CSC 436 Lab 1: Exploring TCP/IP

Name: Isha Rijal

1. I have set up an ftp server at 10.2.56.30. You will use this for the next few steps. Create a file in your current directory called *name*.txt (using your user name such as zappaf1) and in the file place your name.
   1. *How many files do you see in this directory?*

A screenshot of a computer

Description automatically generatedSix

* 1. Type **help** to view commands available. *Which commands are the same as Linux commands?*

Ls,cd,pwd,mkdir,rmdir,chmod,dir,quit,!,ascii,append,cd,chmod,cdup(used as cd ..),close,delete(used as rm),exit,get(used as wget),help,lcd(used as cd),status(used as top)

A screenshot of a computer

Description automatically generated

*Aside from these, list 5 other commands you feel you might use in an ftp session.*

quit,nmap, send ,passive,size

If you are unsure about any command, type **help *command*** where *command* is the name of the command, such as **status**. Type **exit** to leave ftp.

* 1. *What do you notice all of the FTP commands?*

They are in all caps letters and are no more that 4 letters and these commands are text based, they return a response with status code.

*Do you see any that are identical to those you saw when running help in ftp?* Yes ,(Size ,User,site stat ,syst)

A screen shot of a computer

Description automatically generated

* 1. Type **STAT**. This returns the status of your connection. *What does this display under the entries Connected to, Logged in as, and TYPE? What is the session timeout set to?*

*Connected to : ::ffff:10.2.60.105*

*Logged in as: Student*

*TYPE: ASCII*

*What is the session timeout set to? 300*

The last line of this output lists the service that 10.2.56.30 is running, *what is it called and what version number is it using?*

*A black screen with white text

Description automatically generatedvsFTPd version 3.0.5*

Another status-like command is **SYST**. Type this. *What does it respond with? What does SYST do?*

This command helps in querying the type of operating system running in the server.



* 1. Type **CWD pub**. Type **PWD**. *What response do you get?* It should be obvious what PWD does, but what about CWD? *What does it stand for and what does it do?*

A black background with white text

Description automatically generated

CWD changes directory on client computer, it stands for change working directory.

A screenshot of a computer

Description automatically generated *What do you see in your second window?*

I see the ls Command listing directory listed for the home directory of window 1

* 1. A screenshot of a computer

     Description automatically generatedIn your first window, type **MDTM *name*.txt** (where *name* is your username). *What response did you get?* Now type **SIZE *name*.txt**. *What response did you get?* Another Type **DELE *name*.txt** to delete your file. *What response are you given?*
  2. *Is your file listed in the second window?Yes*  If not, then you successfully deleted it.

A screenshot of a computer

Description automatically generated

* 1. Two other commands of use are **RETR** and **STOR**, both of which require the data channel. *What do each of these commands do?*

RETR command is used to retrieve or download a file from the FTP server to the local machine

The STOR command is used to store or upload a file from the local machine to the FTP server.

* 1. Three other commands of note are **CDUP**, **MKD** and **RMD**, none of which require the data channel. *What do each of these commands do? In general, when would an FTP command need the data channel and when would it not?*

CDUP command is used to change to the parent directory of the current working directory on the FTP server.

MKD command is used to create a new directory on the FTP server.

RMD command is used to remove a directory from the FTP server

The FTP command needs the data channel whenever command involves transferring of data and files but when the changes operate on directory structure we donot need the data channel.

* 1. *What headers are returned? What is the body of the html file?*
  2. A computer screen with white text

     Description automatically generatedA screenshot of a computer

     Description automatically generatedRedo the command from 2a but change GET to **HEAD**. *How does your response differ?*

The HEAD command does not print the html content instead displays just the header information.

* 1. A computer screen with white text

     Description automatically generatedRedo the command from 2a but change / to **/foo.html**. *How does your response differ?*

This response displays the content and header data of the file foo.html

* 1. A screen shot of a computer

     Description automatically generatedRedo the command from 2a, changing \r\n\r\n to \r\nRange: bytes=16-24\r\n\r\n. This version is a two-line HTTP command where the first line specifies the HTTP method (GET), URL and protocol while the second line specifies that we only want the server to return bytes 16-24 of the document.
  2. A screen shot of a computer

     Description automatically generated*What do both lines show (what information does the request have, what information does the reply have)?*

Both the lines have the request and response data, request has the IP version, server name , ip address, type, sequence number , identifier and length of the request . The ICMP packets normally consists of type, code and checksum.

* 1. The response code was 206. Look up this code, *what does it mean?*

*206 code means partial content response, in this response the server will only send the partial request based on what data the client wants.*

*What are the lengths of all four of these packets? Why do you suppose the returned packets (the ones with 200 and 206) are longer than the ones with the GET commands?*

A screenshot of a computer screen

Description automatically generated

All the four packets have different lengths: 18,46,26,38. The 200 and 204 packets have information of the such as last modified and E tags , acceptable ranges which has more meta data for their header.

