Network Penetration Testing Methodology-External

1 Hr 7 Min Remaining

Instructions Resources Help  100%

Exercise 2: Accessing Misconfigured FTP Connection on a Remote Machine

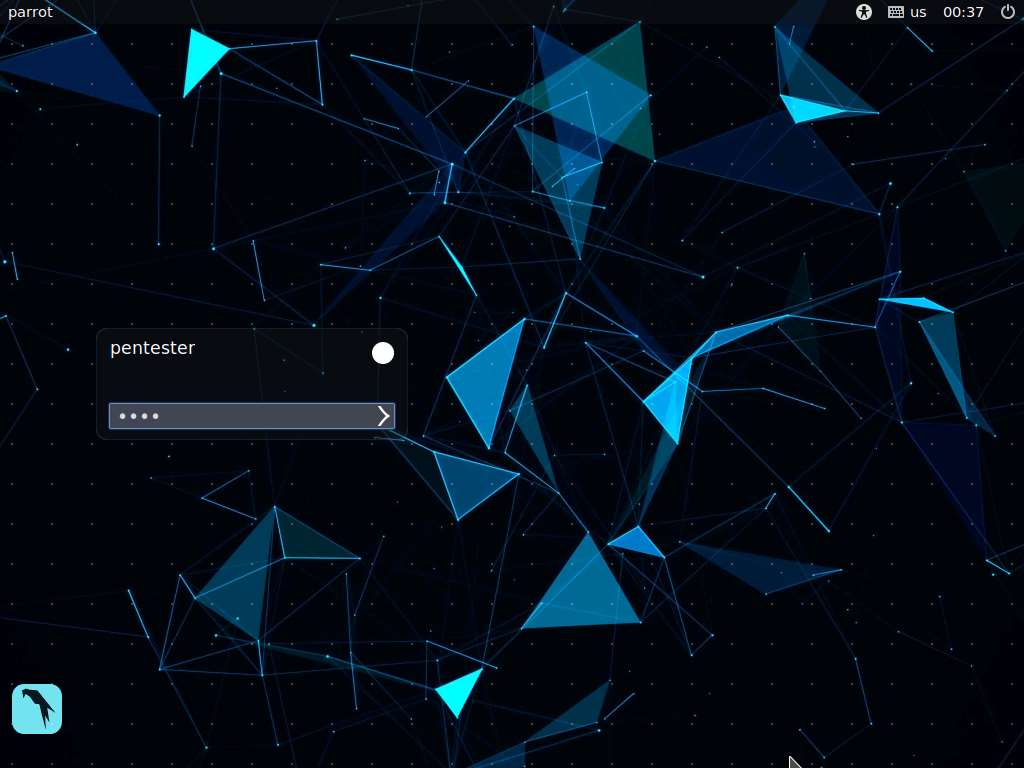
Scenario

File transfer protocol allows authenticated users to upload/access and download files and folders between a client and a server. When anonymous access is enabled on the server, it allows everyone access files on it, leaving the security of sensitive information at risk.

As a pentester, you should be able to find the FTP servers inside a network which have anonymous access enabled. In this lab, you will be learning how to identify the FTP servers which have anonymous access enabled.

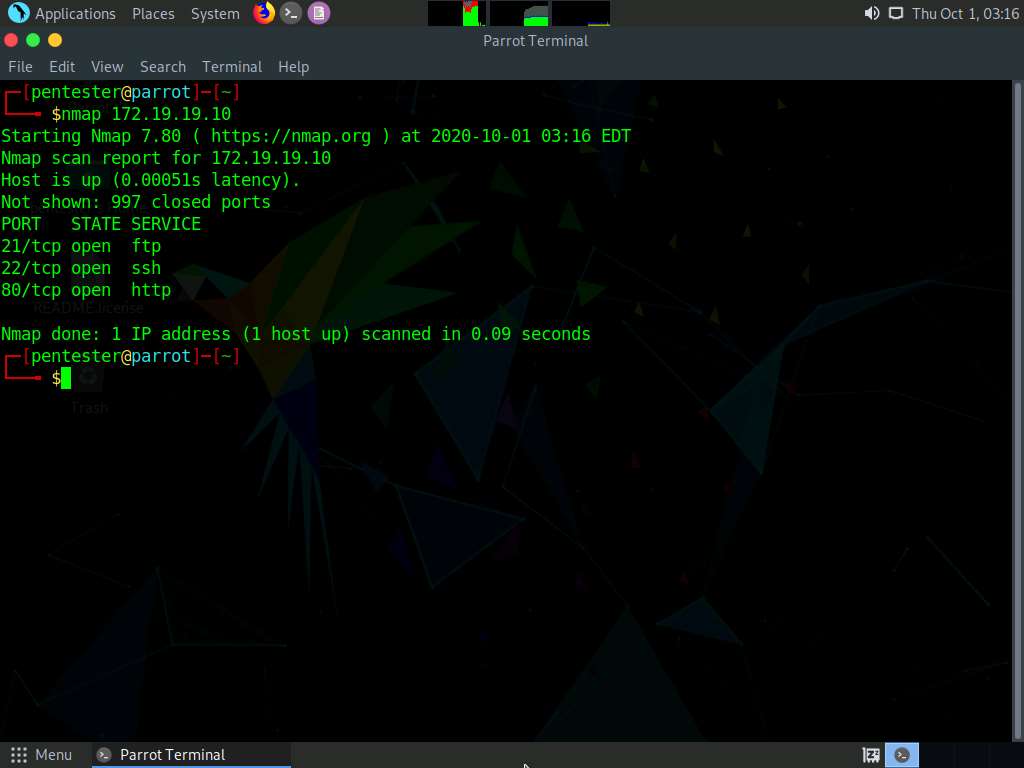
**Lab Duration**: **20** Minutes

1. Click [Parrot](https://labclient.labondemand.com/Instructions/d51b1821-8ebe-4479-bf4b-33b56a1978d1?rc=10). Parrot logon screen appears, type **toor** in the Password field and press **Enter**.

