Southern Polytechnic State University

Electrical and Computer Engineering Technology Program

ECET 4820 Laboratory Exercise: TCP/UDP Ports

Objective:

The student will use telnet to access TCP/UDP ports, examine some features of TCP using a network protocol analyzer, and learn the basic operation of a port scanner.

Overview:

The TCP and UDP transport protocols use ports as "doors" through which clients and servers exchange information between applications using particular protocols. The telnet protocol normally operates through TCP port 23. You will use telnet to interact with ports designated to operate with other TCP protocols, such as HTTP. You will also use the Wireshark network protocol analyzer to examine some of the network traffic. Finally, you will use the NMap port scanner tool to test for open ports on computers in the lab.

Procedure:

You will document your results in the telnet portions of the exercise using a log file and/or screen captures. Logging stores all of your input as well as the responses from the server in a log file. If you want, you can use screen captures to store this information. Screen captures are bitmap "snapshots" of the *active* window. Each screen capture is initiated by pressing Alt and Prt ScrUse the Wordpad application to paste the screen captures.

Boot Your Workstation

1. Boot your workstation to Windows and log on with the user name and password given by your instructor. Use the user name and password given by your instructor.

Start the Network Analyzer

2. Start the Wireshark network analyzer. In the following sections you will be asked to examine some of the frames entering and leaving your workstation. This will require you to set appropriate capture filters.

Using Telnet to Access (and Fingerprint) Web Pages

3. You will download a web page header using the HTTP HEAD commands through telnet. A telnet client connects to a server through port 23 by default, but you can initiate a telnet session to another port as well. You will attempt to "fingerprint" a couple of web servers by using telnet to issue the HEAD command to the server. If all goes well, the server will download the header of its html landing page, which will include some information of interest. You will try this with the www.yahoo.com, www.earthlink.com, www.spsu.edu, and www.google.com servers.

   Important: you must enter the commands carefully and exactly as shown for everything to work.

   a) Start a new capture session using an appropriate filter.

   b) Open a **command prompt** window.

   .

c) At the prompt type the command **telnet www.yahoo.com 80** followed by a return**.**. Here you are asking telnet to open port 80 on the Yahoo server.

The server will respond by blanking the command window. ***This is normal***. It is now ready for you to type the following command. It will not echo the letters you type. You will have to type **Enter *twice*** to execute the command, so you must be careful. Note in the command below that there is a space after "D" and after the first "/" but nowhere else. The letters are capitalized, so you can use **Caps Lock**.

HEAD / HTTP/1.0

Fig. 1 shows you the response obtained by the instructor.

When you execute the command, save the response for future analysis.

d) Stop your capture and answer the following questions by examining the captured frames.

- Do you see the connection establishment exchange between source and destination?
- Do you see frames containing the downloaded web page information?

Make a screen capture or printout of the capture buffer illustrating the connection establishment.

Have your instructor verify your results.

e) Repeat the command with www.earthlink.net, www.spsu.edu, and www.google.com. Note the responses. You do not have to repeat the Wireshark captures for these.

Note: the web server may not respond with a prompt or message. Just wait about 20 seconds before completing the next step.

```
HTTP/1.1 200 OK
Date: Sun, 28 Sep 2008 23:39:52 GMT
P3P: policyref="http://info.yahoo.com/w3c/p3p.xml", CP="CAO DSP
COR CUR ADM DEV TAI PSA PS
D IVAi IVDi CONi TELo OTPi OUR DELi SAMi OTRi UNRi PUBi IND PHY
ONL UNI PUR FIN COM NAV IN
T DEM CNT STA POL HEA PRE LOC GOV"
Cache-Control: private
Vary: User-Agent
X-XRDS-Location:
http://open.login.yahooapis.com/openid20/www.yahoo.com/xrds
Last-Modified: Sun, 28 Sep 2008 23:27:33 GMT
Accept-Ranges: bytes
Content-Length: 9554
Connection: close
Content-Type: text/html; charset=utf-8



Connection to host lost.
```

Fig. 1 Response by the Yahoo web server to the HEAD command.

