PASSWORD CRACKING

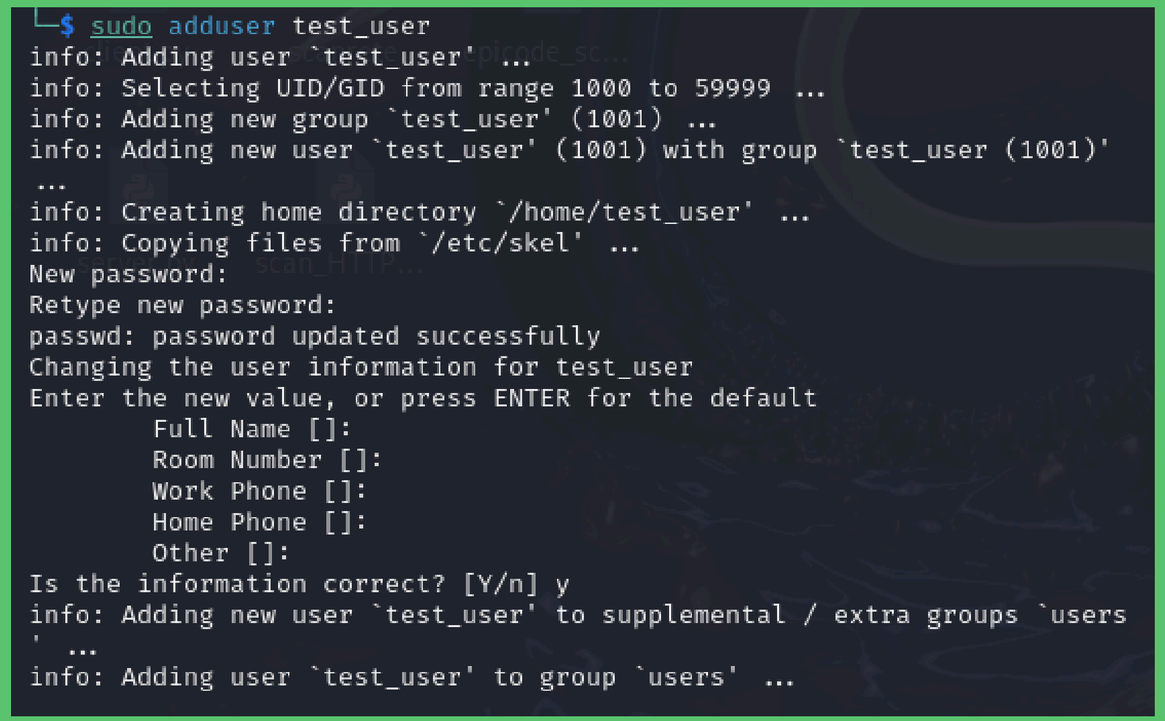
Morgan Petrelli S6L4

L’ESERCIZIO DI OGGI HA UN DUPLICE SCOPO:

- FARE PRATICA CON HYDRA PER CRACCARE L’AUTENTICAZIONE DEI SERVIZI DI RETE.
- CONSOLIDARE LE CONOSCENZE DEI SERVIZI STESSI TRAMITE LA LORO CONFIGURAZIONE.

L’ESERCIZIO SI SVILUPPERÀ IN DUE FASI:

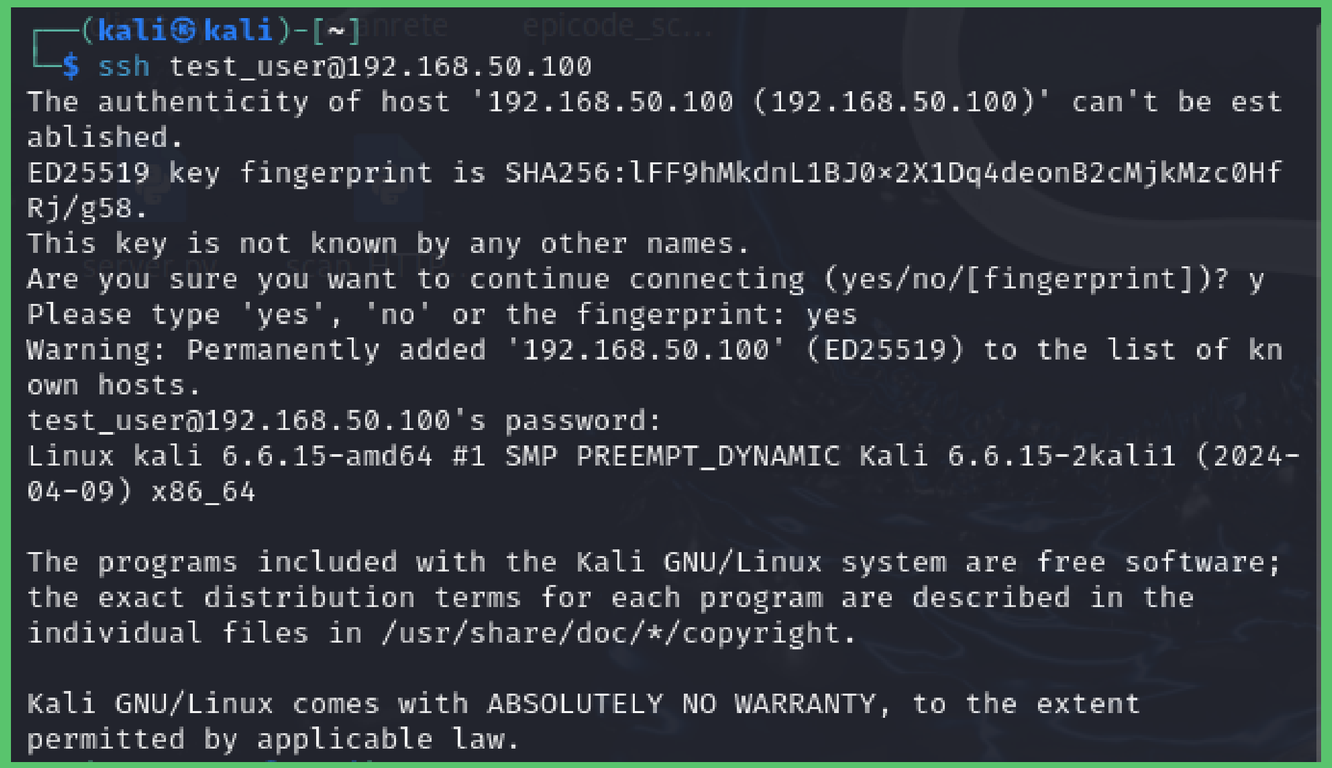
- UNA PRIMA FASE DOVE INSIEME VEDREMO L’ABILITAZIONE DI UN SERVIZIO SSH E LA RELATIVA SESSIONE DI CRACKING DELL’AUTENTICAZIONE CON HYDRA.
- UNA SECONDA FASE DOVE SARETE LIBERI DI CONFIGURARE E CRACCARE UN QUALSIASI SERVIZIO DI RETE TRA QUELLI DISPONIBILI, AD ESEMPIO FTP, RDP, TELNET, AUTENTICAZIONE HTTP.



HO INIZIATO CREANDO UN NUOVO UTENTE CON IL COMANDO SUDO ADDUSER E HO ASSEGNATO UN USERNAME “TEST_USER” E UNA PASSWORD “TESTPASS”

con il comando sudo service ssh start ho attivato il servizio ssh.
in seguito con il comando sudo nano /etc/ssh/sshd_config ho aperto il file di configurazione del servizio