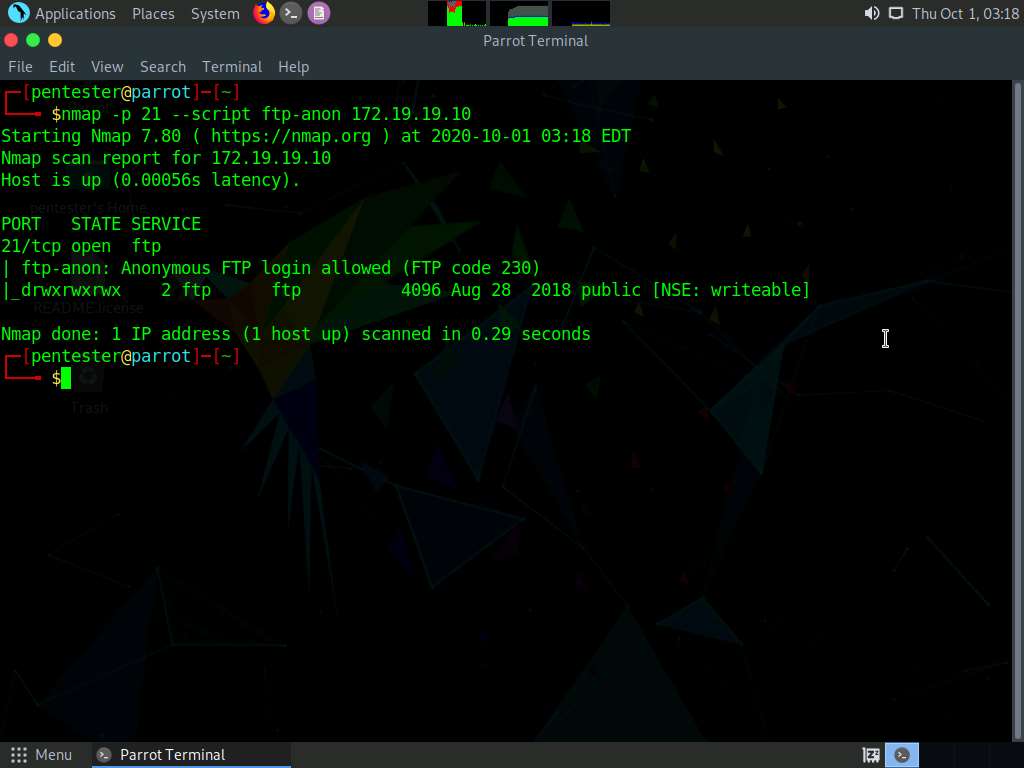


1. In this lab, we will be performing penetration testing on a machine to find any loopholes and gain access to its resources. For this, we are going to scan **Ubuntu Server** for open ports and services running on the machine. To scan, launch a command line terminal, type **nmap 172.19.19.10** and press **Enter**. This performs a Nmap regular scan on the machine and displays the results as shown in the screenshot.

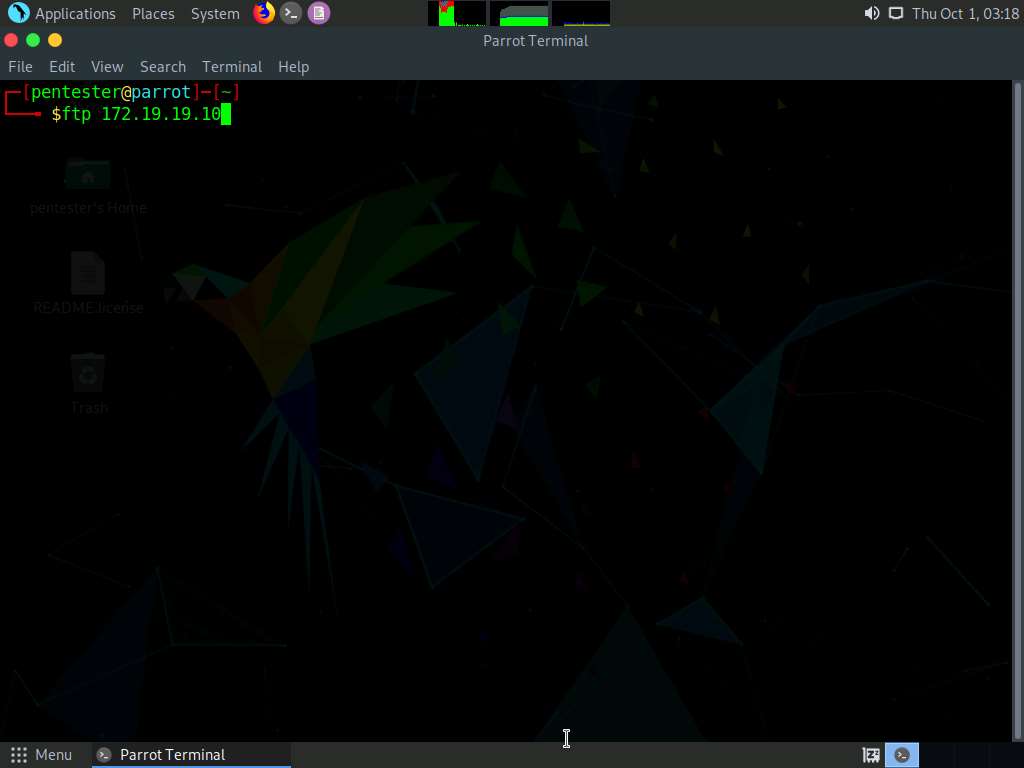
In this lab, we are scanning IP address of the target machine located in the external network, whereas, in real-time, you will be scanning domains for eg. **ftp.[targetwebsite].com**.



