**CMSC 491/791 Active Cyber Defense HW 3**

**Name:**

**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)
2. What port does vsftpd listen on? What command did you run to find this information? (8 pts)
3. What is the full path of the file that vsftpd logs to? (6 pts)

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.

1. 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)

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.

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

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

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

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.”

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

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.

1. 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)

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

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