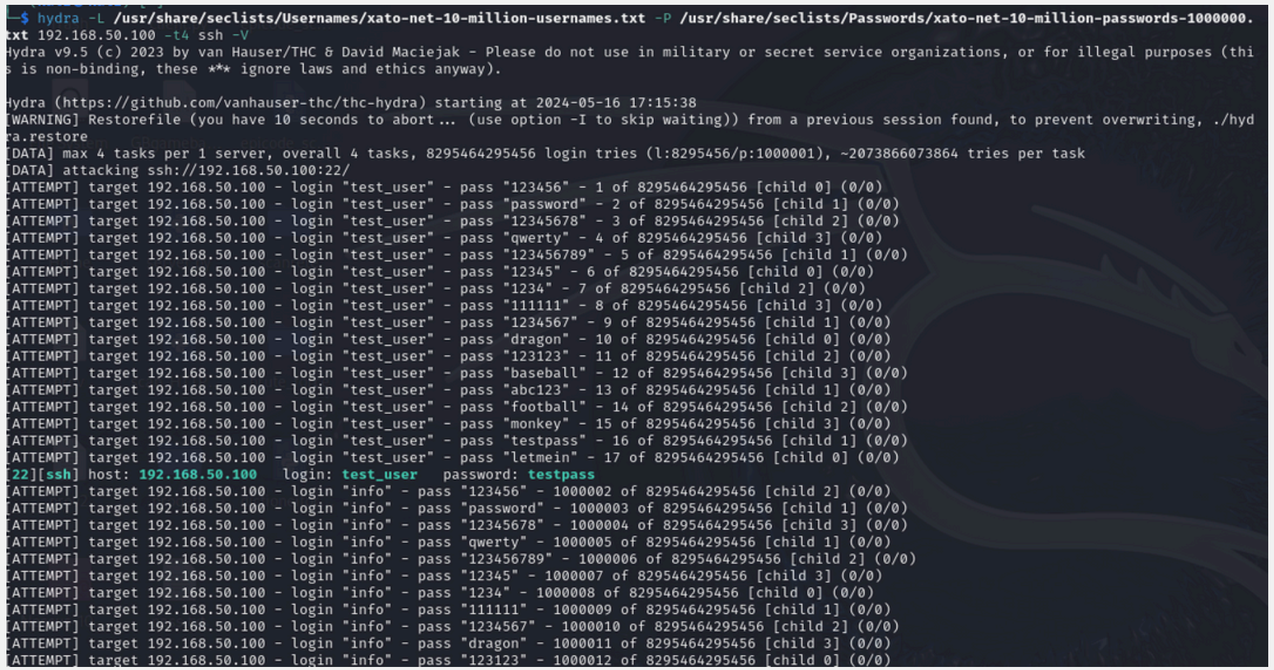
ho usato il comando ssh test_user@193.168.50.100 per verificare la connessione in ssh dell’utente creato, inserendo le credenziali riceveremo il prompt dei comandi del utente creato



USO DI HYDRA PER CRACK DELLA PASSWORD

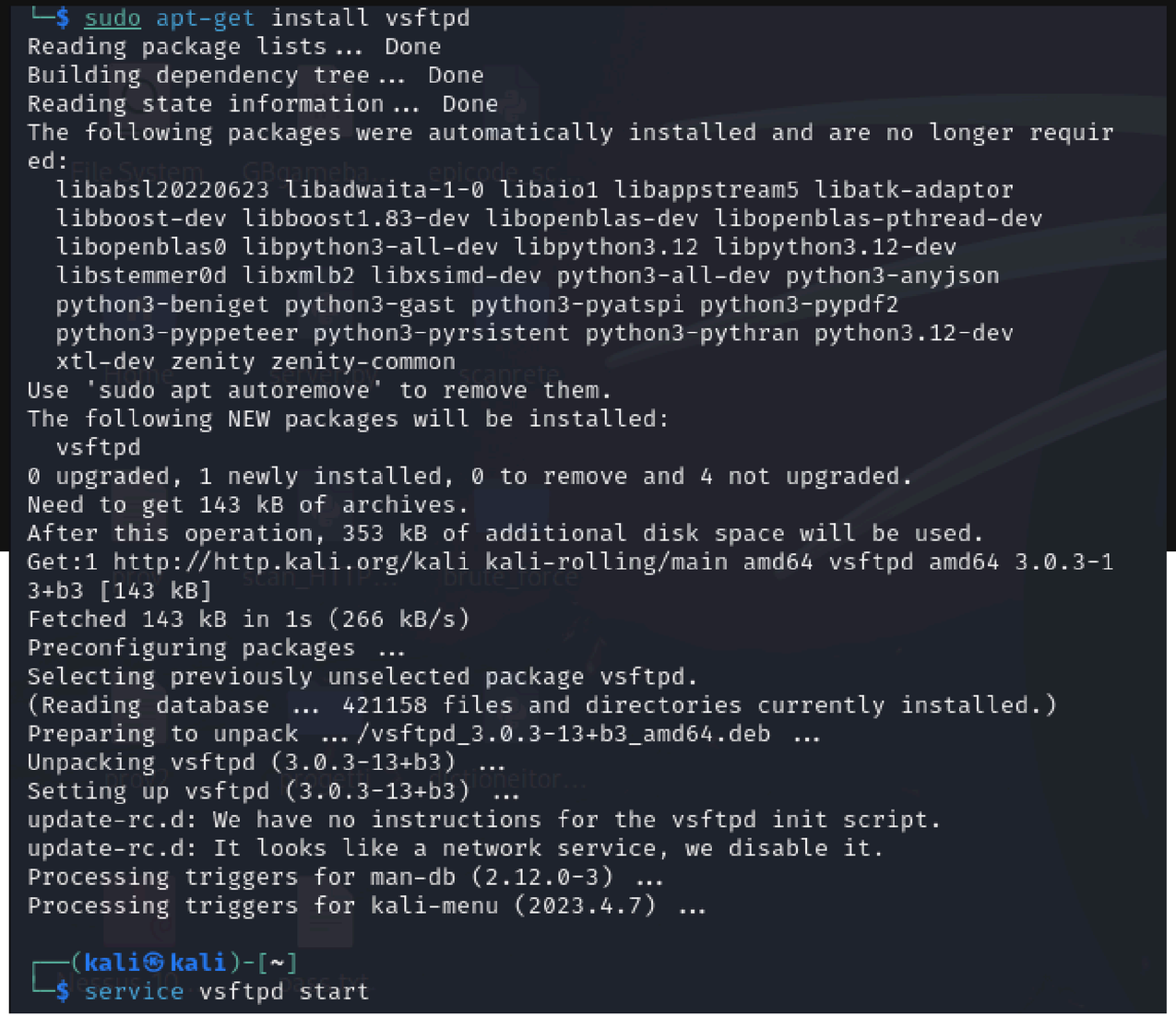
ho usato il comando hydra -L lista_username -P lista_password INDIRIZZO_IP -t 4 ssh -V con il quale Hydra utilizzerà l'elenco di nomi utente e l'elenco di password forniti per provare diverse combinazioni nel tentativo di ottenere l’accesso.