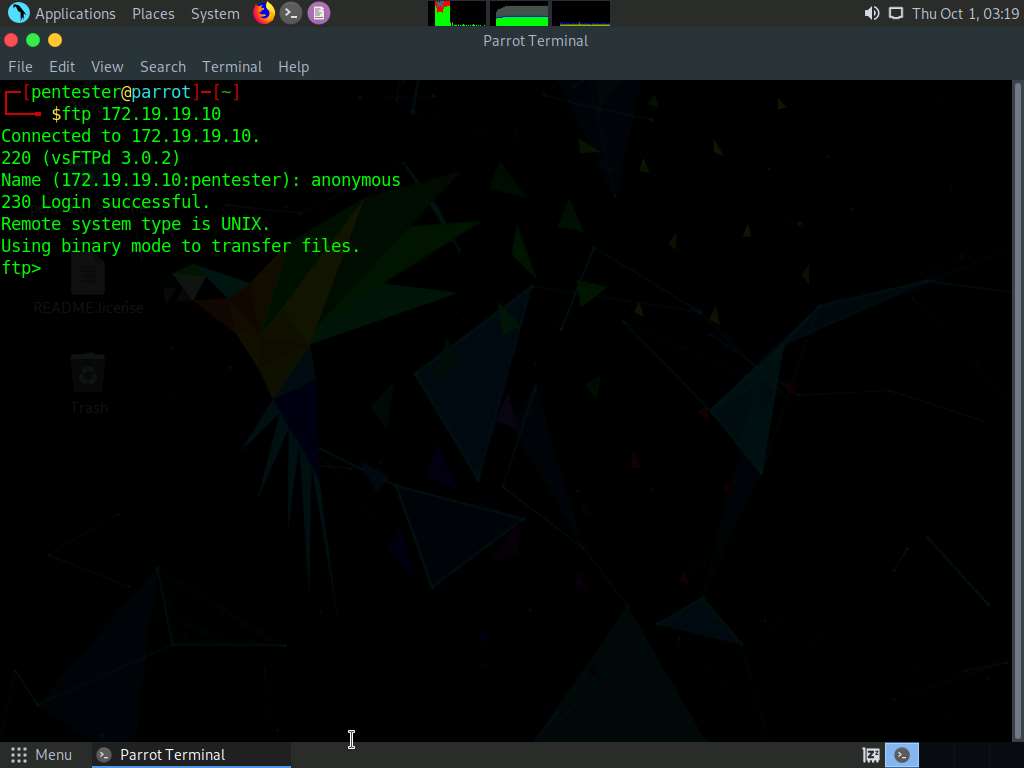
1. In the previous task, it was observed that ports **21**, **22**, **80** are open. Let us begin with port **21**. We shall first check if we can access FTP on the machine anonymously. For that, we will run Nmap scan with the **ftp-anon** script to find out whether anonymous login is enabled on the machine. Type **nmap -p 21 --script ftp-anon 172.19.19.10** and press **Enter** to begin the Nmap scan.
2. It is observed that Anonymous FTP Login is enabled on the FTP Server.



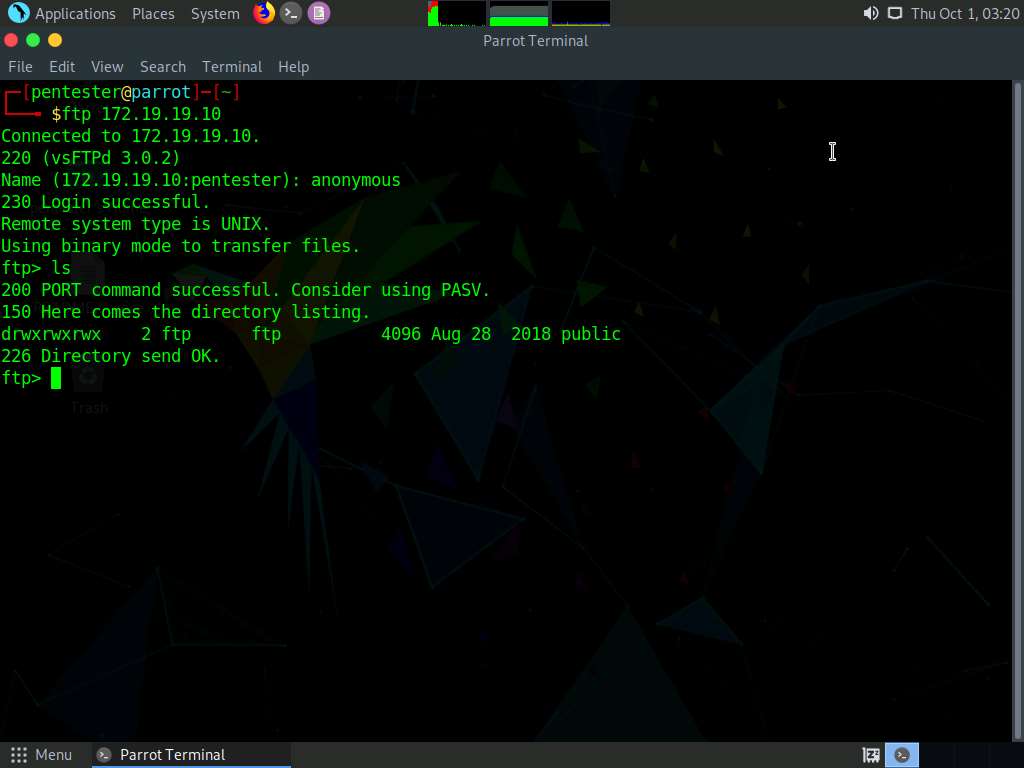
1. Now, we shall log in to the FTP server and access contents in the FTP directory. Type **ftp 172.19.19.10** and press **Enter.**



