**Individual Project: FileZilla Server**

FTP (File Transfer Protocol) is a way for you to access, download and upload files to web server. Generally, users need to login when they use FTP to share or transfer files. Each user is given specific privilege what they can do (ie; read access, would let you to view files only, read/write access allows you to read, and write/upload/modify files etc.) You can access FTP via a web browser, command line, or other software application.

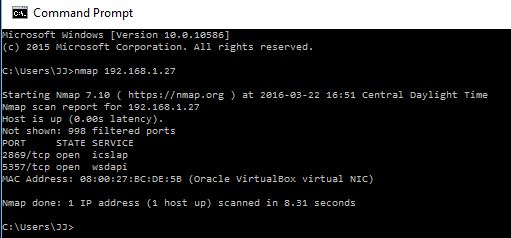
FileZilla is a type of FTP and an open-source sorfware. It includes FileZilla server which is a FTP server and FileZilla client to upload or download files.

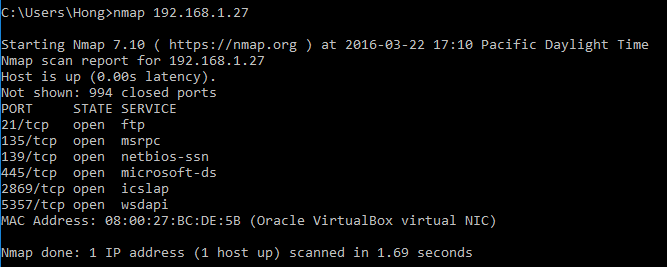
Here are the default configurations for FileZilla server which is not safe and use to be hacked.

* The default installation directory is c:\Program Files (x86)\FileZilla Server. In this installations folder, there are FileZilla application and a XML document which is plaintext and includes all users information.
* In the managing menu, the default welcome message will shows the FileZilla Server version.
* The default mode setting is port mode and the default Listen on port is 21. The default port which is the admin interface of FileZilla Server is 14147.

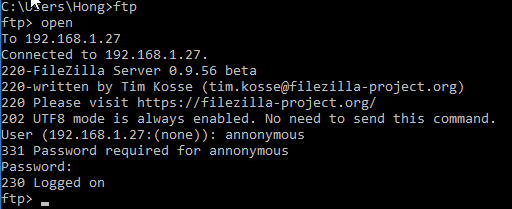
These default setting give hackers some opportunities to attack. Next, I create a scenario of a possible aatatck against the FileZilla server with default configurations. This server has two users. One username is test which has all privileges, can read, and write/upload/modify files. Another username is anonymous which is a guest account and only has the privilege to read file. Usually, most FTP server has this kind of anonymous account to the public. Sometimes, this account has no password. These two accounts use C drive as the sharing folder.

The first thing that I need to do is to identify which systems are running the FTP service. I did a simple scan with Nmap in order to find the open ports. Here is the screenshot which I install the FTP service.

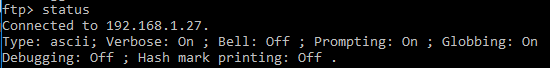


The following screenshot is taken after I install the FTP service. 

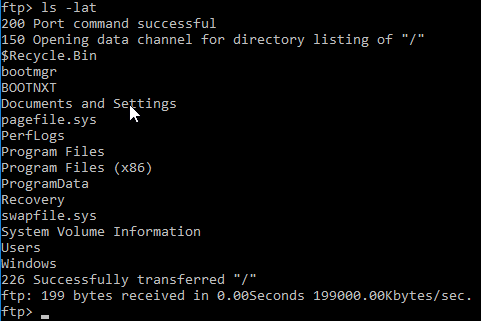
We can see that the FTP port, 21 is open. Now the next logical step that we have to do is to identify which version the FTP application is running by using command line. We will see the default welcome message which tell you this server is FileZilla and the version is 0.9.56 beta.

