

# Lab - Using Hydra to Brute Force a Password

## Overview

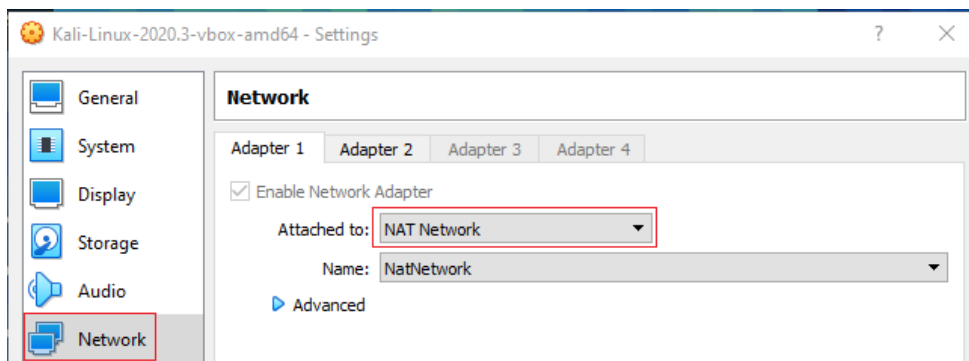
In this short lab, you will learn how to use the password cracking utility Hydra to brute force a password for VNC running as a service on Metasploitable2. Hydra is a pre-installed tool in Kali Linux used to brute-force username and password to different services such as ftp, ssh, telnet, MS-SQL, etc. Brute-force can be used to try different usernames and passwords against a target to identify correct credentials.

## Lab Requirement

- One virtual install of Kali Linux
- One virtual install of Metasploitable2

## Begin the lab

Ensure that both your virtual installs of Kali Linux and Metasploitable2 are up and running and configured for NAT networking.



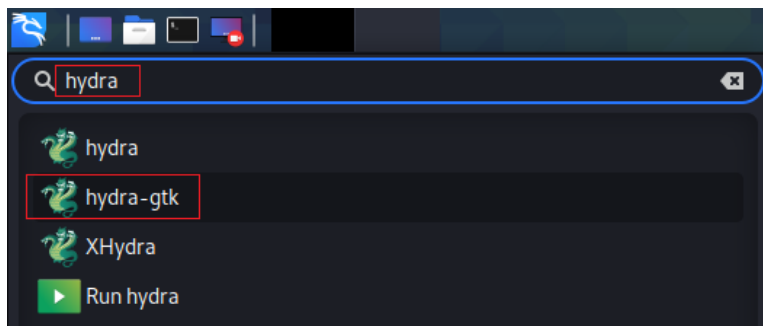
Use ifconfig on your Metasploitable2 machine to find its assigned IPv4 address.

```
msfadmin@metasploitable:~$ ifconfig
eth0: Link encap:Ethernet HWaddr 08:00:27:f6:69:30
      inet addr:10.0.2.11 Bcast:10.0.2.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe6:6930/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
      RX packets:32 errors:0 dropped:0 overruns:0 frame:0
      TX packets:68 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:6664 (6.5 KB) TX bytes:7648 (7.4 KB)
      Base address:0xd020 Memory:f0200000-f0220000
```

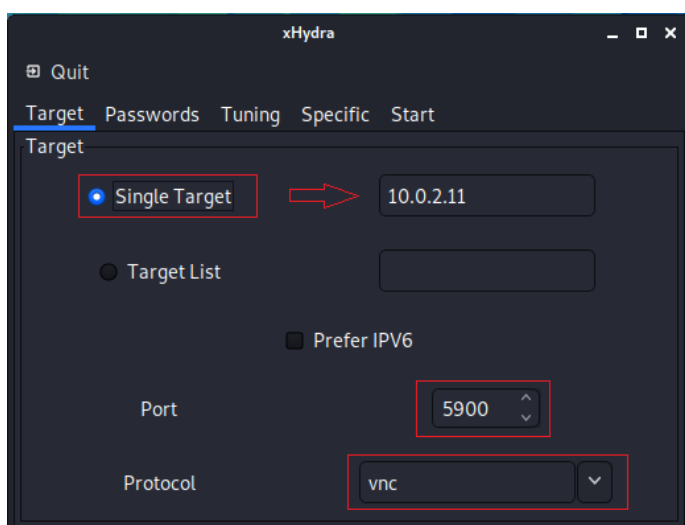
This is my IP address; yours will differ!