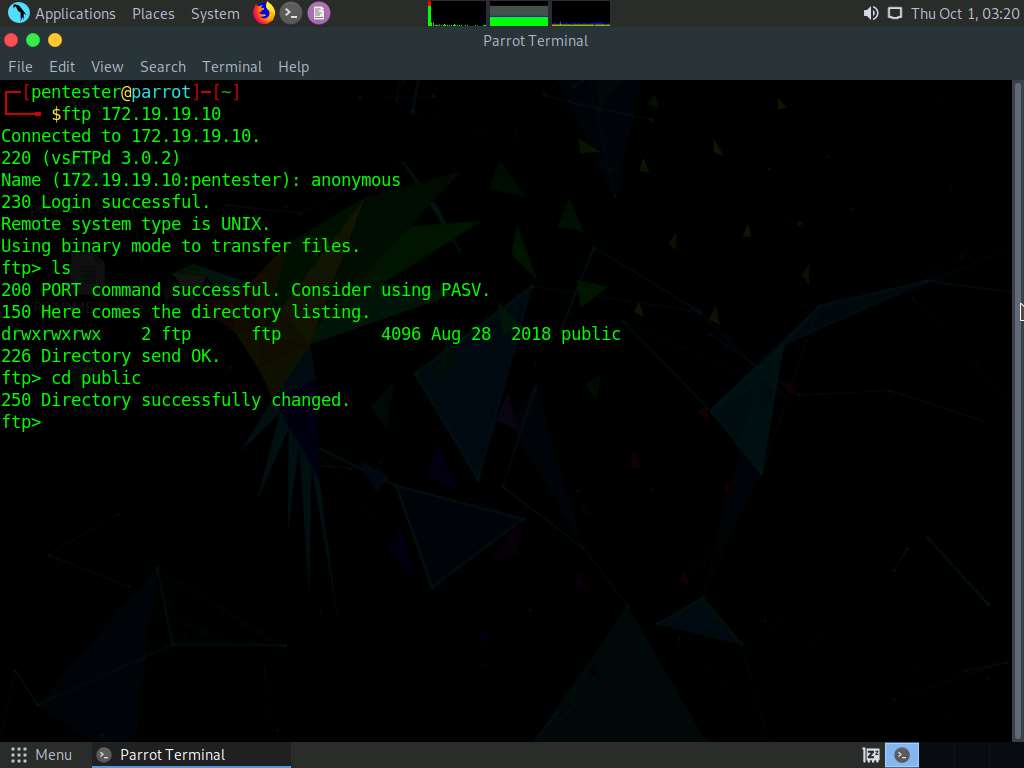
1. You will be asked to enter a login name. Type **anonymous** and press **Enter**.
2. Upon entering the login name, an ftp shell appears, stating that the FTP login has been successful. This shows we have successfully logged in to the remote machine using FTP.



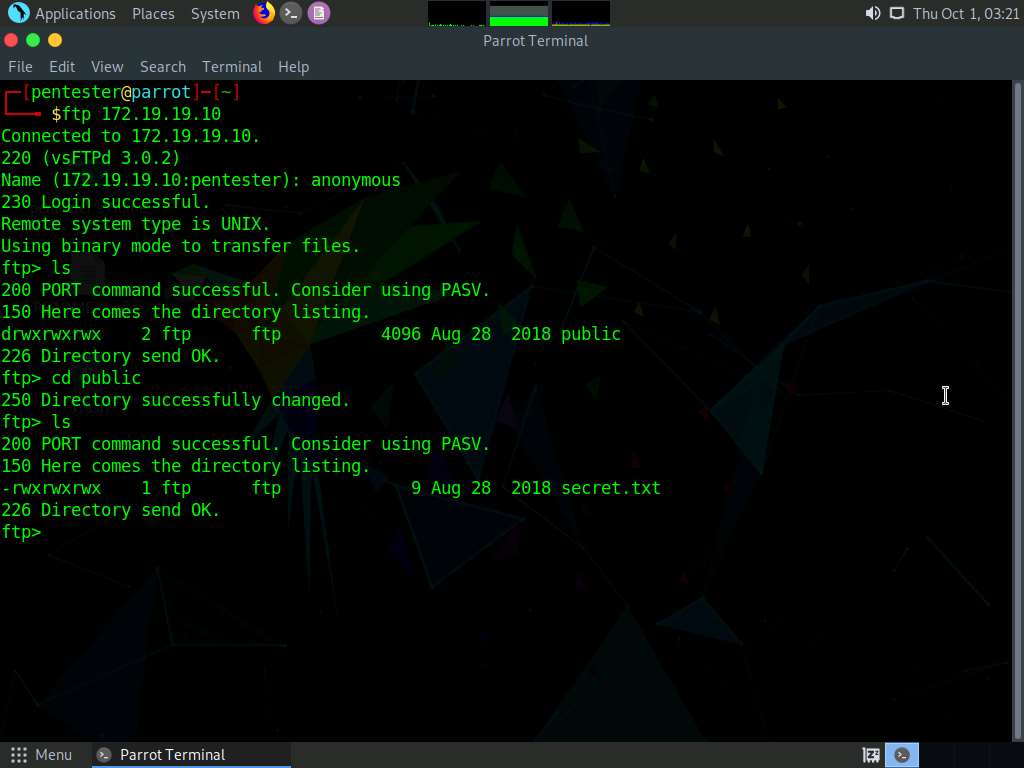
1. Now, we shall view the files and directories inside the FTP root directory. To view them, type **ls** and press **Enter**. This displays all the directories and files in the FTP root directory, along with their file/directory permissions as shown in the screenshot below. It is observed that the directory permissions for "public" folder have read-write-execute access enabled to all the user groups. We shall attempt to upload a file to this directory in the forthcoming tasks.