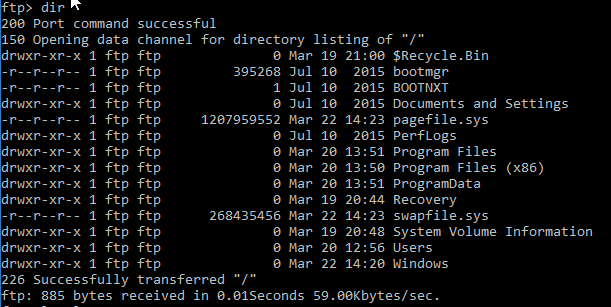


I login the server using the anonymous account. Then, we can check the status of the server.

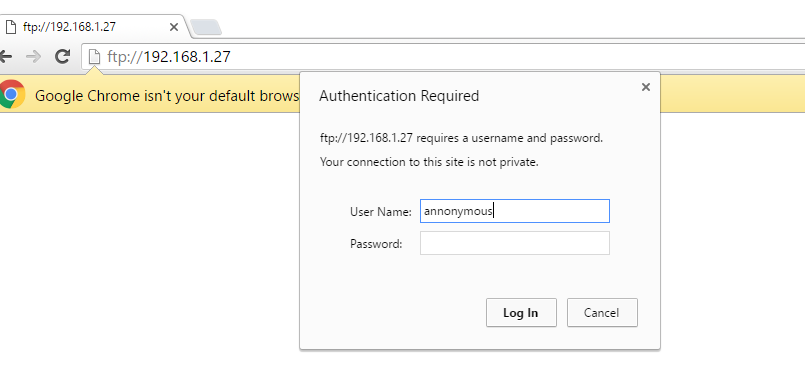


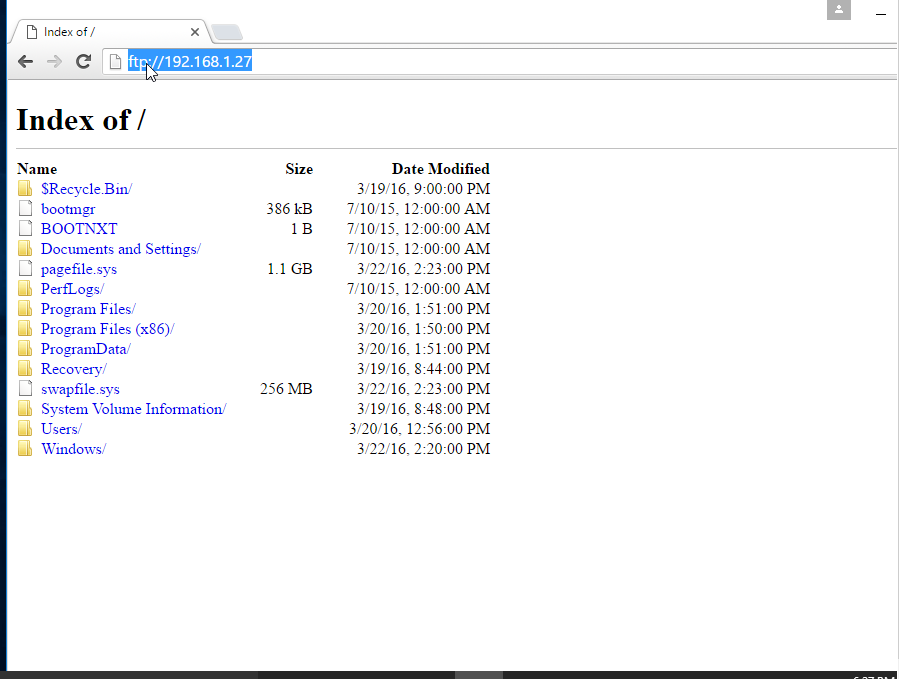
Using the command of “ls -lat” or “dir”, we will see the directories and the files name in the sharing folder of the server. I choose the C driver as the sharing folder because we can access to the default installation derectory, Program Files (x86)\FileZilla Server.



