**CPS3498 Computers Security**

**Lab 1: Identity and Security**

**Description:**

In order for two computers to communicate in a TCP/IP network, both computers must have a unique Internet Protocol (IP) address. The IP address is divided into a network address and a host address. The subnet mask identifies which portion of the IP address is the network address and which portion is the host address. On a local area network (LAN), each computer must have the same network address and a different host address. When communicating between computers on different networks, packets are sent via the default gateway on the way into and out of the LAN. The routing is done using (layer 3) IP address. If the computers are on the same network, then the IP address gets resolved to a (layer 2) Media Access Control (MAC) address. MAC addresses are hard coded onto a network card by the manufacture.

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 1 Windows Client Configuration**

**Lab A ipconfig (IP Configuration)**

1. Long on to a PC with the administrator account, or an account that has ***administrator privilege***. Please take a note of your system information and location where you perform the lab.
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 /?** (use **man** **ifconfig** For Unix/Linux and Mac OS) and press Enter.
   * Observe the options available for ipconfig.
   * Which options do you think would be most useful for an administrator?
   * Which option would you use to obtain an IP configuration from a Dynamic Host Configuration Protocol (DHCP) server?
4. Type **ipconfig** (use **man** **ifconfig** For Mac OS) and press Enter.
   * What is your IP address?
   * What is your subnet mask? What is the purpose of an IP address mask?
5. Type **ipconfig /all** (**ifconfig -a** For Mac OS) and press Enter.
   * Observe the new information shown on screen
   * What is the MAC address of your computer?
   * What is your DNS server address? (For Mac OS, **ifconfig -a** does not provide this information. How do you get such information?)
6. To access the Local Area Connection Properties dialog box in Windows XP, click on Start 🡪 Control Panel 🡪 Network and Internet Connections 🡪 Network Connections 🡪 Local Area Connection. For Windows 7/8, click on Start 🡪 Control Panel 🡪 Network and Internet 🡪 Network and Sharing Center 🡪 Change Adaptor Setting (on the left panel). For Mac OS 9.X and higher, click on the Apple Menu, select Control Panels, and then click TCP/IP.
   * For Windows XP, in the Local Area Connection Status window, click Properties.
   * For Windows 7, double click on Local Area Connection. For Windows 8, double click on Ethernet.
   * For Windows XP, select Internet Protocol (TCP/IP) and click Properties. For Windows 7/8, select either Internet Protocol 4 (TCP/IPv4) or Internet Protocol 6 (TCP/IPv6) and click Properties.
7. Record the IP address information shown in the IP address text box and compare it with the IP address you recorded at step 4. If you connect your computer through an ISP, such as Verizon or Optimum Online, you may see “Obtain an IP address automatically.”
8. If IP address is shown in Properties window, change the last octet to 110 and click on OK. Click on OK or close the Local Area Connection windows. . If it doesn’t allow you to save, record the result and explain why. If you are able to save the change,
   * Repeat steps 2-4 to observe that your IP address has changed.
   * Repeat steps 6-10 to change the last octet from 110 back to its original value you recorded in step 4 (or 9).

**Lab B ping (Packet Internet Groper) and tracert (Trace Route)**

1. Repeat step 2 in Lab A, and type **ping /?** And press ENTER to view the ping help file.
2. To ping the connected Server, at the command prompt, type **ping** xxx.xxx.xxx.xxx. Note that the xxx.xxx.xxx.xxx is the **IP address of Default Gateway** you recorded at step 4 and Preferred DNS server at step 9.
   * Observe the information shown. What is the time value observed for all four replied?
   * What is the TTL (Time To Live) value? What does this number refer to?
3. How can you be sure that this response is actually coming from the correct computer?
4. To ping not only the connected Server but also the intermediate nodes, at the command prompt, type **tracert** xxx.xxx.xxx.xxx (use **traceroute** in Mac OS). Note that the xxx.xxx.xxx.xxx is the URL or IP address of the targeted server. Here, we will ” “tracert www.kean.edu.”
   * Observe the information shown. How many actual intermediate hops?
   * Which intermediate node takes the longest time?
   * Repeat step 4 four more times. Comparing the routes, do you see any difference in the intermediate nodes? If yes, can you think of any reason why that happens?
   * Using the intermediate notes in the 5 routes to draw the network topology.
5. Repeatstep 4 by “tracert www.google.com.”
   * Observe the information shown. How many actual intermediate hops?
   * Which intermediate node takes the longest time?
   * Repeat step 4 four more times, using the intermediate notes in the 5 routes to draw the network topology.

**Lab C ARP (Address Resolving Protocol)**

1. At the command prompt type **arp /?** and press ENTER. Observe the options for this command. Which option displays the current ARP entries?
2. At the command prompt type **arp -a** and press ENTER. Note that the MAC address for the Windows Server is listed.
3. At the command prompt type **arp -d** and press ENTER. For Mac OS, type **sudo** **arp –d [IP address]**.This –d option deletes the ARP cache. If you get the message “The ARP entry deletion failed: The requested operation requires elevation,” close command prompt and do:
   * 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). And then press CTRL+SHIFT+ENTER.
   * If the **User Account Control** dialog box appears, confirm that the action it displays is what you want, and then click **Continue.**
   * Retype **arp -d** and press ENTER..
4. Repeat step 2. The ARP cache should have no entries now.
5. Repeat step 2 in Lab B.
6. Repeat step 2. Note that the MAC address is once again listed.

**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.