Use Telnet to Download a Computer's Time of Day Clock (Optional)

4. You will access another computer to retrieve its date and time information.
   a) Determine the TCP/UDP port for the time of day or daytime.
   b) Telnet to your neighbor's computer using this port number. Try again with the same web servers from step 3.
   c) Print out the log file or screen captures documenting your work.

Using the NMap Port Scanner

5. NMap is a network diagnostic tool that allows the user to determine, among other things, listening TCP ports on remote hosts. It can use using different techniques to find the open (listening) ports and it can attempt to identify the operating system on the remote host. Network managers can use NMap to see if servers and other hosts have open ports that should not be because they can be exploited by hackers. You will perform a port scan on your neighbor's computer and a server in the lab. Zenmap is the graphical user interface version of NMap. You can use either here.

   Important: ***Do not*** scan a host outside the lab.

   a) **Important: ask the instructor to disconnect the lab from the campus network**.
   b) When NMap boots, enter the following command in the **Command** box:

      nmap –sV –sS –O *address*

      Where *address* is the IP address of your neighbor's computer. This is a TCP SYN scan with operating system detection and services detection. Note that you can also build a command using the **Command Wizard**. Do not start the scan yet.
   c) Start a Wireshark scan and then click the **Scan** button to start the scan. It will take several minutes, depending on the number of tasks to be performed. When NMap finishes the scan, stop the Wireshark capture.
      - Which ports were open?
      - What functions are the open ports associated with?
      - Which operating system does the scanned host use?
   d) Use a Wireshark display filter to specify a TCP port (source or destination) corresponding to one of the open ports discovered by NMap. This will eliminate most of the packets from the display.
      - From the Wireshark display, how do you know that the port is open?
   e) If the scanned computer had a running firewall, disable it and repeat the scan. Look for differences in the results. You do not need to run a Wireshark capture.
   e) Perform the same scan the server computer designated by your instructor. Which machine had more open ports? You do not need to run a Wireshark capture.
   f) Use the help feature of NMap to determine what the scan command options specified in parts (b), do. Also, use help to find out what a TCP ping is.

Using the NMap Port Scanner to Test a Guest Virtual Operating System (Optional)

6. In this step, you will use NMap in the Windows XP host operating system to scan the guest Ubuntu Linux operating system for open ports.

a. Start Oracle VirtualBox.
b. Start the Ubuntu Linux operating system from the VirtualBox window.
c. Once Ubuntu starts, click on the Devices drop down menu at the top of the Ubuntu window. Select **Network Adapters**. In the **Adapter 1** tab, make sure the **Attached to:** selection is **Bridged Adapter**. If it is not, change it.
d. In Ubuntu, open a terminal window and enter the **ifconfig** command. Check that the address is on the same IP network as the Windows Ethernet card. If it is not, in Ubuntu select **System→Preferences→Network Configuration** and choose either DHCP or enter an IP address manually. You will have to reboot Ubuntu to make the changes.
e. Test Ubuntu's network configuration by pinging the default gateway.
f. Now run NMap from Windows, issuing the same command as in step 5 (b) above. You do not need to run Wireshark in this case.
g. If NMap is installed in Ubuntu, scan the same computer's Windows IP address. Note that you will need to start NMap or Zenmap from the terminal window using the **sudo** command: **sudo Nmap**.

Questions:

1. When you executed the HEAD commands, did any of the servers respond with the server software used?
2. In general, how did the servers respond to the HEAD command? That is, did they respond with useful information?
3. When you accessed the daytime of another computer in step 4, is this the same port that is used by a computer to access Internet time using NTP?
4. Write a paragraph explaining the significance of TCP/UDP ports as they relate to Internet-based security. Cite any references. Internet references are OK.
5. Go to the www.insecure.org web site and find some documents describing NMap's operation. Write a short paragraph about the TCP SYN scan.

Report:

Discuss the results obtained in the lab exercise. Answer all questions. Make conclusions regarding your results.