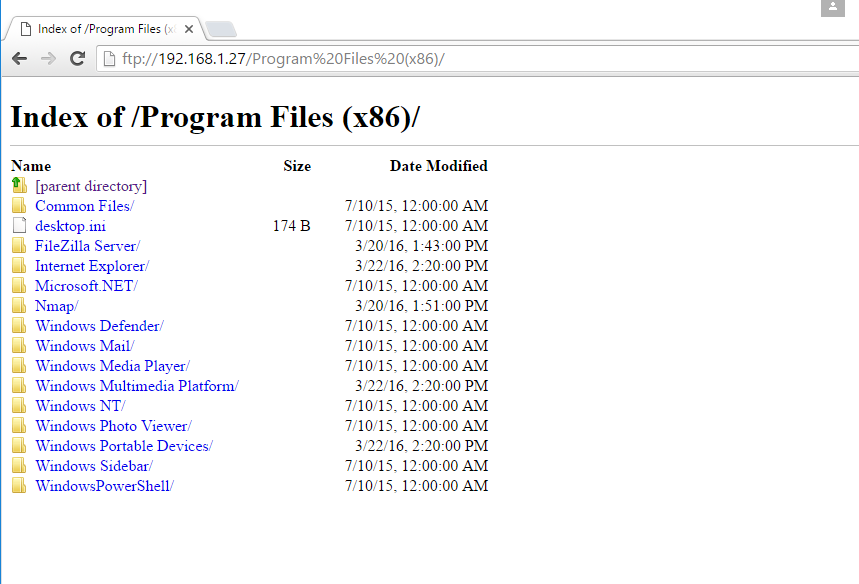


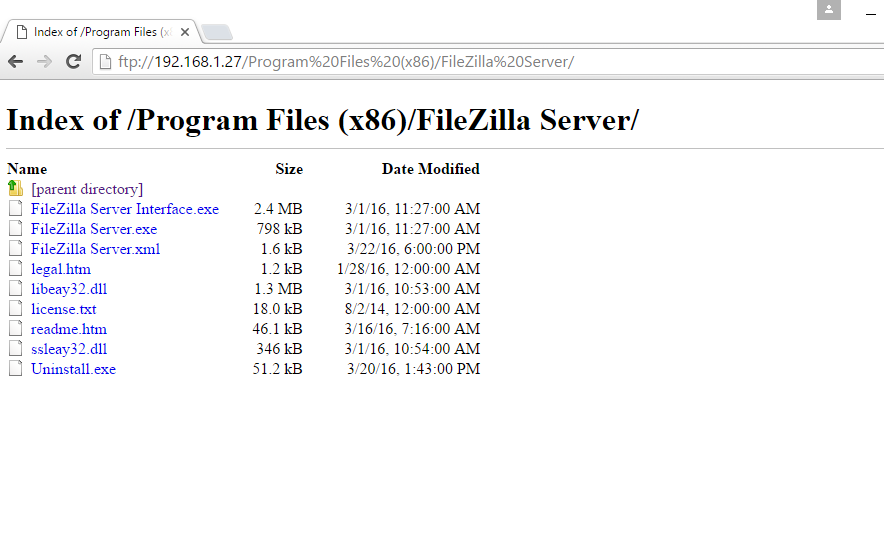
If you think it is not convenient to use command, we can choose to use web browser. Because the default Listen on port is 21, we can type “ftp: ip address of the server:21” in the web browser and access to the sharing folder.