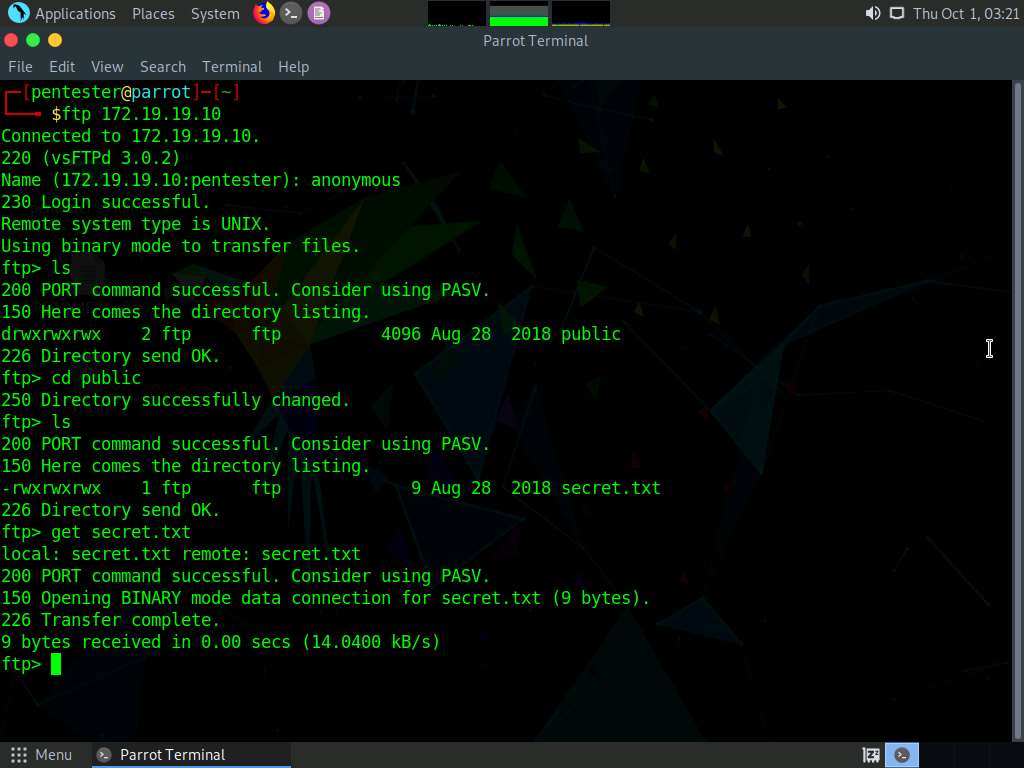
1. Now, we shall navigate to the **public** folder to view its contents. To navigate, type **cd public** and press **Enter**.



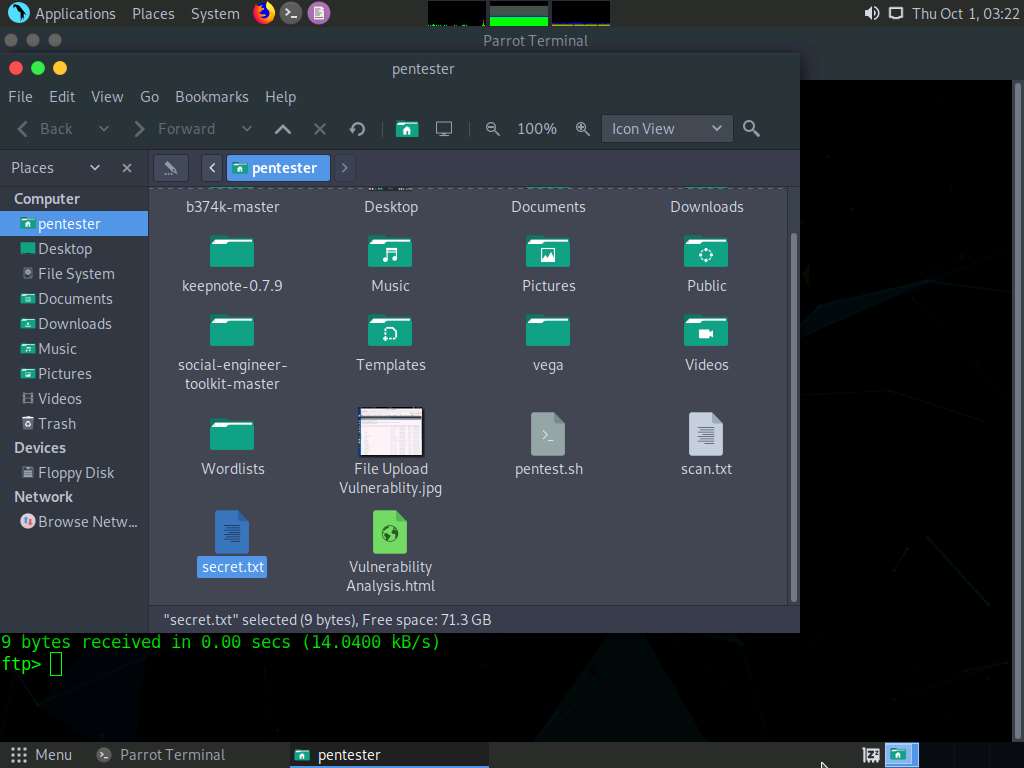
1. Type **ls** and press Enter to view the files and folders inside the "**public**" folder.



