Brute Force attacks [VM is required]

In this experiment you will use the software THC Hydra via the GUI version called Hydra-GTK. Run Hydra on your VM by issuing the following commands in a terminal:

```
$ sudo xhydra
```

Using the graphical interface, you can easily customize the brute force attempts.
Exchange IP-addresses with another group if you haven't already (previous assignment).
After opening the program, locate the **target** tab and set the following parameters.

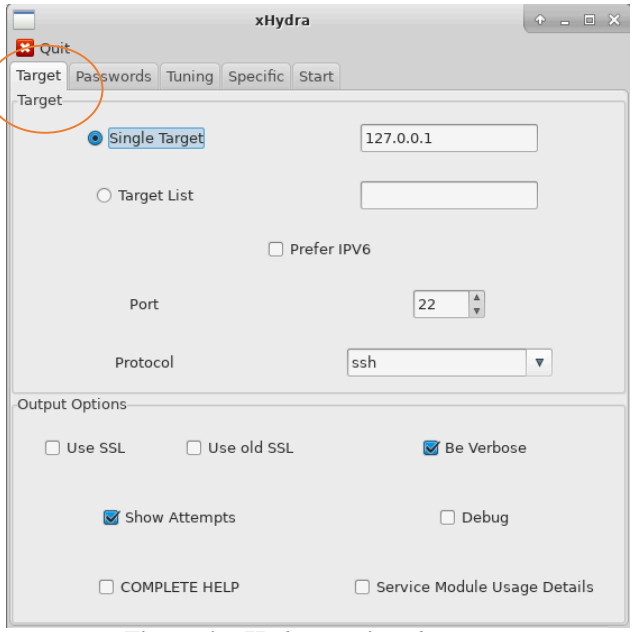

Figure 1. xHydra: setting the target.

Target Tab

Single Target – <TARGET IP>
Port – 22
Protocol - SSH
Be Verbose – Checked
Show Attempts – Checked

After you have defined the target and the protocol that will be used in the login attempts, it's important to set the target user and the password dictionary that will be used in the attack.

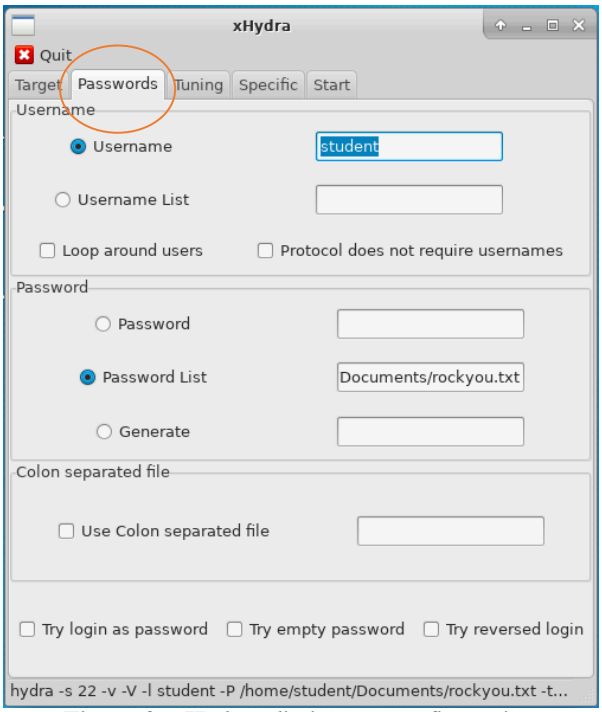

Figure 2. xHydra: dictionary configuration.

Passwords Tab

Username – **student** (target user name presents on VM)
Password List – custom password list file

We will use a popular password list that is already on the Linux Virtual machine called **rockyou.txt**. You can find it under**:**

/home/student/Documents/

It is compressed using the "bzip2" utility. Read the manual page to find out how to decompress the file:
$ man bzip2

We also want to check "**Try login as password**" and "**Try empty password**" out of good habit.

Next, you can define another customization, such as, ask to the program to stop the login attempts as soon as one password is successfully discovered.

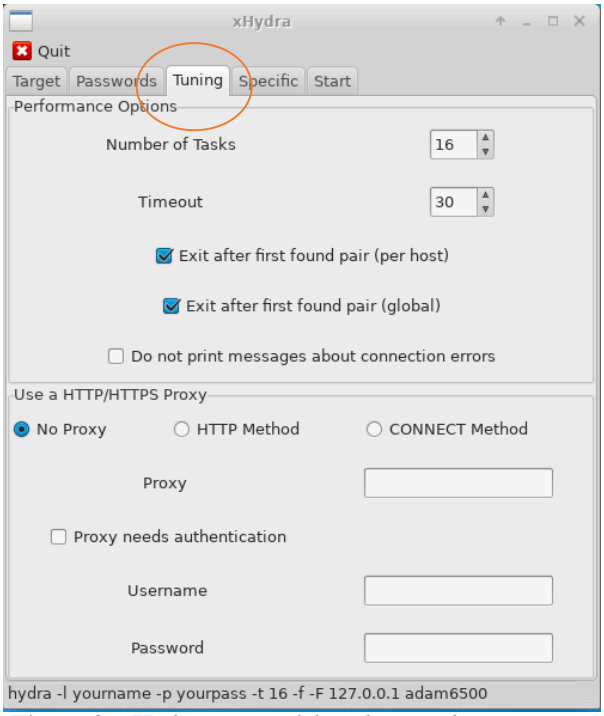

Figure 3. xHydra: customizing the attack parameters.

Tuning Tab

Make sure "**Exit after first found pair**" is checked.

Finally, we can start the attack! Go to the **start** tab and select **Start** to begin the attempts (Figure 4). After launching the attack, you can see the login attempts happening in parallel, using the passwords from the dictionary file.

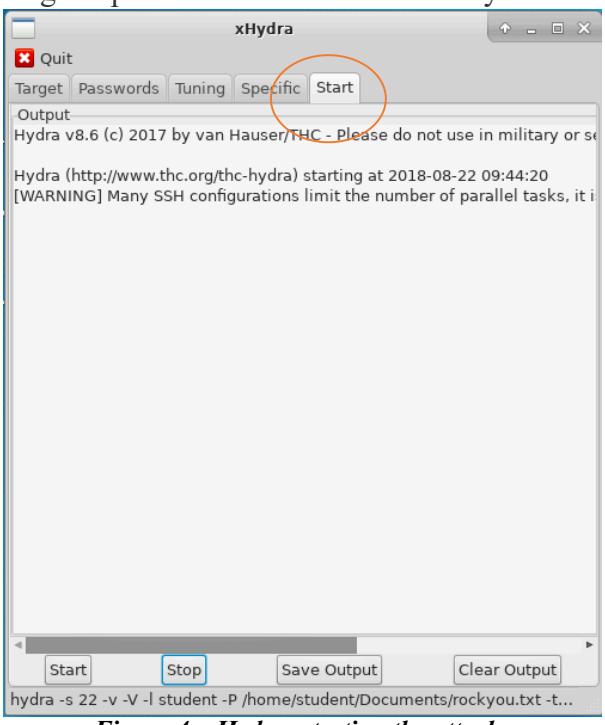

Figure 4. xHydra: starting the attack.

Tab Start

Starts the brute force
Stop – Stops the brute force
Save Output – checked