INDIAN INSTITUTE OF INFORMATION TECHNOLOGY KALYANI
Autonomous institution under MHRD, Govt. Of India
&
Department of Information Technology & Electronics, Govt. of West Bengal
WEBEL IT Park Campus (Near Buddha Park), Kalyani -741235, West Bengal
Tel: 033 2582 2240, Website: www.iiitkalyani.ac.in

Lab Assignment #05

Submit on or before 13/02/18

Weekly contact	**: 0 – 0 – 3 (L – T – P)**
Course No.	**: CS 612**
Course Title	**: Computer Networks**
Instructor-In-Charge	**: Dr. SK Hafizul Islam (hafi786@gmail.com)**

Aim

- To configure a machine as an FTP server and analysis the traffic created by the of FTP protocol using Wireshark.

Objectives

To learn how to setup a FTP server to host our own data for access from anywhere. Also to analyse FTP using Wirshark, one can look into flow graph (through Wireshark) to understand the working of FTP.

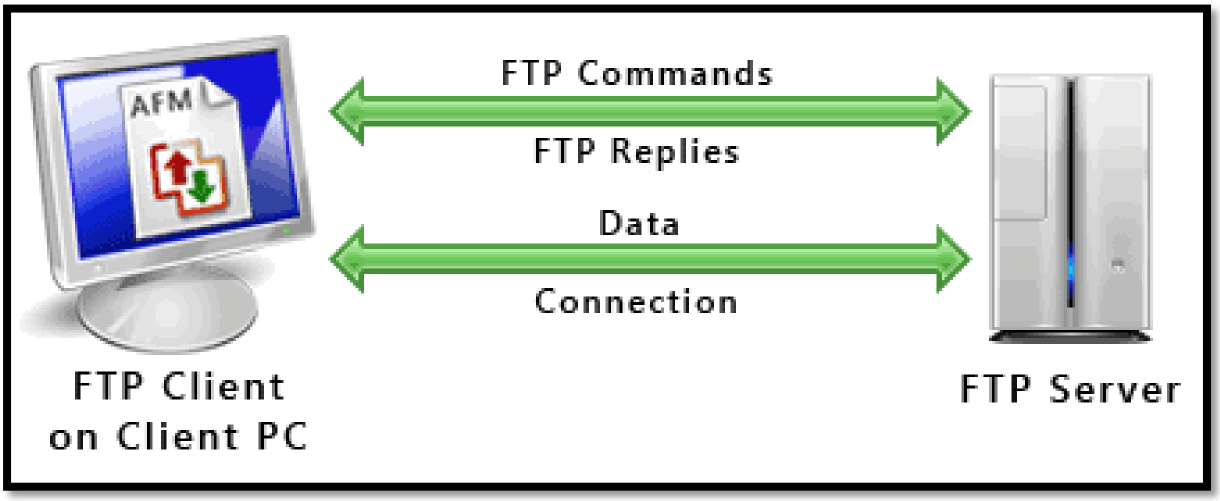
Description

File Transport Protocol, or FTP, is an open protocol standard that is widely used to transport and receive large files. It can also be used to send configuration files and software updates for network switches and routers. FTP uses ports for communications and also uses encryption to protect the information being received and sent.