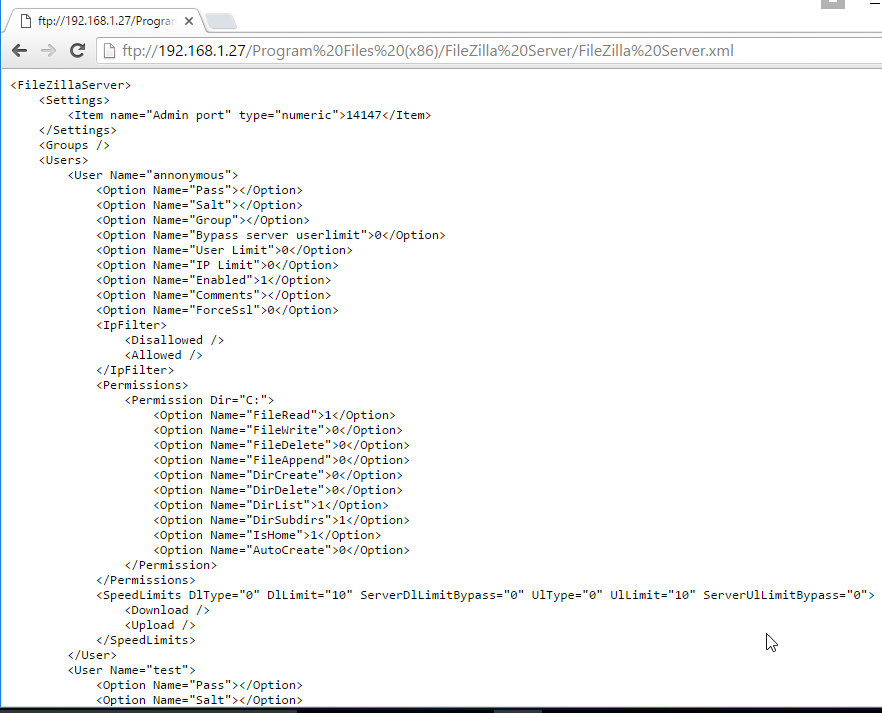


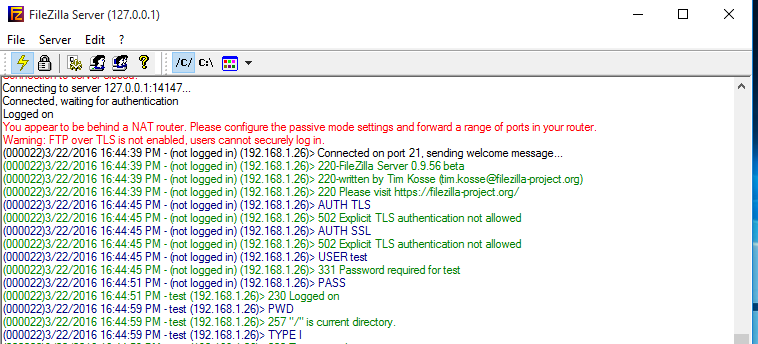
Then, we can go to the installations folder and find the FileZilla XML document which includes all users information.

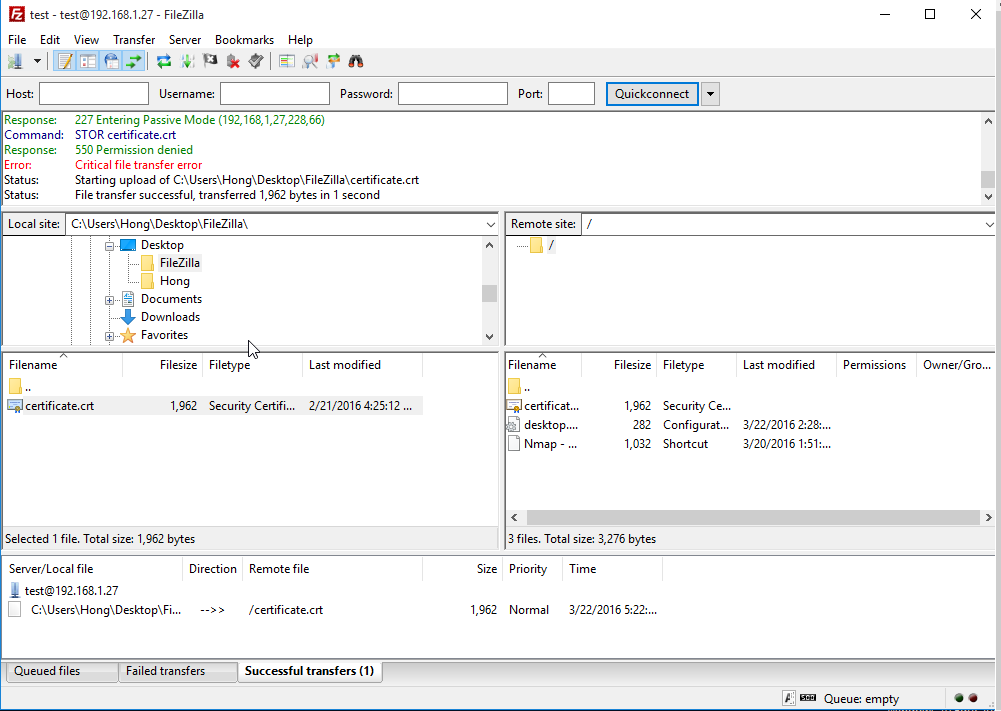




The file name is FileZilla Serr.xml and we can see there are two users. One is anonymous and the other is test.

