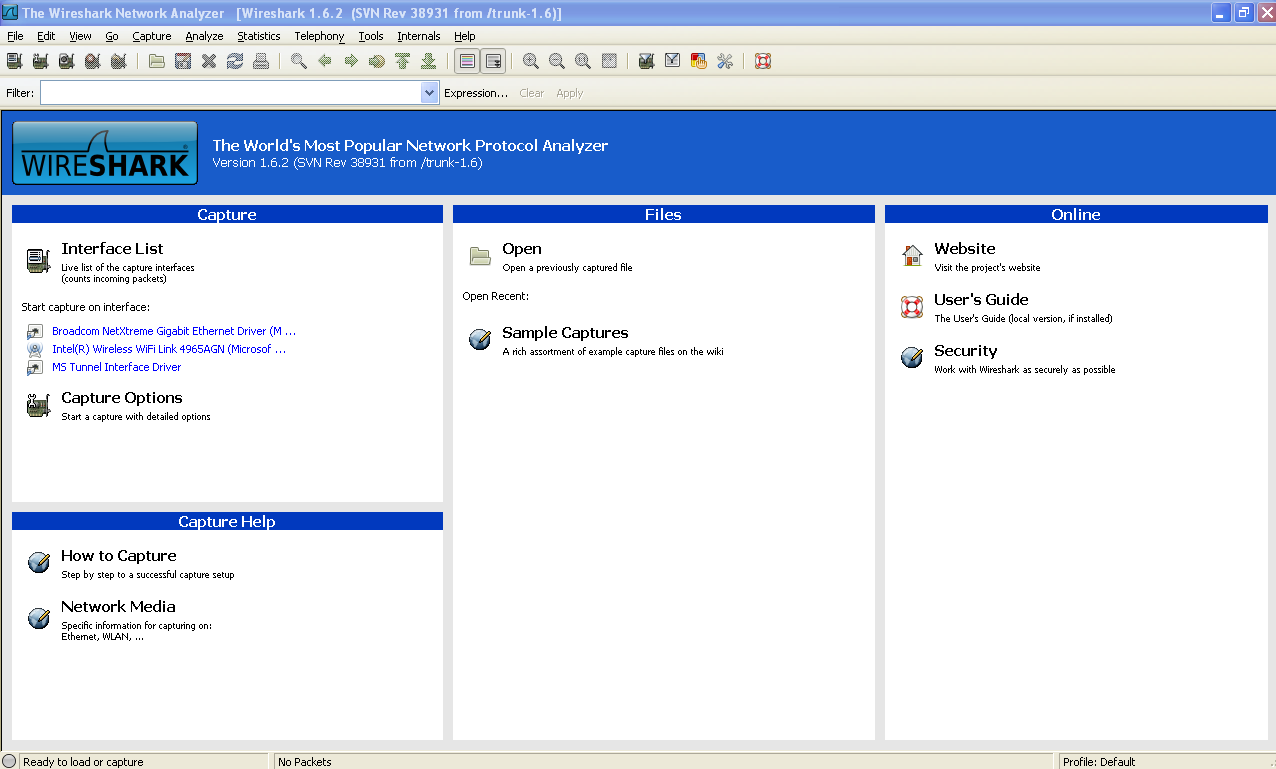
**Lab B nslookup and netstat**

1. At the command prompt type **nslookup** and press ENTER. For Mac OS, type **man** **nslookup.**
   * At the command prompt type **help** and press ENTER. Which option displays the current server/host?
   * At the command prompt type **exit** and press ENTER.
2. At the command prompt type **netstat/?** and press ENTER. For Mac OS, type **man** **netstate.**
   * What is the function of the command?
   * How can you tell (with what option) a process running on your computer creates a network connection?
3. At the command prompt type **netstat** and press ENTER. For Mac OS, type **sudo lsofc -np|grep TCP.** How many active connections you have? What are those?

**Lab 2.2 Windows IPv6 Basics**

**Lab A netsh command and wireshark tool**

1. IPv6 is already installed in Windows 7/8/10. For Windows XP, if there is no IPv6 setting, at the command prompt type **netsh interface ipv6 install** and press ENTER. **Netsh** is not a CLI command in Mac OS, skip this step for Mac.
2. At the command prompt type **netsh interface ipv6 show address** and press ENTER. Record the IPv6 address for Local Area Connection (or Wireless Network Connection if you are using WiFi). For Mac OS, type **ifconig –a.** Record the IP address and types.



1. Install **Wireshark** (<http://www.kean.edu/~jliou/resources.htm>) onto your computer. Start the wireshark. If it doesn’t start, you may have to install **WinPcap** first. For Mac OS, download an equivalent version from the Internet.
2. Within wireshark, click on Capture 🡪 Interfaces, and click on Start for the correct interface that has the corresponding IP address from previous step.
3. At the command prompt type **ping6 [IPv6 address of your computer]%4** and press ENTER. For Win7/8, use **ping -6 [IPv6 address of your computer]%4**. The IP address would look similar to fe80::20c:70ff:feb7:7dd9. Also, 4 isthe interface # as you saw in your ipv6 during ipconfig, use the correct number in the place of 4.
4. At the command prompt type **netsh interface ipv6 set address 4 2001:db8:1234:5678::2 (**use the correct interface number in the place of 4 or **netsh interface ipv6 set address “wireless network connection” 2001:db8:1234:5678::2)** and press ENTER.
5. Verify the address by typing **netsh interface ipv6 show address** and press ENTER. For Mac OS, type **ifconig –a.** Record the IP address and types.
6. You can verify the IPv6 ping by viewing the wireshark output. You can filter the results to show the IPv6 related traffic by specifying ipv6 in the filter field on top just below menu and clicking Apply.
7. At the command prompt type **netsh interface ipv6 reset** and press ENTER.

**Notes and Suggestions:**

* Different computers may have different operating systems and hardware configurations. If you use your own computer for this lab, the above procedure may not be completely applicable. For example, you cannot follow the same procedure for MAC computer.
* Make sure that the computer is back to its original condition. Do not leave a computer in a non-functioning condition.

**Lab report:**

* Your report should include all information required to be noted in the procedure, any problems/issues you encountered during the lab and how did you resolve them.