

CMSC 491/791 Active Cyber Defense HW 3

Name: Daniel Roh

Due: September 25, 2019 at 7:00pm

Summary:

In this lab you will install and configure a File Transport Protocol (FTP) server called vsftpd. The instructions assume you are using the Ubuntu 18.04 VM from lab 1, though any Linux distro is fine as long as you can complete the lab. Make sure to follow the directions very carefully!

Instructions:

Run the following command to install vsftpd:

```
sudo apt-get install vsftpd
```

- 1) **What is the PID of vsftpd? What command did you run to find this information? (8 pts)**
PID = 3982
Command: "ps -A"
- 2) **What port does vsftpd listen on? What command did you run to find this information? (8 pts)**
Port = 21
Command: "sudo lsof -i -P -n"
- 3) **What is the full path of the file that vsftpd logs to? (6 pts)**
Path = "/usr/sbin/vsftpd"

Now that we have installed vsftpd, we will configure it so that it is secure. First we will ensure that only a specific user (named ftpuser) can access it.

- 4) **Create a user named ftpuser. Make sure that they have a non-empty password. What command did you use to do this? What is ftpuser's UID? (8 pts)**
Command: "sudo adduser ftpuser"
UID = 1001

The ftpuser user is not expected to log in through a shell. They should only be able to access the system via ftp. You can do this by editing the ftpuser entry in /etc/passwd.

5) What did you change to prevent ftpuser from logging in via a shell? (8 pts)

I changed "bin/bash/" to "/sbin/nologon"

By default, vsftpd checks that the user is allowed to login via a shell. However, we do not want this. To bypass this setting, edit the file `/etc/pam.d/vsftpd`. Change the final line to:

```
auth    required      pam_nologin.so
```

In the next step, we will edit vsftpd's configuration to deny access to any users who are not ftpuser. You can find the vsftpd configuration file at `/etc/vsftpd.conf`. We recommend making a backup copy of the config file prior to changing it. You can find all of the configuration options for vsftpd here: <https://linux.die.net/man/5/vsftpd.conf>

Any time you edit vsftpd.conf, you will need to restart the vsftpd service to let all changes take effect. To do this, run the following commands:

```
sudo systemctl restart vsftpd
sudo systemctl status vsftpd
```

If you need to debug further, try checking the logs or running vsftpd as a process:

```
sudo /usr/sbin/vsftpd /etc/vsftpd.conf
```

Next, edit vsftpd.conf to limit which users can access the ftp server. Do the following:

- Enable the userlist
- Set userlist_file to be `/etc/vsftpd.userlist`
- Deny any users from logging in unless they are listed in userlist_file

6) What lines in vsftpd.conf did you edit to do this? (12 pts)

```
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

After editing vsftpd.conf, run the following command to add ftpuser to userlist_file:

```
sudo bash -c 'echo "ftpuser" > /etc/vsftpd.userlist'
```

Make sure to restart the vsftpd service. We will check to make sure that our configuration is working before moving on. Run the command `sudo ftp 127.0.0.1` to connect to the ftp server. Log in as ftpuser. You should see "230 Login successful" after entering your password if everything is working properly. Type quit to exit the ftp prompt, and then connect to the ftp server again, this time logging in as any user other than ftpuser. You should see "530 Permission denied."

- 7) Provide a screenshot showing your successful ftp login as ftpuser and your unsuccessful login attempt as another user. (15 pts)

```
cyber@cyber-VirtualBox:/etc$
cyber@cyber-VirtualBox:/etc$
cyber@cyber-VirtualBox:/etc$
cyber@cyber-VirtualBox:/etc$
cyber@cyber-VirtualBox:/etc$
cyber@cyber-VirtualBox:/etc$ sudo ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:cyber): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
cyber@cyber-VirtualBox:/etc$
cyber@cyber-VirtualBox:/etc$ sudo ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:cyber): notme
530 Permission denied.
Login failed.
ftp>
```

Currently, ftpuser can navigate anywhere within the filesystem via ftp. We will add a chroot jail so that ftpuser is restricted to a specific directory that files will be served from. To do this, uncomment the following line to /etc/vsftpd.conf:

```
chroot_local_user=YES
```

Make sure to restart the vsftpd service for changes to take effect.

The chroot jail is located in ftpuser's home directory by default. It is important that ftpuser does not have write access in the chroot jail.

- 8) Who is the owner of the ftpuser's home directory? The group? What permissions does the owner have on the ftpuser's home directory? The group? Other users? (10 pts)

The owner of ftpuser home directory is ftpuser.

The group is ftpuser.

The owner has read and write permissions.

The group has read permissions only and the other users have read permissions.

Set the following permissions on ftpuser's home directory such that:

- The ftpuser user can read files in it and access it
- Users in the ftpuser group can read files in it and access it

- No one else has any permissions.

9) What command did you use to set these permissions? (10 pts)

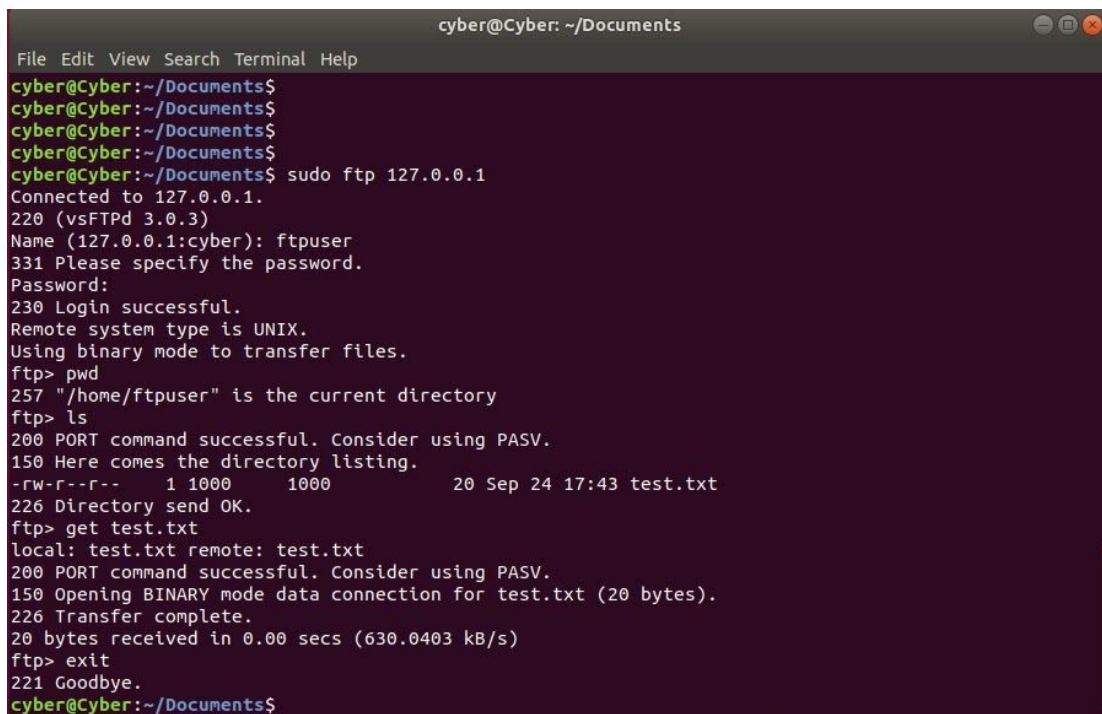
`sudo chmod 550 /home/ftpuser`

At this point, vsftpd should be configured securely. To verify that everything is working properly, create a file named `test.txt` in the ftpuser's home directory. Then run the command `sudo ftp 127.0.0.1` to connect to the ftp server.

Perform the following actions in the ftp prompt:

- Print the path of the working directory
- List the files in the current directory
- Receive the file `test.txt` from the remote server

10) Provide a screenshot of your ftp session. (15 pts)



```
cyber@Cyber: ~/Documents
File Edit View Search Terminal Help
cyber@Cyber:~/Documents$
cyber@Cyber:~/Documents$
cyber@Cyber:~/Documents$
cyber@Cyber:~/Documents$
cyber@Cyber:~/Documents$ sudo ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:cyber): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/home/ftpuser" is the current directory
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 1000    1000      20 Sep 24 17:43 test.txt
226 Directory send OK.
ftp> get test.txt
local: test.txt remote: test.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for test.txt (20 bytes).
226 Transfer complete.
20 bytes received in 0.00 secs (630.0403 kB/s)
ftp> exit
221 Goodbye.
cyber@Cyber:~/Documents$
```