From your Kali Desktop, click on the application launcher and type the word, hydra, in the search bar.

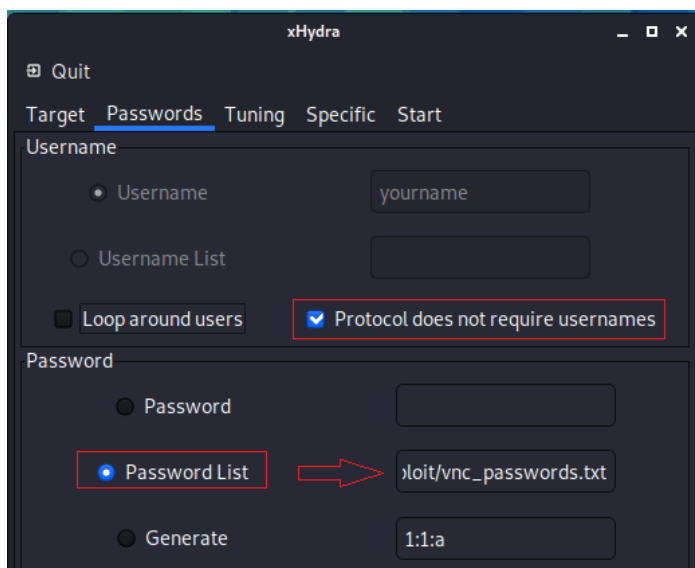
From the available options, select **hydra-gtk**. For this lab, we will be using the GUI interface version of hydra.



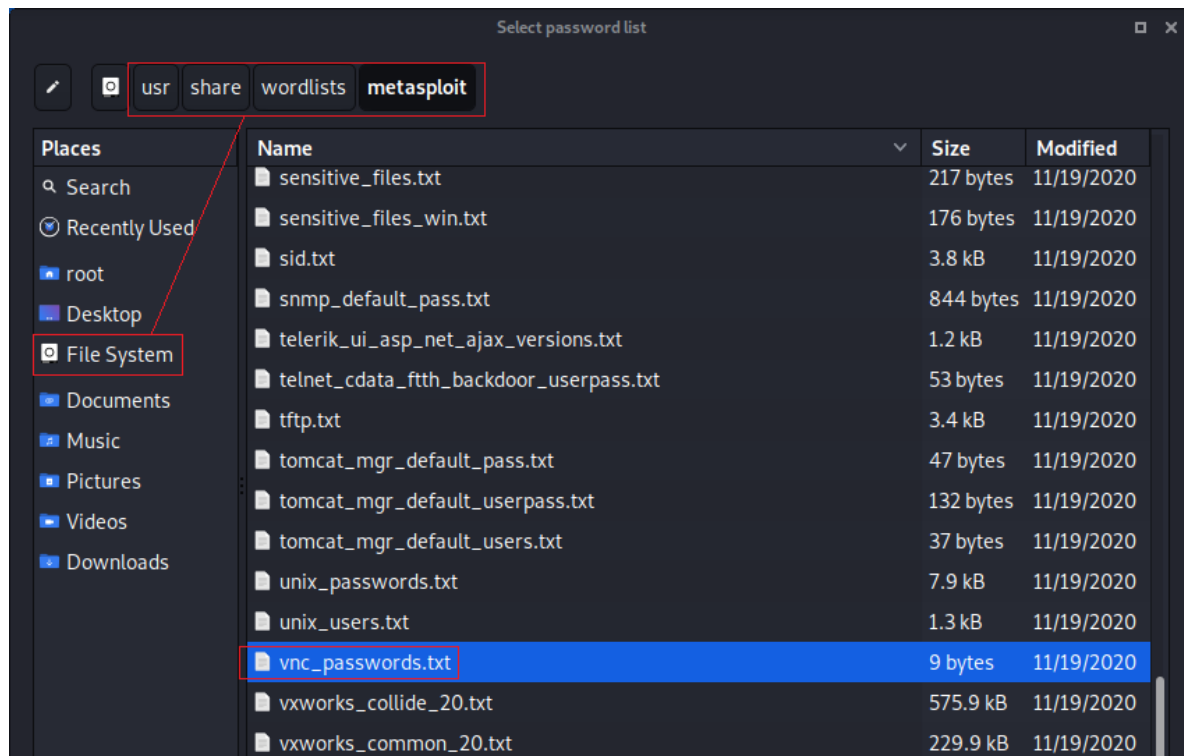
For the Target tab, select Single Target. For the IP address, type in the IP address for your Metasploitable2 target. For the port number, use 5900. From the Protocol, form the list, select VNC.