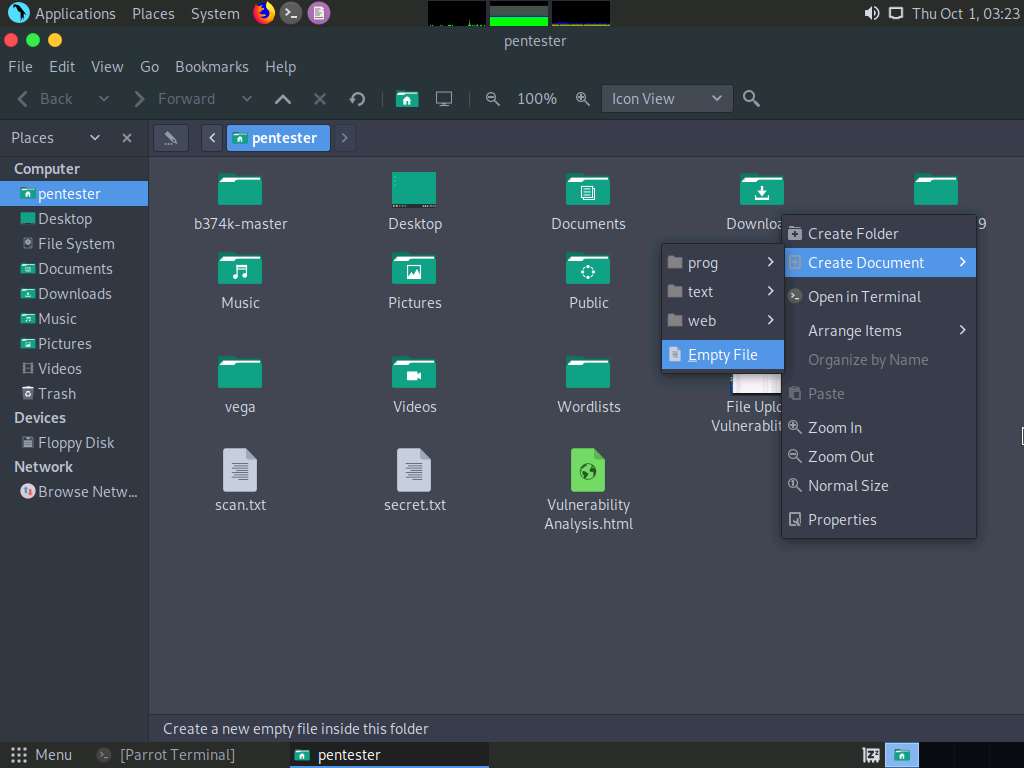
1. You will observe the file named **secret.txt** in the folder.
2. Now, we shall see if we can download the files from the server. To download **secret.txt** file, type **get secret.txt** and press **Enter**.