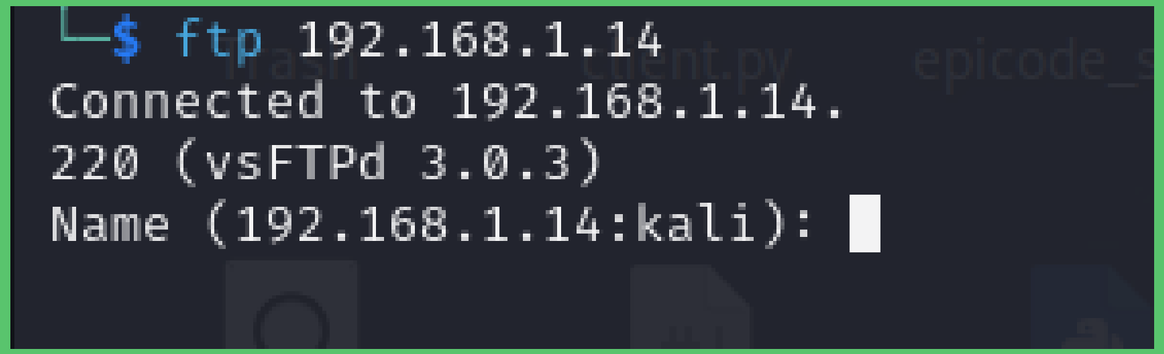
Come si può vedere dopo pochi minuti essendo password molto facili è riuscito a trovare user e password



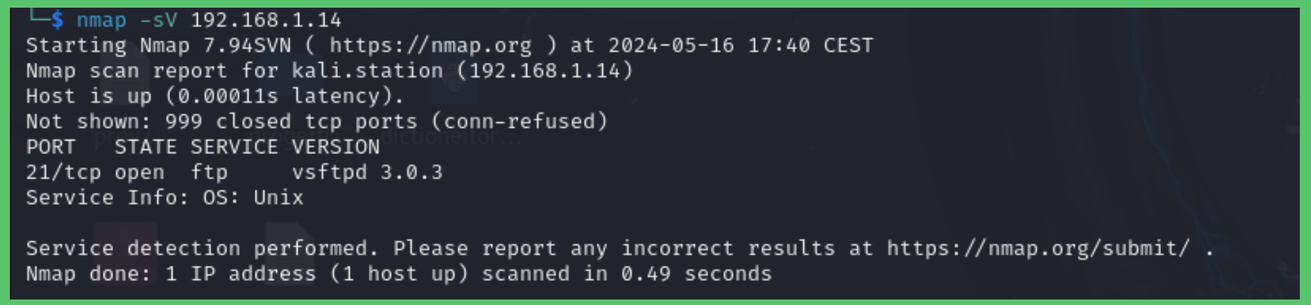
per la seconda fase dell’esercizio ho iniziato installando il server FTP

