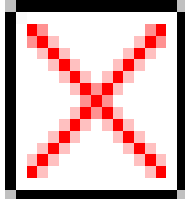


How to Crack SSH, FTP, or Telnet server using Hydra - Ubuntu

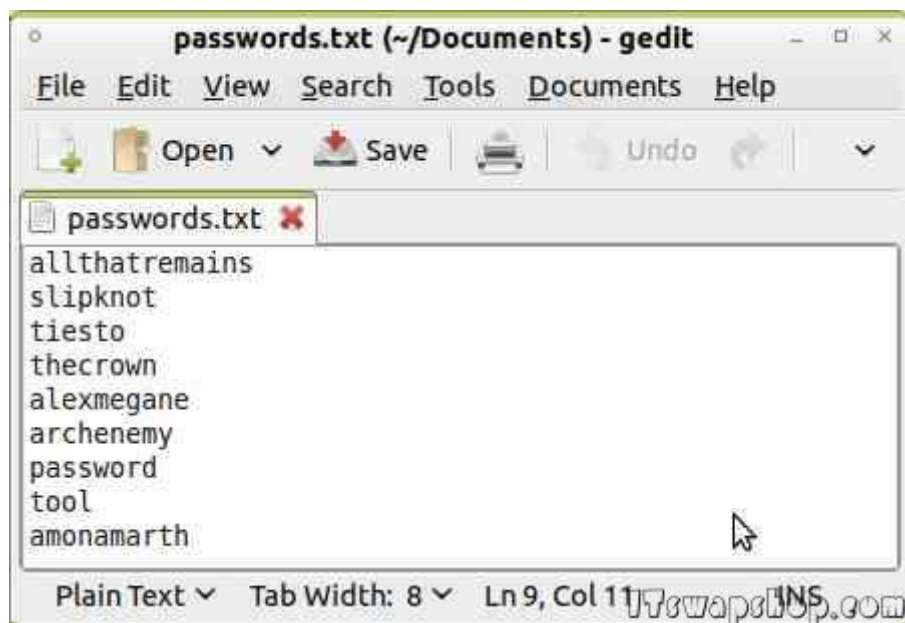
Submitted by ingram on Sat, 08/13/2011 - 5:02pm



Hydra is a tool that makes cracking protocols such as ssh, ftp and telnet relatively easy. In my example, I will be cracking SSH using Hyrda 5.9.1 on Ubuntu 10.10 64 bit (****Update for Ubuntu 12.04** - Replace all references of Hydre 5.9.1 with Hyrda 7.3, which can be downloaded [here](#) [1]). Although this example uses Ubuntu, these commands should work on any Debian based system such as Debian and Linux Mint. Hydra uses password lists to brute force the SSH server. If you need help finding a good password list, check here:

<http://www.google.com/search?aq=f&sourceid=chrome&ie=UTF-8&q=password+list> [2]

Here is what my password list looks like (this is a short list that I made solely for this tutorial):



To begin, we will need to install a few packages:

- **sudo apt-get install libssh-dev nmap build-essential linux-headers-\$(uname -r) libgtk2.0-dev libssl-dev cmake**

I put nmap in there just to do fingerprinting before we attack. Run the following for the nmap

scan:

- **nmap -A -T4 -F 192.168.1.95**

Use the output to confirm that the SSH server is active. You also can see what SSH server it is, what protocol, what port, and what operating system it is running.



Next, we will download and build Hydra:

```
wget http://www.thc.org/releases/hydra-5.9.1-src.tar.gz
```

```
tar -xvzf hydra-5.9.1-src.tar.gz
```

```
cd hydra-5.9.1-src
```