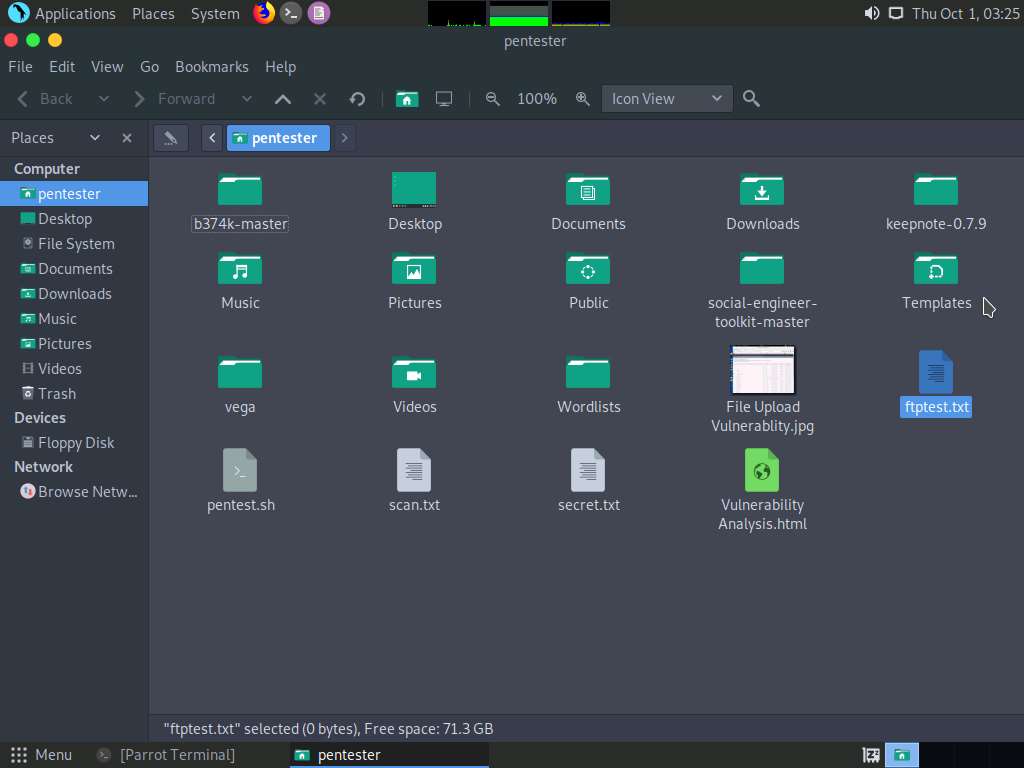


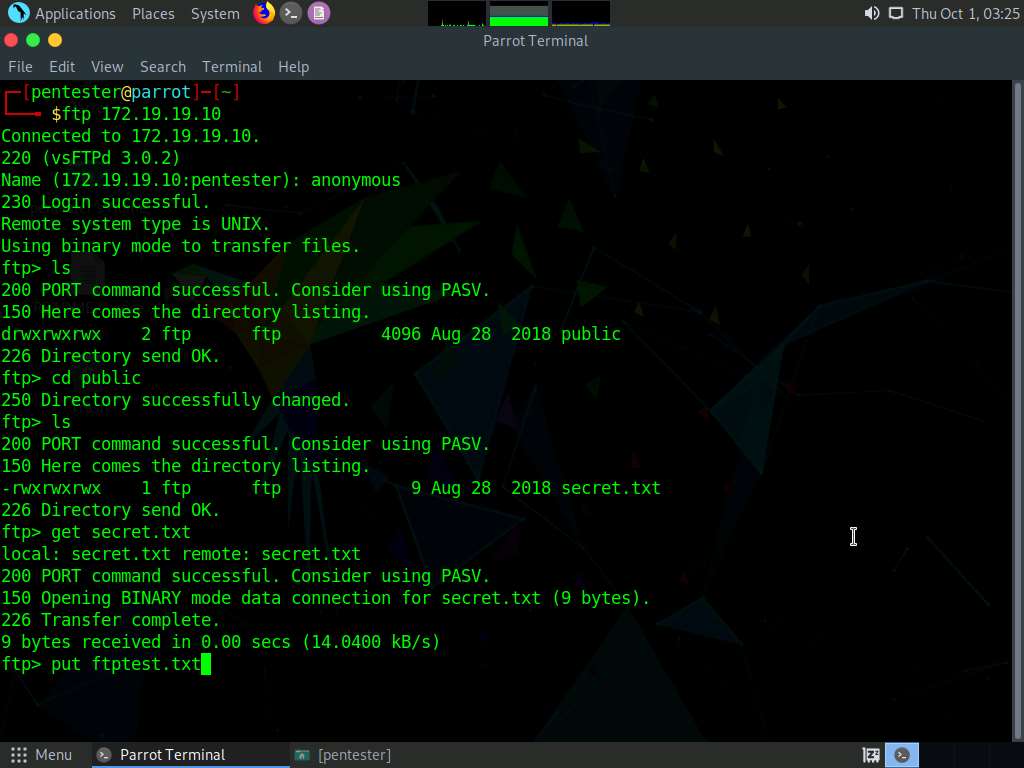
1. The downloaded file is saved to the **Home** folder as shown in the screenshot below.



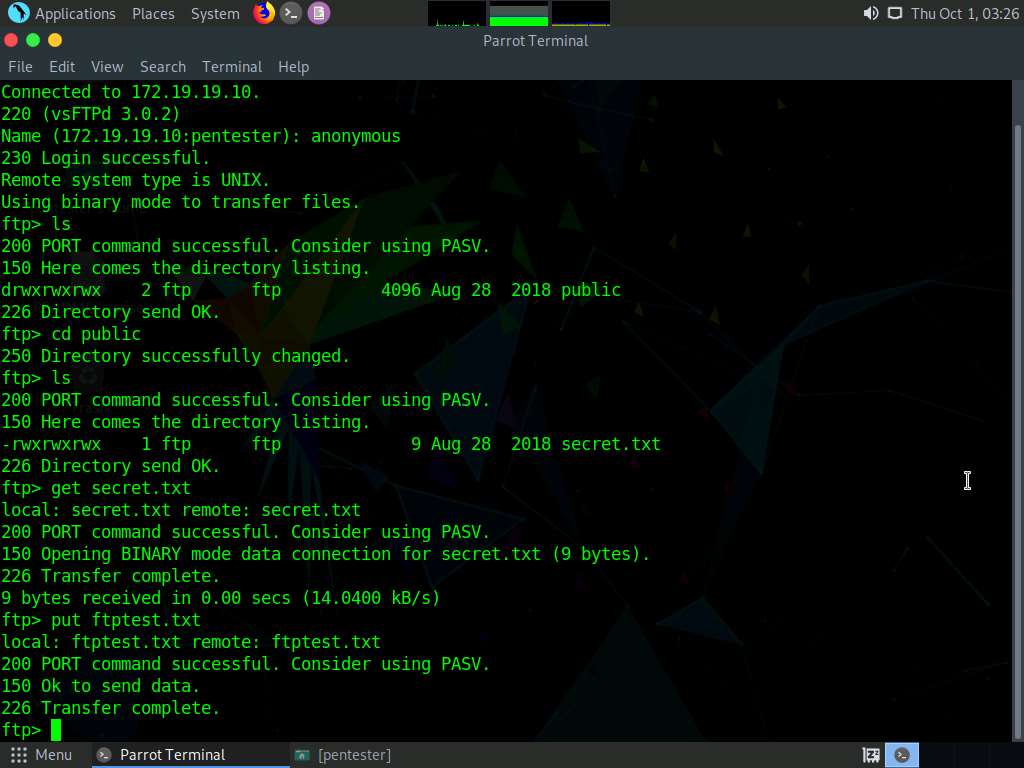
1. Now, we shall see if we can upload a file to the FTP server. Create a file **ftptest.txt** (as an example) in the **Home** folder of Parrot machine to send it to the FTP Server. Open your **Home** Folder and **Right Click** and navigate to **Create Document** and click **Empty File** and name the file as **ftptest.txt**. Go back to **Terminal**, to upload type **put ftptest.txt** and press **Enter**.