On the Password tab, Check the box for Protocol does not require usernames. Select the radio button for password list,

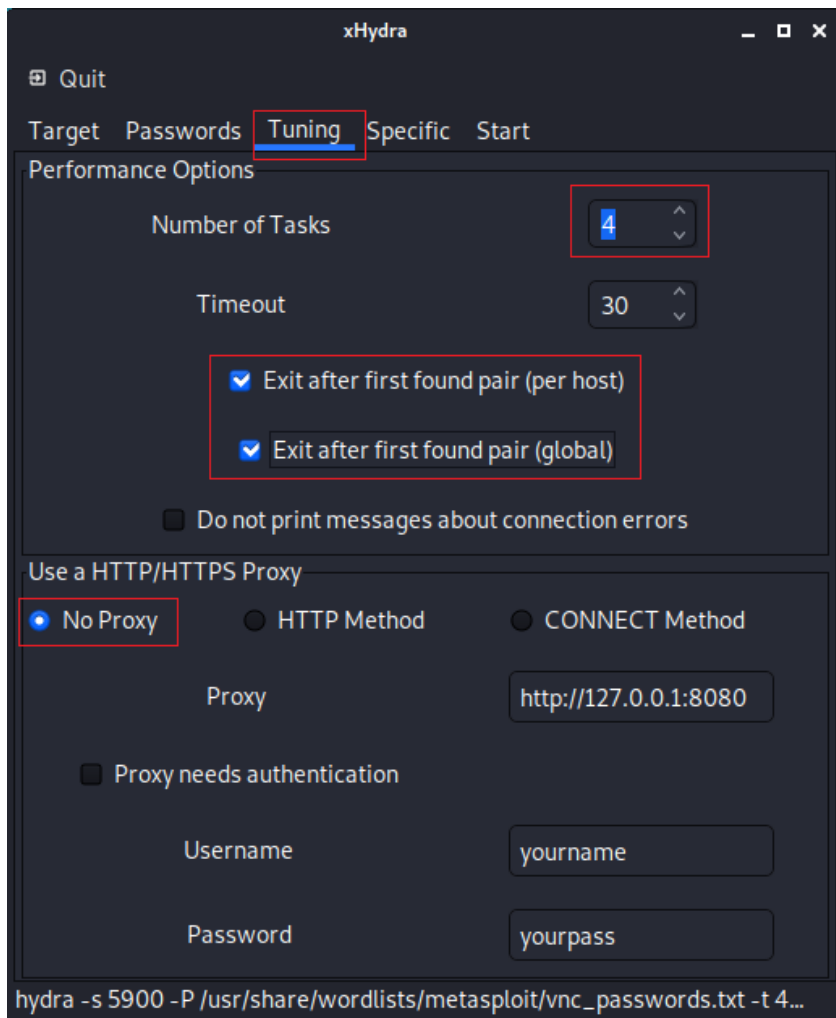


Click on the windows to insert the path for the password list. From the left windowpane, click on File System. From the right windows pane, scroll to the bottom of the available directories and open the **usr** share, next open the directory named **share**, next, open the directory labeled **wordlist**, and finally, the directory marked **Metasploit**. Scroll through the available wordlists until you come to vnc\_passwords.txt and x2 click the file. This is the wordlist hydra used to brute force the VNC password for VNC running on your Metasploitable2 machine.