* 1. *The two packets corresponding to the GET commands specify what value for IP?*

*What is the IP value for the two response packets (with 200 and 206)? What is the port listed for these?*

*Source Server’s IP :10.2.56.30.http*

*Destination IP: localhost.localdomain*

*Since 200 has the http response it runs in port 80 while gets the response from port 60390*

*And 206 has the http response in 59130*

* 1. *Provide the specific HTTP: message listed in each of these four captured packets.*

*The http massage listed for each packets GET /foo.html ,GET /HTTP/1.1*

* 1. Type **tcpdump -r dump | egrep 'FTP'**. *How many packets are there?*

There are 10 packets each packets associate with the steps taken from login and captured on the command line .

*What is the specific FTP: message in each?*

Each messages are the steps taken to for user to login, process for the passive session , system information command and logged out command all this run in the ftp session *.*

One packet has an FTP message of LIST. *What action does this correspond to from your ftp session?*

This corresponds to the action taken to print the contents of the current directory and returning the result over the data channel.

A screen shot of a computer

Description automatically generated

* 1. Type **tcpdump -r dump | egrep 'ARP'**. Most if not all of these packets are request who-has queries from your VM to your network gateway (router) asking who has a particular address. You will likely see a few different names listed among these ARP commands. *What is the most common name being sought?*

*My VM ‘s IP 192.168.1,1 to router 192.168.1.10*

A screenshot of a computer program

Description automatically generated

These messages generally are of the same length, *what is the length* (if there are multiple lengths, just answer the most common length). 46

Redo the command but add **-c** for egrep. *How many ARP packets are there in this file?* You may delete the dump file.

A screen shot of a computer code

Description automatically generated

1. 1. Type **wget 10.2.56.30**. This will download that server’s index.html file. Once done, make sure the file has download and then delete it. Type **curl 10.2.56.30**. *How do the two commands differ in terms of the results?*

A computer screen with white text

Description automatically generatedA screenshot of a computer

Description automatically generated Type **curl -o index.html 10.2.56.30**. *What output do you receive this time?* Type **ls**. You will see the file stored. Delete it.

Curl command simply showed the output of the file while wget downloaded the file to from the server and saved it to the local directory. Using the **curl -o index.html 10.2.56.30 command** showed the same output as wget command**.**

* 1. A screenshot of a computer

     Description automatically generatedRepeat the echo command from 2a and then repeat the most recent curl command from 4a except add **-v** before -o. The -v option tells curl to provide a *verbose* output. *How does the curl output differ from the echo | nc output?*

A screen shot of a computer

Description automatically generated

The curl command has lot more header meta data with the server’s information like User -agent, host and accept data.

* 1. The server at **10.2.56.30** has been configured for HTTPS and HTTP/2.0. Type **curl**

**-v --http2** **https://10.2.56.30**. Note that there is a single space after the option --http2 and before https. Without -o we are not saving the file, so instead the contents are displayed in the terminal window. Scroll up to find the beginning of the output. *What port was used to connect to the server? What was “offered”?*

80

A screenshot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generatedYou should notice a handshake that takes place between client and server. At the bottom of the output, you will be given a TLS alert. *What is the alert for?* Also at the bottom, you will find a message from curl reporting a problem. *What is the problem?*

The alert indicates the digital signature is a self- signed certificate and not trusted by default.

* 1. We can resolve this issue by adding **k.** Do so (with the **-v** option). This time it works. View curl’s man page. *What does the option -k do?*

A black screen with white text

Description automatically generated

* 1. As noted earlier, curl allows us to submit queries to servers in many different protocols, as opposed to wget which is limited to HTTP/HTTPS. View curl’s man page again. *What protocols are available?*



* 1. A computer screen with white text

     Description automatically generatedType **curl 10.2.56.30/page[1-2]\.html**. *What response did you get?* *Explain what this command does.* *How would you achieve the same downloads using wget?*

This command uses curl to download the files page1.html and page2.html from the server at 10.2.56.30. wget '10.2.56.30/page{1,2}.html

* 1. A computer screen shot of a computer code

     Description automatically generatedRepeat the curl command from 4f but use **[1-3]** instead of [1-2]. *How does the output differ? What can you infer from the output about the files stored on this web server?*

Since we got 404 page not found from the info we can infer that the page doesnot exist for the file in the server. The presence of page1.html and page2.html confirms that these files are stored on the server.

1. *Provide a brief summary about what each of these programs can do for you and when you might use each one.* 
   1. *netcat*

is used when you open network connections and communicate with other device in command line. We could use netcat to receive first 101 bytes of an HTTP response, we can also use this for testing connection, it could be used to store and retrieve the files from FTP server.

* 1. *tcpdump*

tcpdump is a command line tool that catches TCP datagrams and displays the information. Tcpdump could be used for troubleshooting, to display the datagram information and debugging in the issues.

* 1. *curl*

Curl is a command-line tool for transferring data to or from a server using various protocols (e.g., HTTP, HTTPS, FTP). It supports many features such as downloading or uploading files, sending HTTP requests, and handling authentication. Curl could be used in downloading files with URL, testing HTTPS requests and interacting with web APIs.

* 1. *wget*

wget is the non-interactive network downloader that downloads files from the web. It could be used to download the directories or large files from the web and also to resume interrupter downloads.

* 1. *ftp*

ftp is the internet file transfer program that allows user to transfer files to and from a remote network site .ftp could be used to access files from the remote server ,as if they were in the local machine, FTP can be used to back up files from a local system to a remote server, users can also list the files and directories on a remote server to view the file structure and contents.