FTP

Introduction and/or Background

Ftp is the user interface to the Internet standard File Transfer Protocol. The program allows a user to transfer files to and from a remote network site.

Command Usage

ftp [-pinegvd] [host] (port)

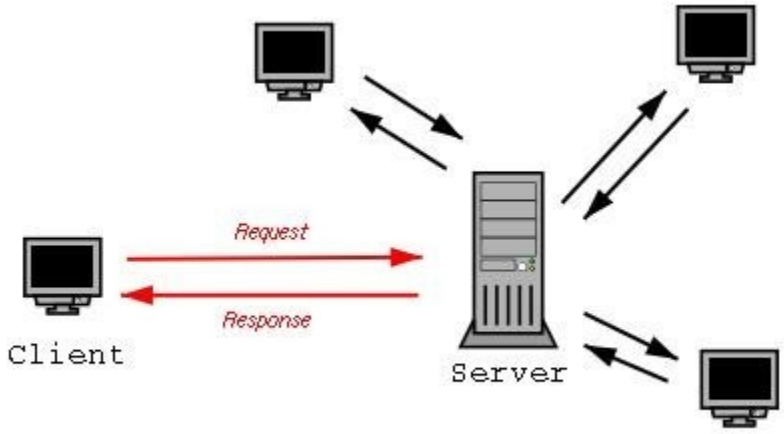
Where the format for the [host] is

<acct>@<address>

Port number is assumed 21 unless provided otherwise.

Concept

FTP was one of the early protocols that support a key component of networking – the client - server model.



The ftp client, a program on the PC, initiates a request. The server listening on a port accepts the request, processes it, and provides a response. For ftp in particular that means either an internal process change or sending or receiving a file.

Commands

A list of commands from the ftp client:

The more common ones are:

- put,mput – forward a file TO the server.
- get,mget – retrieve a file FROM the server.
- ascii – set to ascii text transfer mode.
- binary – set to binary file transfer mode.
- bye – exit the ftp program and close the connection.

Ascii/binary need some explaining. Computers use a carriage return and line feed to designate a new line for the next characters to print. Well back when 300bps was the norm sending 2 characters for each new line was a waste of bandwidth. So in ascii mode the server inserts the new line characters reducing the need to send them. Problem is what if it is a program? You don't want new line characters inserted willy-nilly. That is what binary mode is for. It just sends the file 'as-is'. These days just set your session at 'binary' and don't worry about it. We have bandwidth to burn in most cases.

Security

To be blunt, in the base protocol there IS NONE. It was designed in a time period that the word 'hacker' did not exist. (honest!)

- Logins and passwords are passed in the clear.
- The ftp server uses tools on the server for use by the protocol (eg: ls, cd, etc). That in the past has permitted hackers to gain access to the backend of the server.

Point two is one reason that one should not permit root account login to a ftp server.

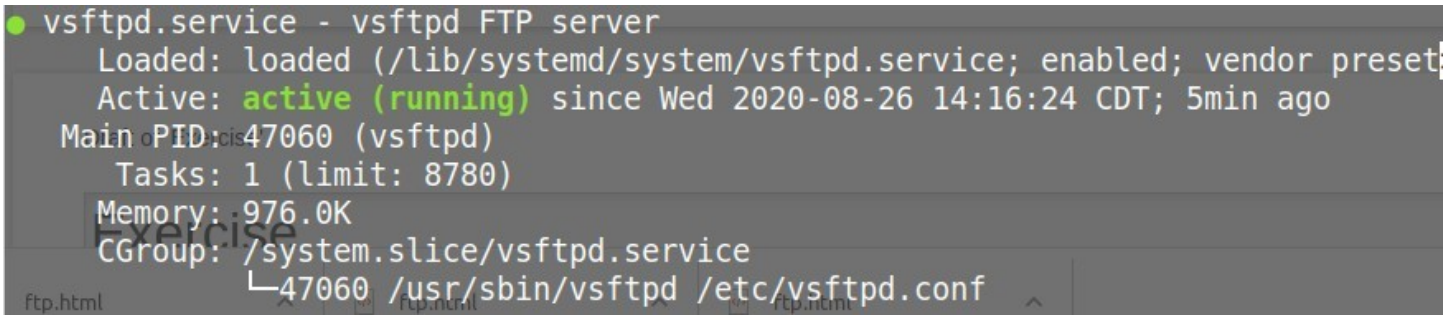
Default configurations for ftp exclude root user logins for that reason.

In an internal network one may not care about this lack of security. But it is certainly a problem once you wish to send data outside the network. Fortunately there are two support programs that solve that issue.