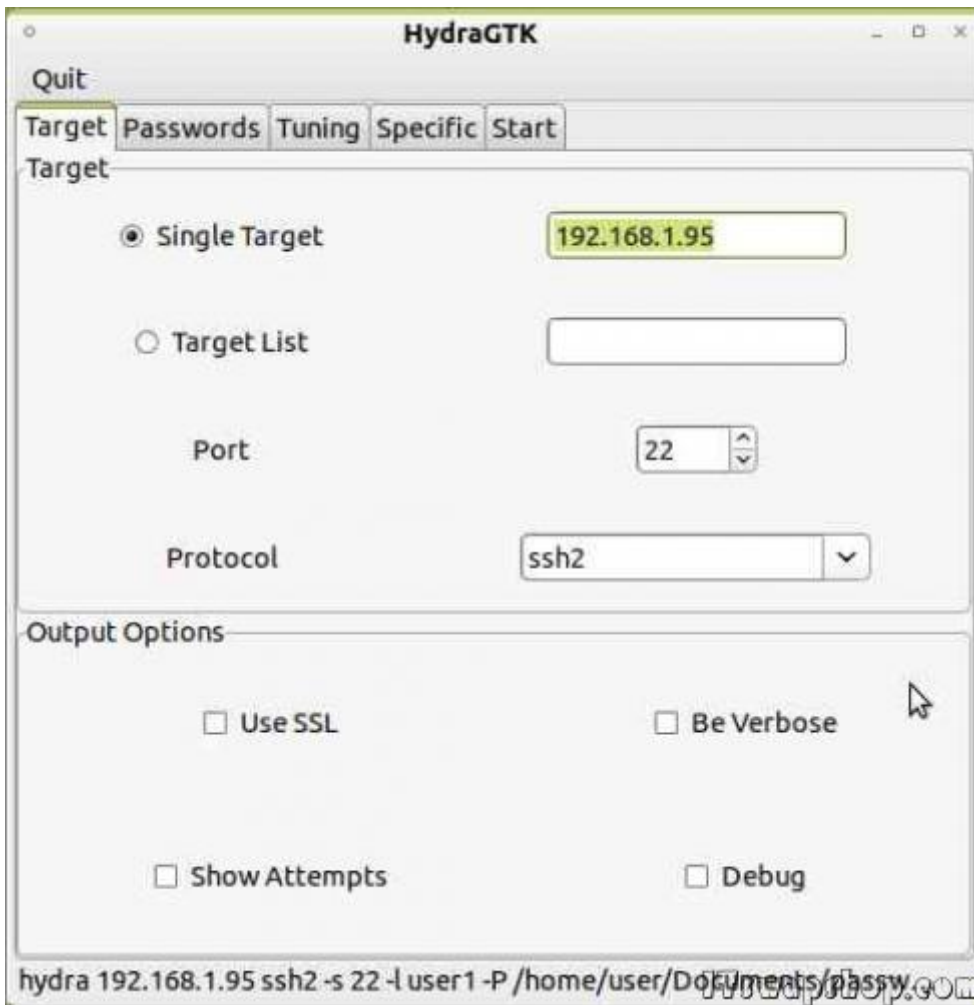
```
./configure
```

```
make
```

```
sudo make install
```

If Hydra installed successfully, press Alt + F2 to bring up the Run menu. Type “xhydra”, the gui for Hyrda, and press enter.

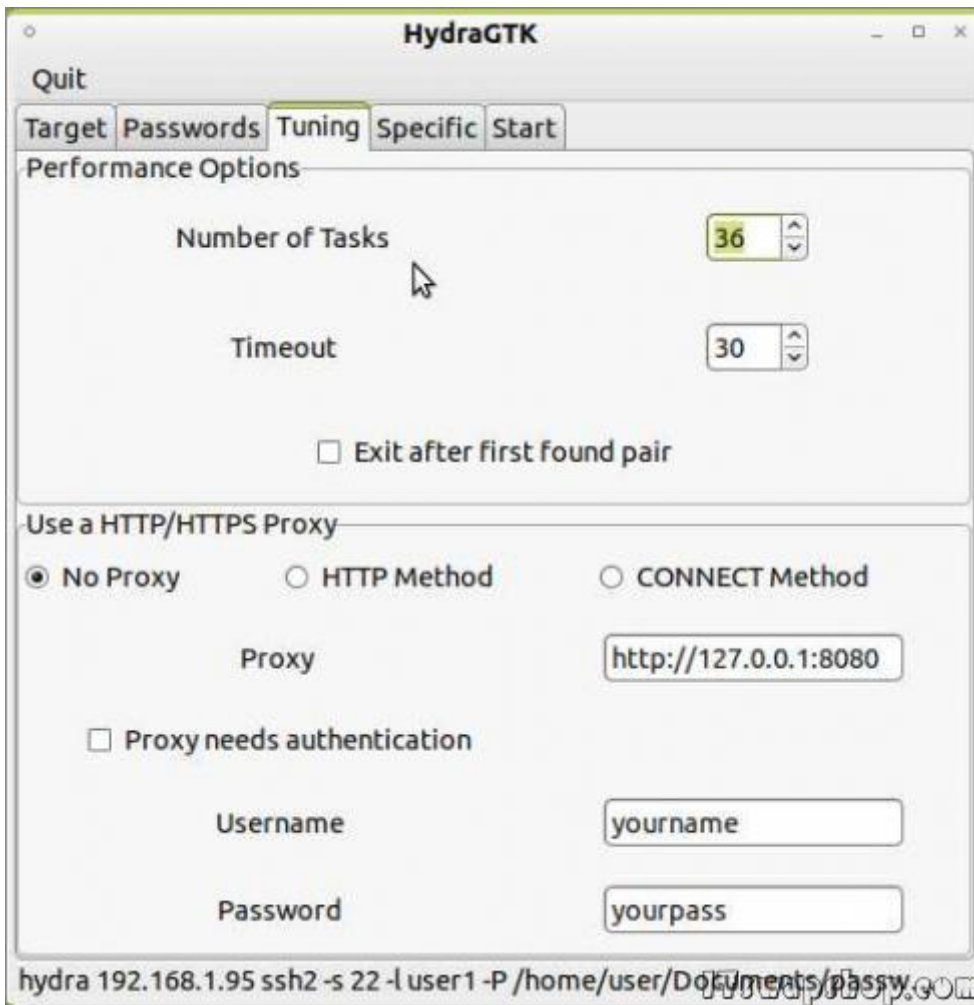
On the Target tab, enter the IP address or hostname of the SSH server, the port, and the Protocol.