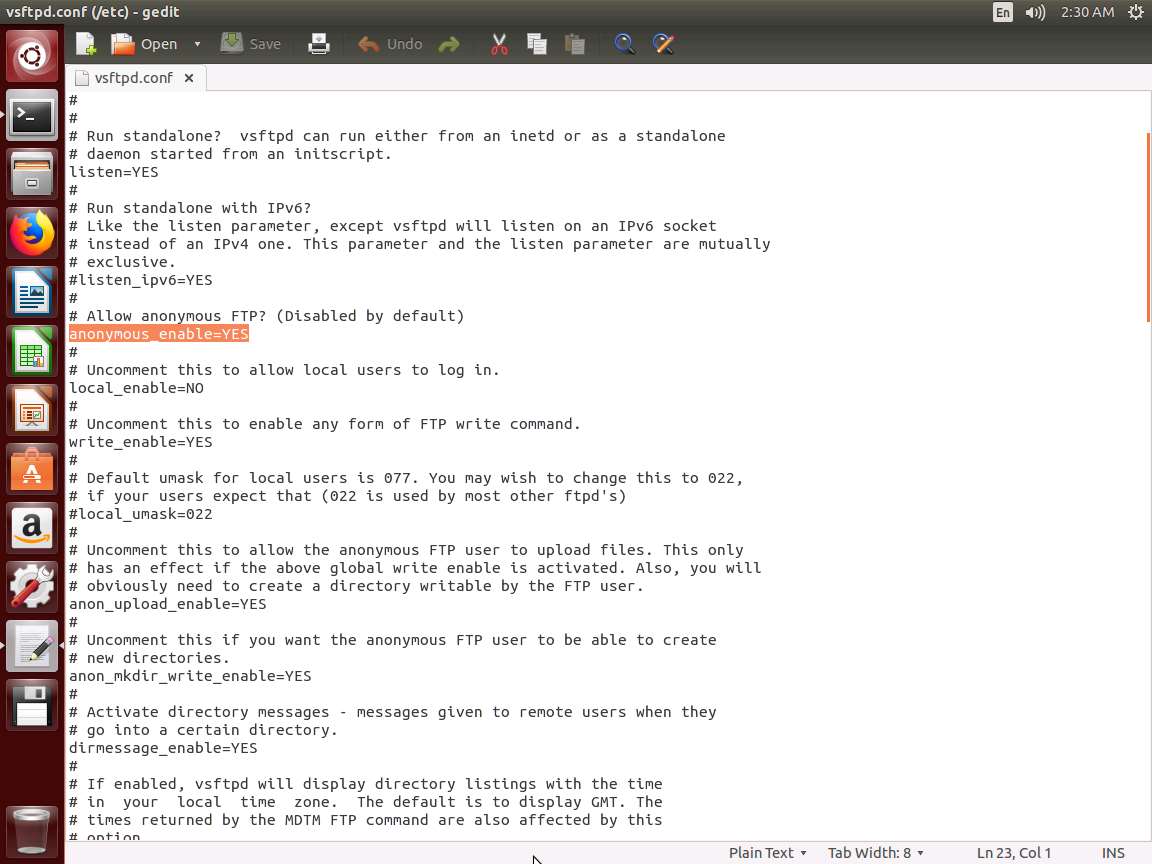


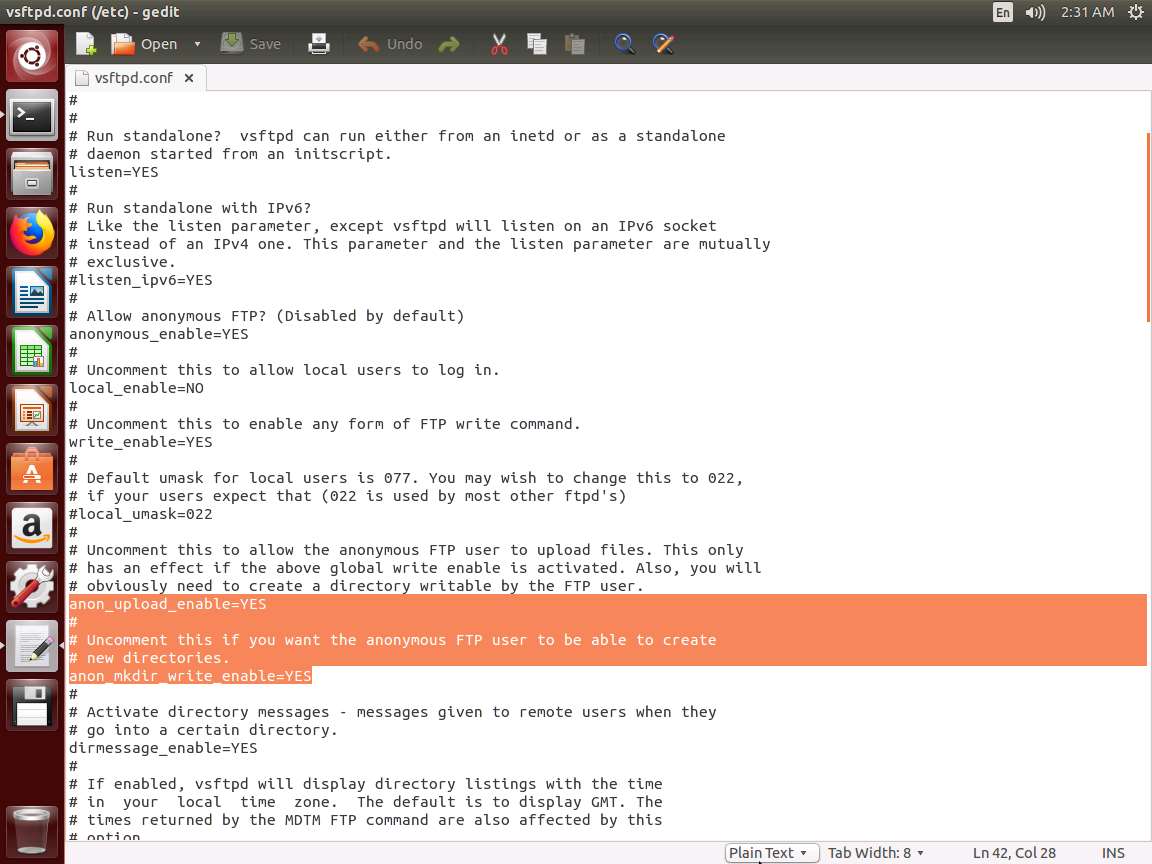


1. The file was successfully uploaded to the server as shown in the screenshot below. This means that file upload access has been enabled on the Ubuntu Server which can allow an attacker to upload malicious files to it.



1. As highlighted in the screenshot, the options **anonymous\_enable**, **anon\_upload\_enable** and **anon\_mkdir\_write\_enable** have been enabled which allowed us to login to FTP server anonymously and upload files to it.





In this lab, you have learned how to identify and connect to FTP servers that have anonymous access enabled.