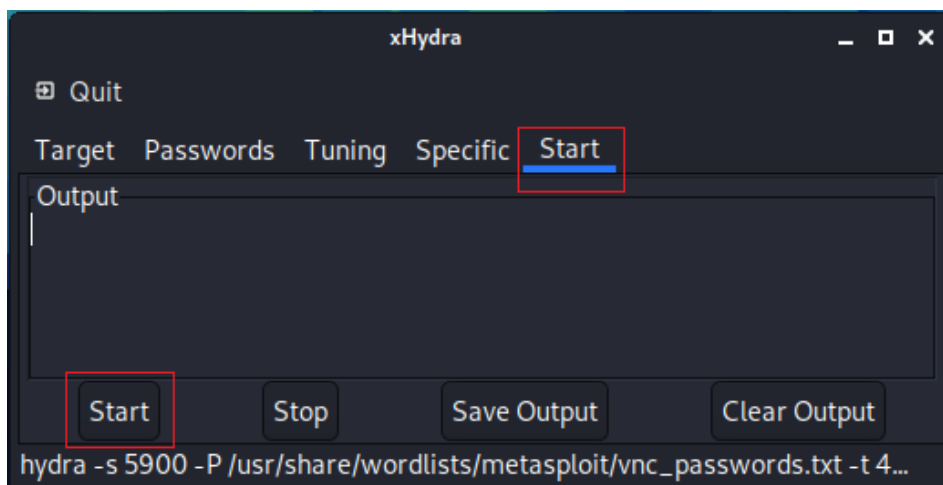
## Tunning tab

On the tuning tab, change the **Number of Tasks** from 16 to 4. Check the two boxes for Exit after the first found pair. Ensure the utility is not configured to use a proxy.

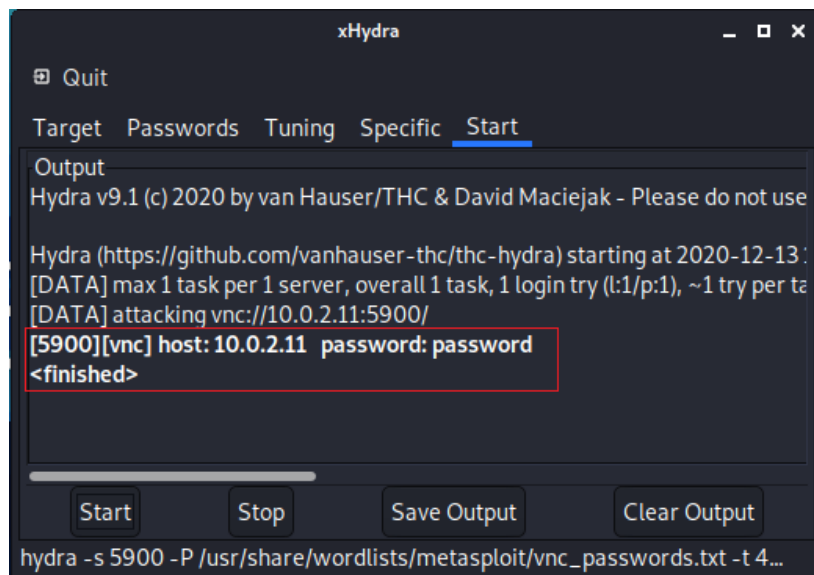


## Start tab

Once your settings are correct, click on the Start tab. Scroll to the bottom and click Start to launch the brute force password attack.



In just a moment, hydra discovers the password for the VNC service running on our target.



The screenshot shows the xHydra application window. The 'Start' tab is selected. The output area displays the following text:

```
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-12-13
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per ta
[DATA] attacking vnc://10.0.2.11:5900/
[5900][vnc] host: 10.0.2.11 password: password
<finished>
```

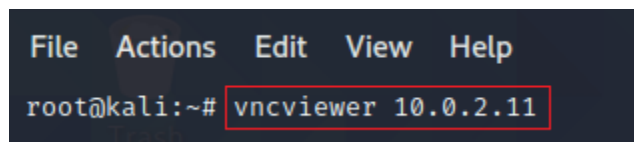
Below the output area are buttons for 'Start', 'Stop', 'Save Output', and 'Clear Output'. At the bottom, the command being executed is shown: `hydra -s 5900 -P /usr/share/wordlists/metasploit/vnc_passwords.txt -t 4...`

Since we check the two boxes for hydra to exit after finding the first pair, it stopped the attack once it found a password. You can uncheck both boxes and rerun the attack to see the difference.

## Connect Using VNC

Now that we have the password, we can open a terminal from our Kali machine and connect to the target using VNC.