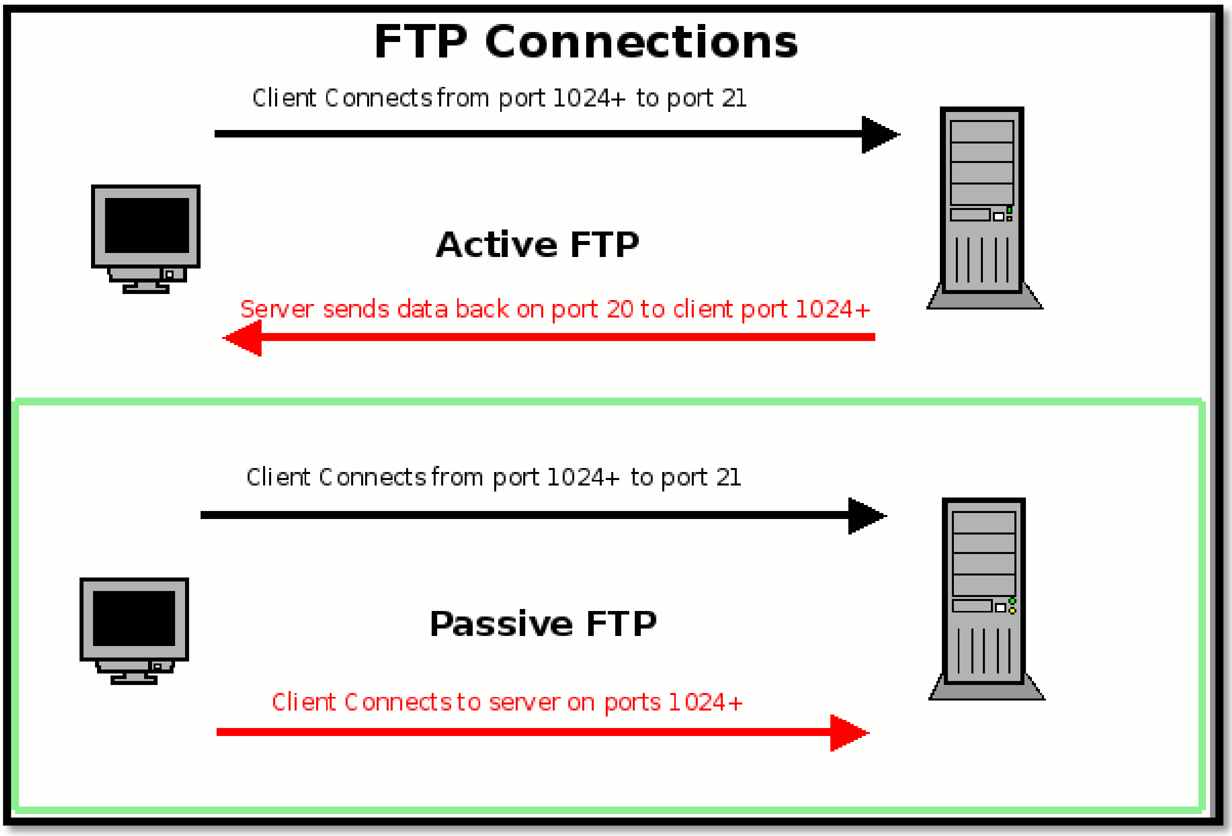
We will learn how to convert a Linux machine into an FTP server using Very Secure FTP Daemon (VSFTPD) package.

It operates in two connection channels:

- FTP Control Channel, TCP Port 21: All commands you send and the FTP server's responses to those commands will go over the control connection
- FTP Data Channel, TCP Port 20: This port is used for all subsequent data transfers between the client and server.



From a networking perspective, the two main types of FTP are active and passive. In active FTP, the FTP server initiates a data transfer connection back to the client. For passive FTP, the connection is initiated from the FTP client.


FTP Connections
Client Connects from port 1024+ to port 21
Active FTP
Server sends data back on port 20 to client port 1024+
Client Connects from port 1024+ to port 21
Passive FTP
Client Connects to server on ports 1024+

You can configure the server to use a different port number if desired; however, the client needs to know which port number so that its FTP request gets processed correctly.

FTP server installation

Step 1: Installing ftp

- *sudo –i*
- *apt-get install vsftpd*

Step 2: When the installation is complete, we'll copy the configuration file so we can start with a blank configuration, saving the original as a backup.

- *sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig*

Step 3: open configuration file and make following changes:

- *sudo -i*
- *gedit /etc/vsftpd.conf*

Enable/Disable anonymous access: VSFTPD runs as an anonymous FTP server. Anonymous FTP is the choice of Web sites that need to exchange files with numerous unknown remote users. Unlike regular FTP where you login with a preconfigured Linux username and password, anonymous FTP requires only a username of anonymous and your email address for the password.