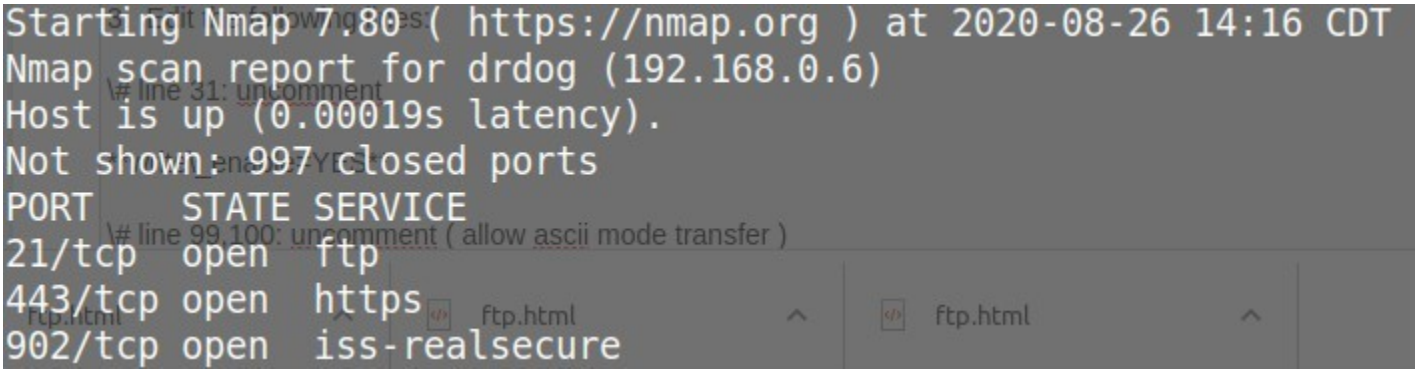
- sftp
- scp

Functionally they accomplish the same thing, send a file thru a secure tunnel to the ftp server. sftp provides a more robust command environment similar to the ftp command.

Service readout with ftp service active:



Nmap readout with ftp service active



Objectives

In this project/lab the student will:

- Gain familiarity with the FTP protocol

Equipment/Supplies Needed

- As specified in Lab 0.0.1.
- A VM image with Linux OS Installed as VMPC1
- A VM image with Linux OS Installed as VMSVR1

Procedure

Perform the steps in this lab in the order they are presented to you. Answer all questions and record the requested information. Use the Linux Virtual Machine to perform lab

activities as directed. Unless otherwise stated, all tasks done as a non-root user. If root access is needed use the sudo command.

Assignment

Install FTP daemon

1. On the VMSVR1 command line, Enter root user mode. The application VSFTP is to be installed.

   Execute:
   `apt search vsftp`

   An entry for vsftpd should appear.

2. Execute:

   `apt install vsftpd`

   Review the screen output and make sure there are no errors displayed.

3. Execute:

   `systemctl start vsftpd`
   `systemctl status vsftpd`

   You should receive a readout that the ftpd service is running.

4. You can validate that by executing:

   `nmap <VMSVR1 server ipaddress>`

   ftp should be listed as an active service
   Install is complete.

Configure FTP daemon

1. You should be at root user. If not, do so. cd to /etc subdirectory. Open vsftpd.conf with the editor of your choice.

2. Modify the following lines:
   - line 31: uncomment write_enable=YES
   - line 99 & 100: uncomment (allow ascii mode transfer), example - `ascii_upload_enable=YES`

ascii_download_enable=YES

- line 122: uncomment (enable chroot), example - chroot_local_user=YES
- Add - allow_writeable_chroot=YES pasv_enable=YES pasv_addr_resolve=YES

3 Save the modified file. Execute:

systemctl restart vsftpd
systemctl status vsftpd

You can validate by running the service routine again.

4 Create an account on the server:

su -
adduser <account name>

Add password and reconfirm when prompted.

Client access

1 On VMPC1, create a file.

2 touch myfile.txt

3 On VMPC1, open a terminal session. Enter ftp:

ftp <VMSVR1 ip address>
enter account id
enter password

If successful, you should see an ftp\> prompt.

4 Enter binary at the prompt.

Lets transfer the file to the server:

put myfile.txt

Enter:

ls

Take a screen shot of the terminal screen. Add that to your document.

5 As an independent exercise work thru the following commands:
- get
- ls
- cd

6. Exit from ftp:

bye

Reflection

1 When using the ls command in ftp which directory tree are displaying?
2 Do you understand the difference between an ascii transfer and a binary transfer?
3 Why is FTP 'out of the box' an insecure protocol?

Lab Submissions Proof: Provide screenshots as indicated in the lab; upload your proof to Canvas for grading.

Rubric

Checklist/Single Point Mastery

Concerns Working Towards Proficiency	Criteria Standards for This Competency	Accomplished Evidence of Mastering Competency
	Criteria #1:Recorded screenshot indicating the successful transfer (70 points)	
	Criteria #2: Provided correct answer to reflection question 1 (10 points)	
	Criteria #3: Provided correct answer to reflection question 2 (10 points)	
	Criteria #4: Provided correct answer to reflection question 3 (10 points)	