At the terminal type, **vncviewer 10.0.2.11** <This is my IP address, yours will differ!>

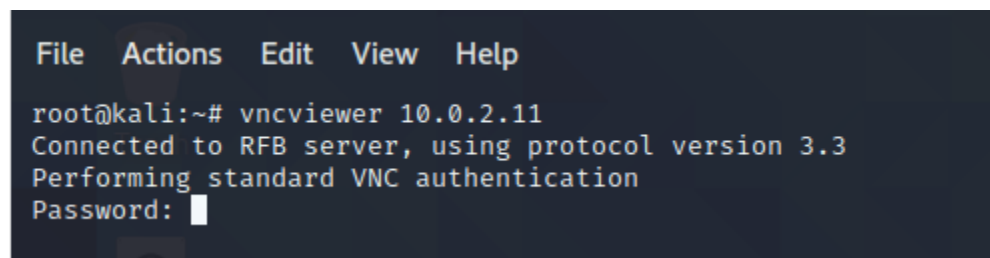


The screenshot shows a terminal window with the following text:

```
File Actions Edit View Help
root@kali:~# vncviewer 10.0.2.11
```

Press enter. Type in the password you discovered during the brute force attack. (In Linux, you cannot see the password as it is being typed at the prompt.)

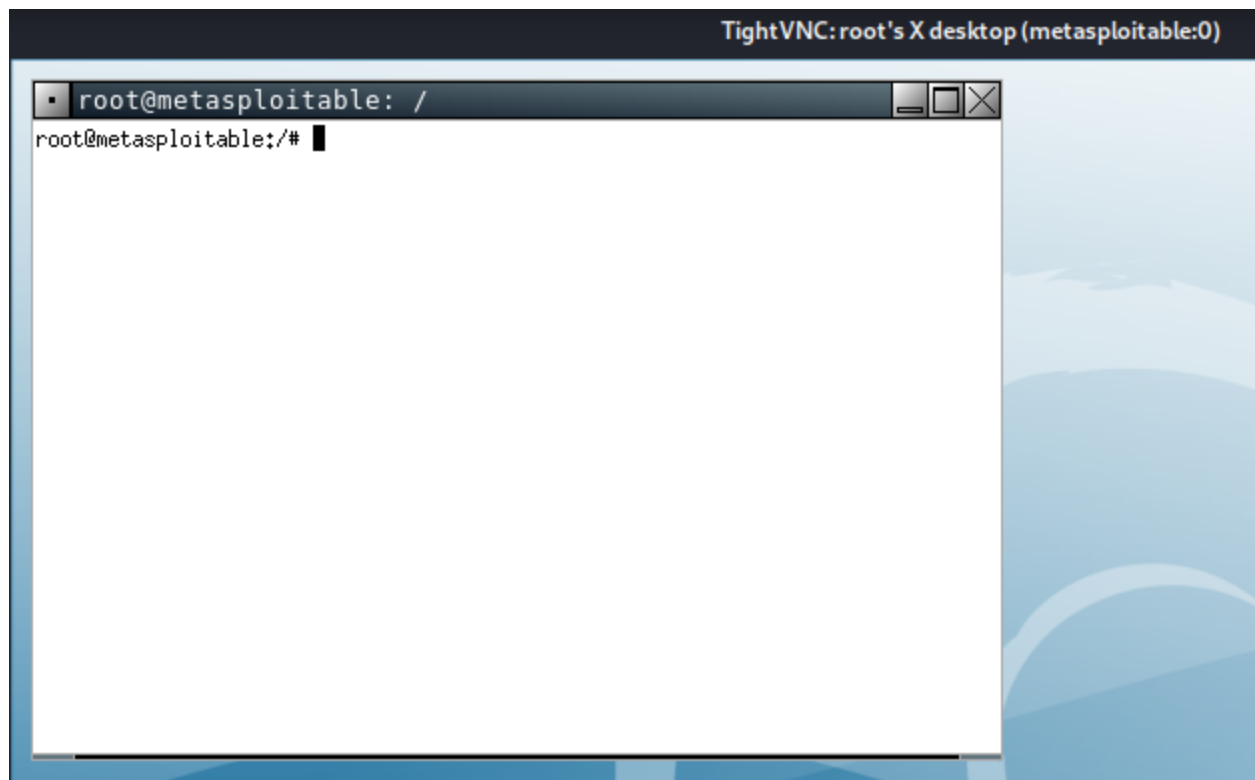
Press enter.



The screenshot shows a terminal window with the following text:

```
File Actions Edit View Help
root@kali:~# vncviewer 10.0.2.11
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password: 
```

You are presented with a remote desktop shell for your Metasploitable2 target.



**End of the Lab!**