- anonymous_enable = yes (for get file)
- anonymous_write_enable = yes (for put file)

Change the "local_enable" setting: You'll also need to simultaneously enable local users to be able to log in by removing the comment symbol (#) before the local_enable instruction.

- Change the "*local_enable*" to YES.

Restrict user access to FTP directory only: You may restrict local users to their home directories. You should uncomment this option keeping in mind security issues with open access to your other folders.

- *Change the "chroot_local_user" to YES*

Optional (for anonymous FTP access only): If you enable anonymous FTP with VSFTPD, remember to define the root directory that visitors will visit. This is done with the anon_root directive:

- anon_root=/data/directory

VSFTPD allows only anonymous FTP downloads to remote users, not uploads from them. This can be changed by modifying the ***anon_upload_enable*** directive.

SFTPD doesn't allow anonymous users to create directories on your FTP server. You can change this by modifying the ***anon_mkdir_write_enable*** directive.

SFTPD logs FTP access to the /var/log/vsftpd.log log file. You can change this by modifying the xferlog_file directive.

By default VSFTPD expects files for anonymous FTP to be placed in the /var/ftp directory. You can change this by modifying the anon_root directive.

There are many other options you can add to this file like limiting the maximum number of client connections (max_clients), maximum rate of data transfer per non-anonymous login. (local_max_rate). Descriptions on this and more can be found in the vsftpd.conf man pages:

- *sudo man vsftpd.conf*

VSFTPD only reads the contents of its vsftpd.conf configuration file only when it starts, so you'll have to restart VSFTPD each time you edit the file in order for the changes to take effect.

Step5: Restart VSFTPD for the configuration file changes to take effect

- *sudo service vsftpd restart*

Establish Connection from client

Step 1: ftp <ip address of server>

ftp 100.100.100.25

Step 2: Get or Put files

get <file name>
put <file name>

Note: After dong all the experiments, you must execute the following

sudo cp /etc/vsftpd.conf.orig /etc/vsftpd.conf

Assignment

In this example, anonymous FTP is not desired, but a group of trusted users need to have read only access to a directory for downloading files.

Step 1: Install and start a terminal for login as root.

- *sudo –i*
- *sudo apt-get install vsftpd*
- *sudo service vsftpd start (Start VSFTP).*

Step 2: open configuration file and make following changes:

- *sudo -i*
- *gedit /etc/vsftpd.conf*

To disable anonymous login and to enable local users login and give them write permissions:

# No anonymous login

- *anonymous_enable=NO*

#Let local users login. If you connect from the internet with local users, you should enable TLS/SSL/FTPS

- *local_enable=YES*

# Write permissions

- *write_enable=YES*

Step 3: Create a user group and shared directory. In this case, use */home/ftp-docs* and a user group name of ftp-users for the remote users:

- *groupadd ftp-users*
- *mkdir /home/ftp-docs*

Step 4: Make the directory accessible to the ftp-users group:

- *chmod 750 /home/ftp-docs* (7 (rwx) for owner, 5 (r-x) for group and 0 (- - -) for others)
- *chown root:ftp-users /home/ftp-docs*

Step 5: Add users, and make their default directory */home/ftp-docs*:

- *useradd -g ftp-users -d /home/ftp-docs user1*
- *useradd -g ftp-users -d /home/ftp-docs user2*
- *passwd user1 (You'll be prompted to enter and then retype a new UNIX password for the user)*
- *passwd user2*

Step 6: Copy files to be downloaded by your users into the /home/ftp-docs directory through the file explorer.

- nautilus /home/ftp-docs

Step 7: Change the permissions of the files in the /home/ftp-docs directory for read only access by the group:

- _chown root:ftp-users /home/ftp-docs/*_
- _chmod 740 /home/ftp-docs/*_

Step 8: Log off as the root when you are done configuring the FTP

- *logout*

Users should now be able to log in via FTP to the server using their new usernames and passwords.