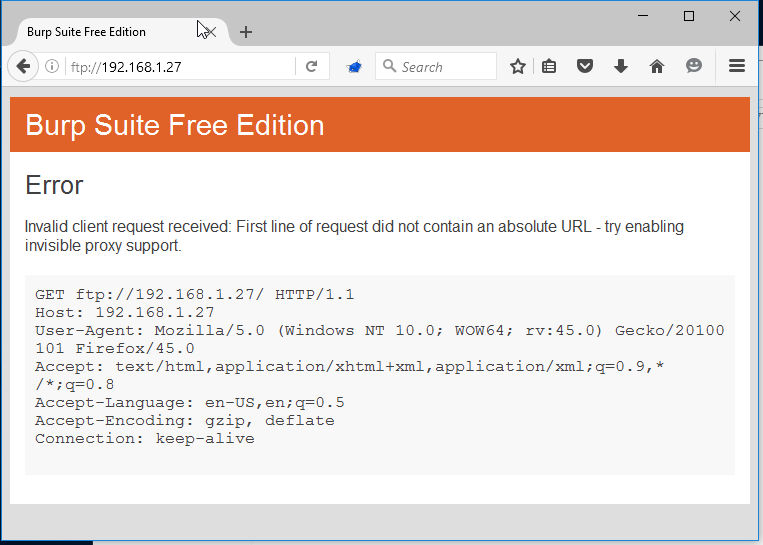


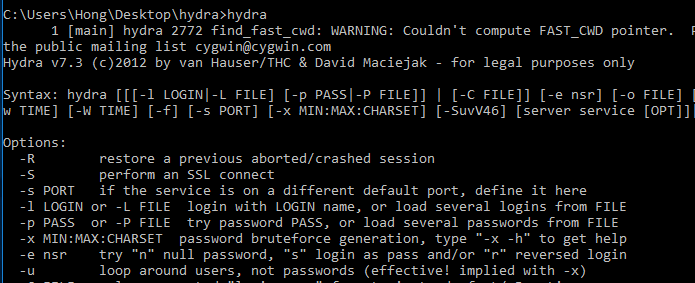
Comparing these two users, we can find the user, test has more privileges. Then, we login the FileZilla Client using the username, test and transfer a file to the server. 



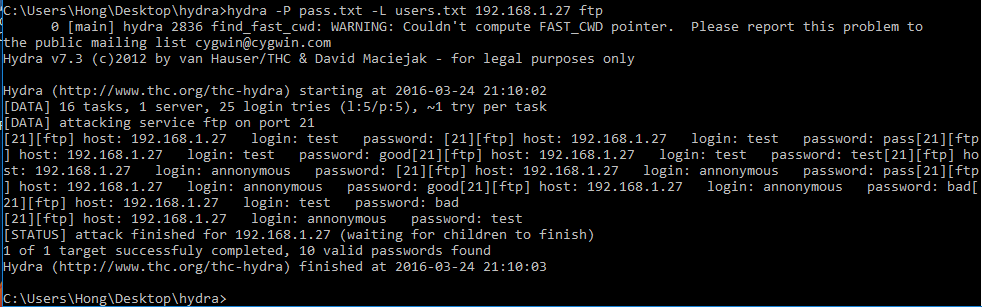
Honestly, there are many other attacks you can perform against the server that aren’t related to default configuration options, such as Brupsuit and Hydra. We can choose different tools but the process is almost the same. It can be divided into five steps. Find the username, crack the password, connect with the FileZilla server, find the installation folder and get or change the privileges.

Brup can inject commands and break the password but it only works with URL, not ftp://.



Hydra is another popular online password cracking tool and can be used to do a dictionary attack to login a FileZilla server. 

I create a users text file and a password text file. Then, hydra will run any combinations of usenames and password supplied in the files. The best way to use it is only using usernames you know exist, such as annonymous, and a list of passwords.



After you get the username and password, you can login the server and find other information which you want.