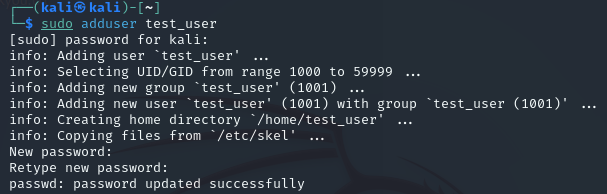
**Authentication Cracking with Hydra.**

**Tasks:** 1) Enable and set up the SSH service and crack its authentication process.

2) Enable and set up a service of choice and crack its authentication process.

Let’s start with task number 1.

We’re going to create a new user in Kali.



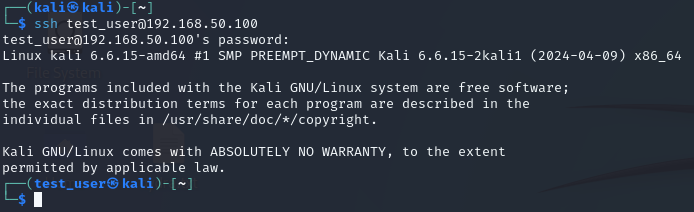
From here, we’re going to activate the **SSH Service**.



If we wanted to change the parameters and configuration of the service, we would go into the **/etc/ssh directory** where we would find the **sshd\_config** file.

If we open that file, we can change the values of the daemon such as port, authentication permissions, authentication retries and so on and on. For the purpose of this task, we won’t change anything.

Now we’re going to see if the ssh service connection with the new user is up and running correctly on our machine.



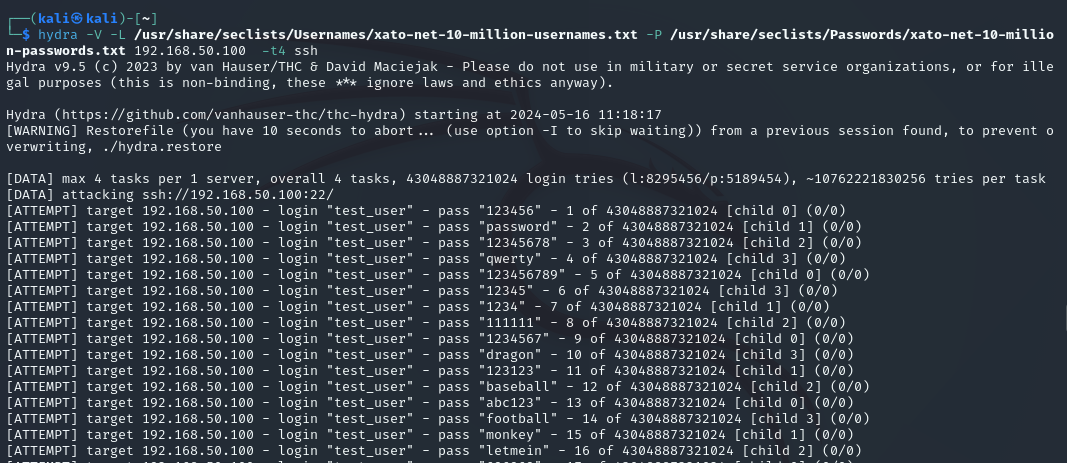
With the line **ssh test\_username@ip**, we’re asked to enter the password of the user. After we do that, we can see that  **test\_user is now accessing the terminal**.

So now we know that the service runs. Now we’re going to use Hydra to crack the authentication process.

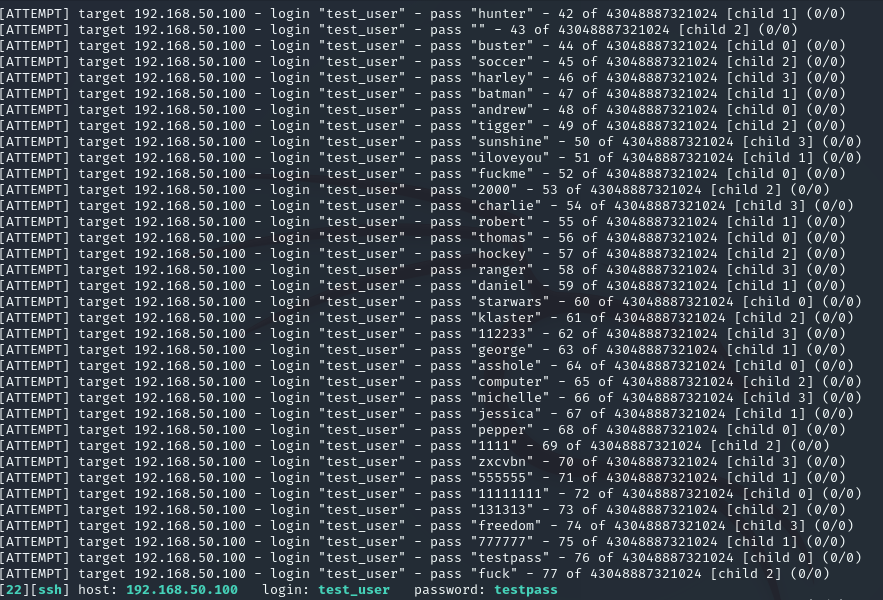
We’ll ’use this command:

**hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.100 -t 4 ssh**

The switch -V means verbose so we’ll see step by step every approach the Hydra program will take to crack username and password. The switch -L lets us use a txt file for the username while -P lets use a txt file for the passwords. Here we’ll use the **xato 10 million username list** and the **xato 10 million password list** we got from Seclist. Then we’ll put the target IP and then the -t 4 switch to help us limit the parallel tasks that the program runs. In the end we put the service name then we hit enter and start the cracking.



We’ll see that the program will find the matching username and password in a matter of minutes.

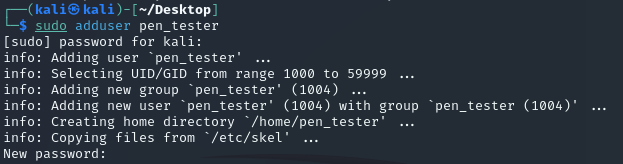


Now we’ll proceed with the second task.

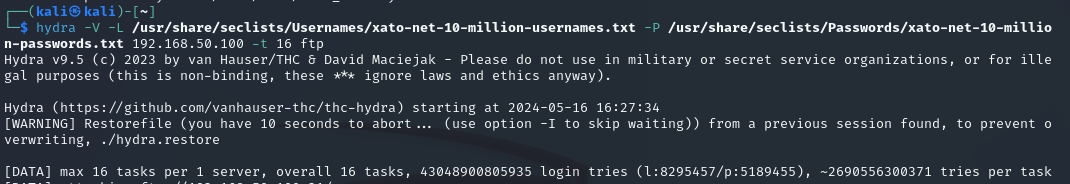
We’ll set up another service and we’ll crack its authentication process.



Now that we have confirmed that the service is up and running, we’ll add a new user to it.



New user is up and we linked it with ftp. Now we’re going to use hydra to find the user and the password using the same command with the same lists we used earlier. But this time we’ll use the switch -t 16, because the ftp protocol doesn’t limit the parallel task the program can run.



And we’ll have the user and the password in just a few minutes.