If you absolutely don't want any FTP users to be able to write to any directory, then you should change the write_enable line in your vsftpd.conf file:

- *write_enable = NO*

Step 8: Restart VSFTPD for the configuration file changes to take effect

- *sudo service vsftpd restart*

Sample login session:

Step 1: ftp <ip address of server>

- *sudo –i*
- *ftp 100.100.100.25*

or

An FTP server can also be accessed in a user interface manner through a basic web browser by supplying ftp://<ip address of the FTP server> in the address bar

Analysis of FTP Protocol using Wireshark

Step: 1 Start a Wireshark capture

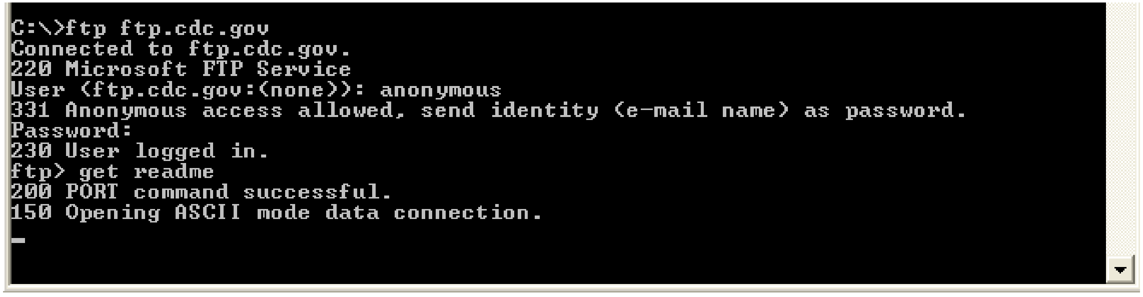
- *Close all unnecessary network traffic, such as the web browser, to limit the amount traffic during the Wireshark capture.*
- *Start the Wireshark capture.*

Step: 2 Download Files

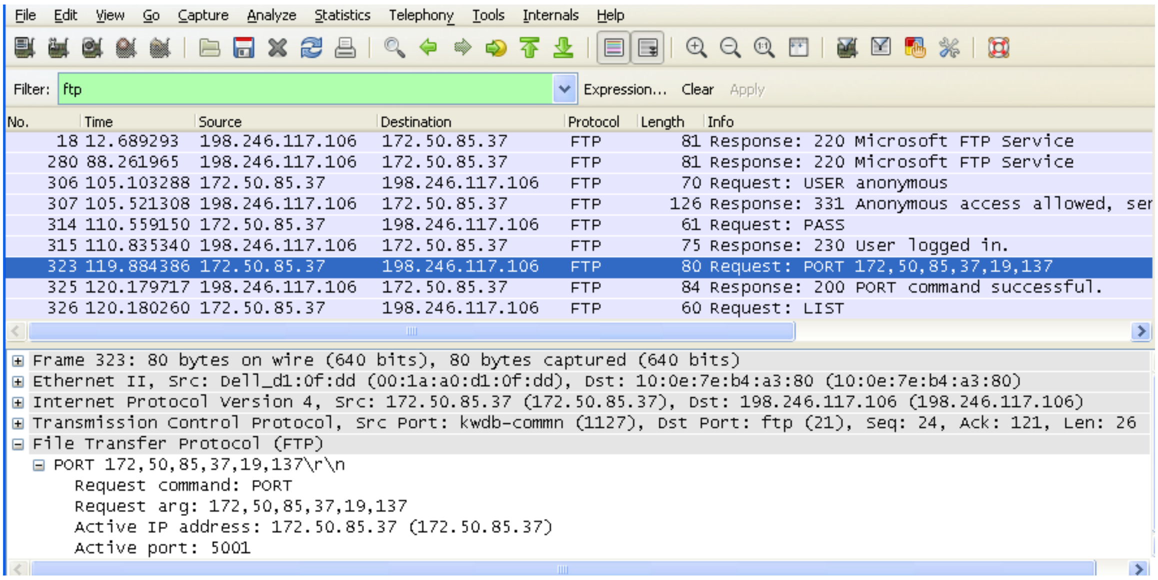
- *Download some file using your currently configured FTP server.*

