

# FTP Breakout

## Mission: FTP user/password enumeration

**Description:**

We got a new target that we would like to compromise and get a secret file from. We already run some assessments and gathered some intelligence - none of this was needed but maybe you will find a way to use it.

**Documentation and intelligence:**

FTP is a basic file transport protocol - its communication done with a basic text-based reference.

Read the next documentation:

<http://www.tcpipguide.com/free/t_FTPControlConnectionEstablishmentUserAuthenticatio-2.htm>

The documentation above describes a basic authentication process of FTP server.

The target VM:

* https://www.dropbox.com/s/e8whgx251hh2y08/ftp-challenge.ova?dl=0
* **ftp-challenge.ova**
* When you run the VM you will get a banner with its assigned IP address

There is a valid user we could put our hands on:

* **anonymous:password**

Wordlist:

* **Passwords:**

<https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/Common-Credentials/best1050.txt>

* **Users:**

<https://github.com/danielmiessler/SecLists/blob/master/Passwords/Common-Credentials/top-20-common-SSH-passwords.txt>

Use all the above information to create an enumeration script:

1. The script will be based on Socket module
2. The script will be able to enumerate available users
3. The script will be able to crack the user password

After we get the user and the password:

1. Use one of the available libraries of python for FTP to create an FTP client
2. The FTP client code should download the **secret.txt** file.