On the Passwords tab, select the username (yes, you must know the username, unless you want to use a username list), check the "Password List" button, then choose the path to your password list.



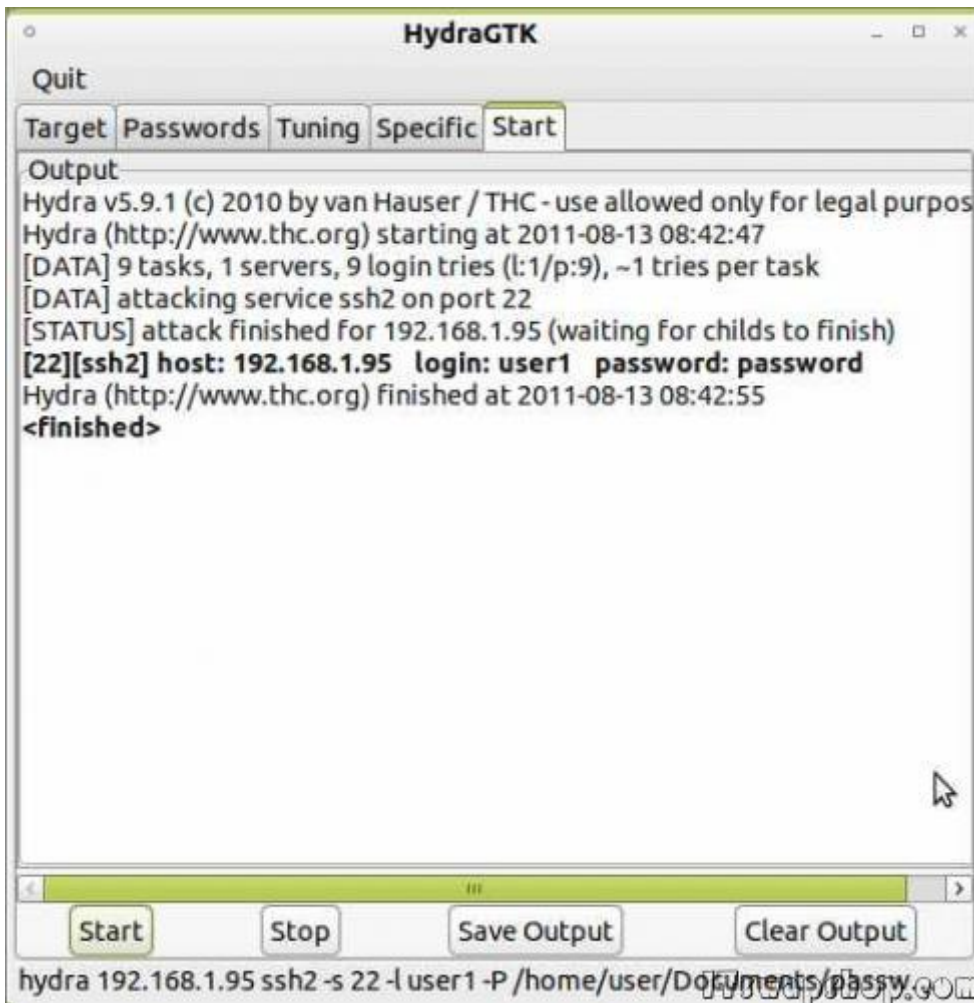
On the Tuning tab, you can select the number of tasks and the timeout time. I left mine at default, but you may need to edit these if you have trouble with the attack.



On the Start tab, click on Start and watch the output.



Once it finds a password match (if it finds one), it will be highlighted in black.



As you can see, it is quite easy to perform a brute force attack on an SSH server using Hydra. Hydra works with much more than SSH though. You can use Hydra to perform a brute force attack on FTP, Telnet, and POP3 servers, just to name a few. Remember, don't run these attacks on anything other than your own servers.

[Privacy Policy](#)

support @ itswapshop . com

Source URL: <http://itswapshop.com/content/how-crack-ssh-ftp-or-telnet-server-using-hydra-ubuntu>

Links:

[1] <http://www.thc.org/releases/hydra-7.3.tar.gz>

[2] <http://www.google.com/search?aq=f&sourceid=chrome&ie=UTF-8&q=password+list>