or

- ***ftp ftp.cdc.gov***
- ***Log into the FTP site for Centres for Disease Control and Prevention (CDC) with username "anonymous" and no password.***
- ***Locate and download the Readme file.***



```
C:\>ftp ftp.cdc.gov
Connected to ftp.cdc.gov.
220 Microsoft FTP Service
User (ftp.cdc.gov:(none)): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
ftp> get readme
200 PORT command successful.
150 Opening ASCII mode data connection.
_
```



Filter: ftp

```
No.   Time       Source          Destination     Protocol  Length  Info
   18 12.689293  198.246.117.106 172.50.85.37    FTP           81 Response: 220 Microsoft FTP Service
  280 88.261965  198.246.117.106 172.50.85.37    FTP           81 Response: 220 Microsoft FTP Service
  306 105.103288 172.50.85.37    198.246.117.106 FTP           70 Request: USER anonymous
  307 105.521308 198.246.117.106 172.50.85.37    FTP          126 Response: 331 Anonymous access allowed, ser
  314 110.559150 172.50.85.37    198.246.117.106 FTP           61 Request: PASS
  315 110.835340 198.246.117.106 172.50.85.37    FTP           75 Response: 230 User logged in.
  323 119.884386 172.50.85.37    198.246.117.106 FTP           80 Request: PORT 172,50,85,37,19,137
  325 120.179717 198.246.117.106 172.50.85.37    FTP           84 Response: 200 PORT command successful.
  326 120.180260 172.50.85.37    198.246.117.106 FTP           60 Request: LIST
```

```
⊞ Frame 323: 80 bytes on wire (640 bits), 80 bytes captured (640 bits)
⊞ Ethernet II, Src: Dell_d1:0f:dd (00:1a:a0:d1:0f:dd), Dst: 10:0e:7e:b4:a3:80 (10:0e:7e:b4:a3:80)
⊞ Internet Protocol Version 4, Src: 172.50.85.37 (172.50.85.37), Dst: 198.246.117.106 (198.246.117.106)
⊞ Transmission Control Protocol, Src Port: kwdb-commn (1127), Dst Port: ftp (21), Seq: 24, Ack: 121, Len: 26
⊟ File Transfer Protocol (FTP)
  ⊟ PORT 172,50,85,37,19,137\r\n
      Request command: PORT
      Request arg: 172,50,85,37,19,137
      Active IP address: 172.50.85.37 (172.50.85.37)
      Active port: 5001
```

Step 3: Stop the Wireshark capture.

Step 4: View the Wireshark Main Window.

- *Wireshark captured many packets during the FTP session to ftp.cdc.gov. The IP address, 198.246.117.106, is the address for ftp.cdc.gov.*
- *You can see the various protocols working underneath FTP in Wirshark (ie TCP, IP etc), or go to Statistics →Protocol Hierarchy to find the same.*

Step 5: FTP Flow graph in Wireshark

- *Select a particular FTP stream.*
- *Go to Statistic Tab->Flow Graph*
- *You will get a window with options select the option given by default and press OK.*
- *You will get the FTP flow graph, analyse the FTP request response using flow graph*.

Reference

1) https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-16-04
2) https://help.ubuntu.com/lts/serverguide/ftp-server.html
3) http://vsftpd.beasts.org/vsftpd_conf.html
4) https://ubuntuforums.org/showthread.php?t=518293&p=3138955#post3138955
5) https://www.eukhost.com/blog/webhosting/how-to-give-ftp-users-with-only-read-access-to-a-shared-directory/
6) http://www.linuxhomenetworking.com/wiki/index.php/Quick_HOWTO_:_Ch15_:_Linux_FTP_Server_Setup#.WnqlOKiWbIU
7) https://www.centos.org/docs/5/html/Deployment_Guide-en-US/s1-ftp-vsftpd-conf.html