in seguito ho startato il servizio

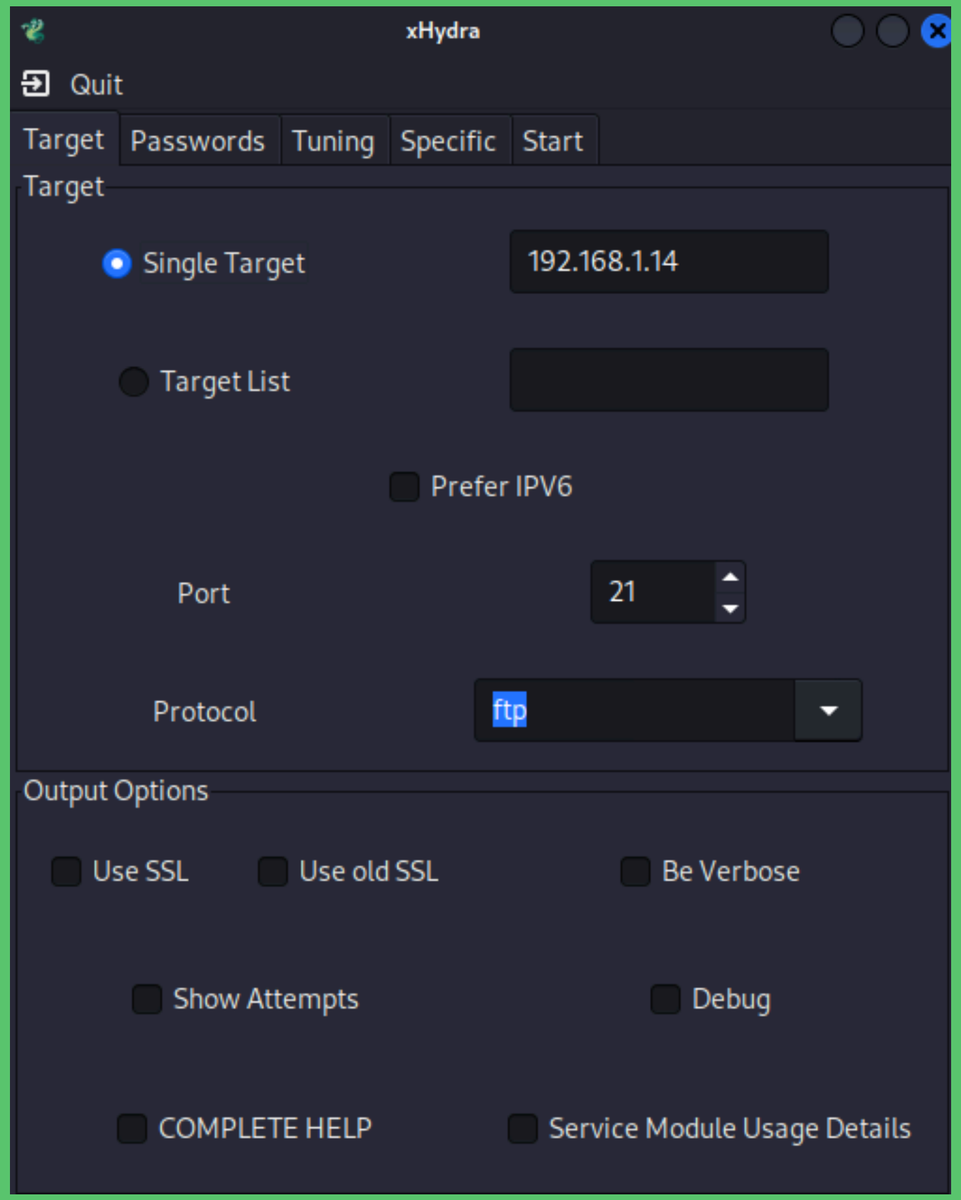




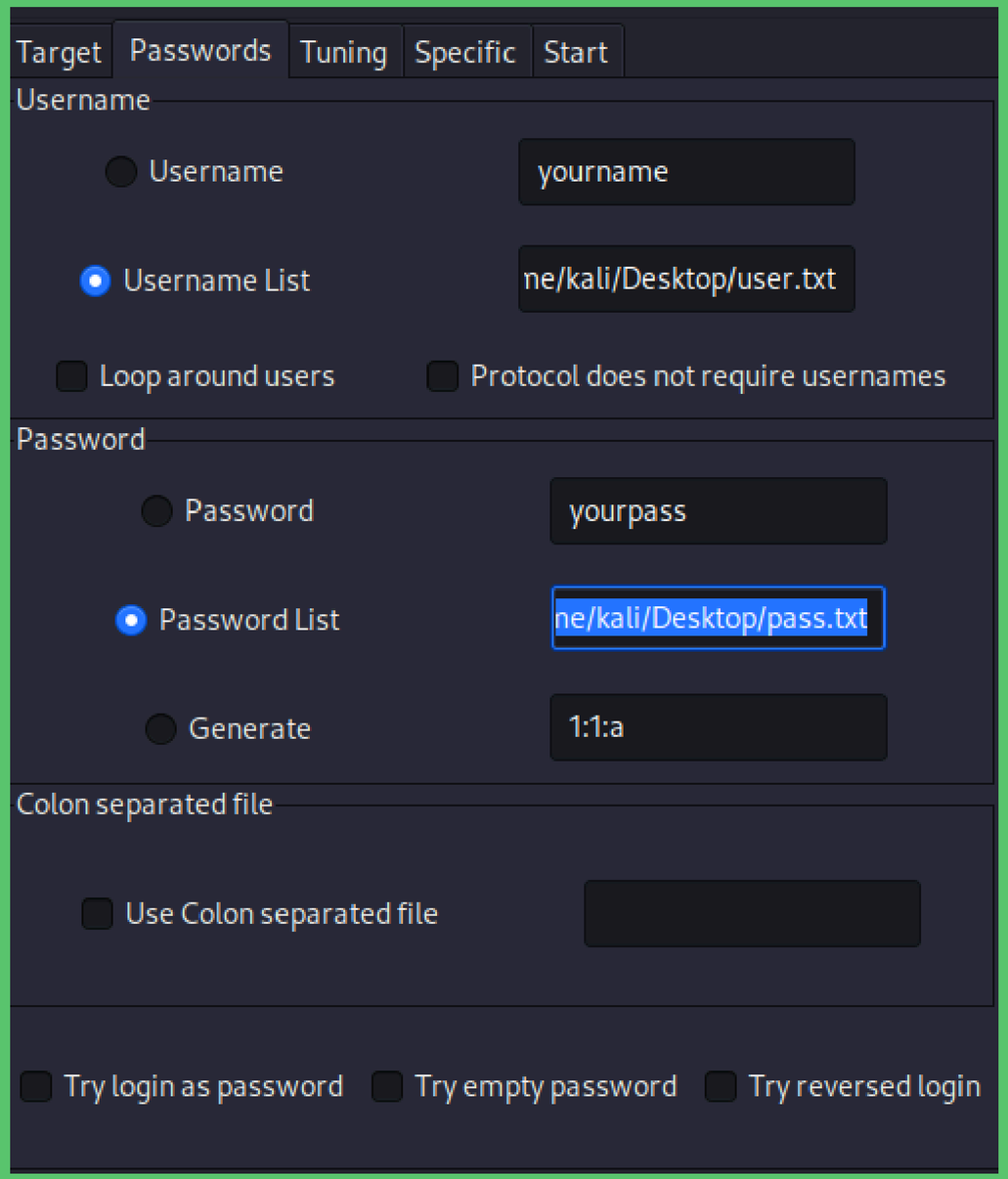
ho verificato che effettivamente il servizio fosse attivo



ho usato nmap per vedere la porta su cui gira il servizio che mi sarà utile per Hydra



ho aperto Hydra versione grafica.
Nella pagina “Target” ho inserito l’IP, la porta e il tipo di servizio che Hydra dovrà cercare di craccare l’autentificazione



nella pagina “Password” ho inserito la wordlist (ho creato una lista con poche parole altrimenti il processo sarebbe potuto durare ore) su cui Hydra si baserà per craccare l’user e la password

Target | Passwords | Tuning | Specific | Start

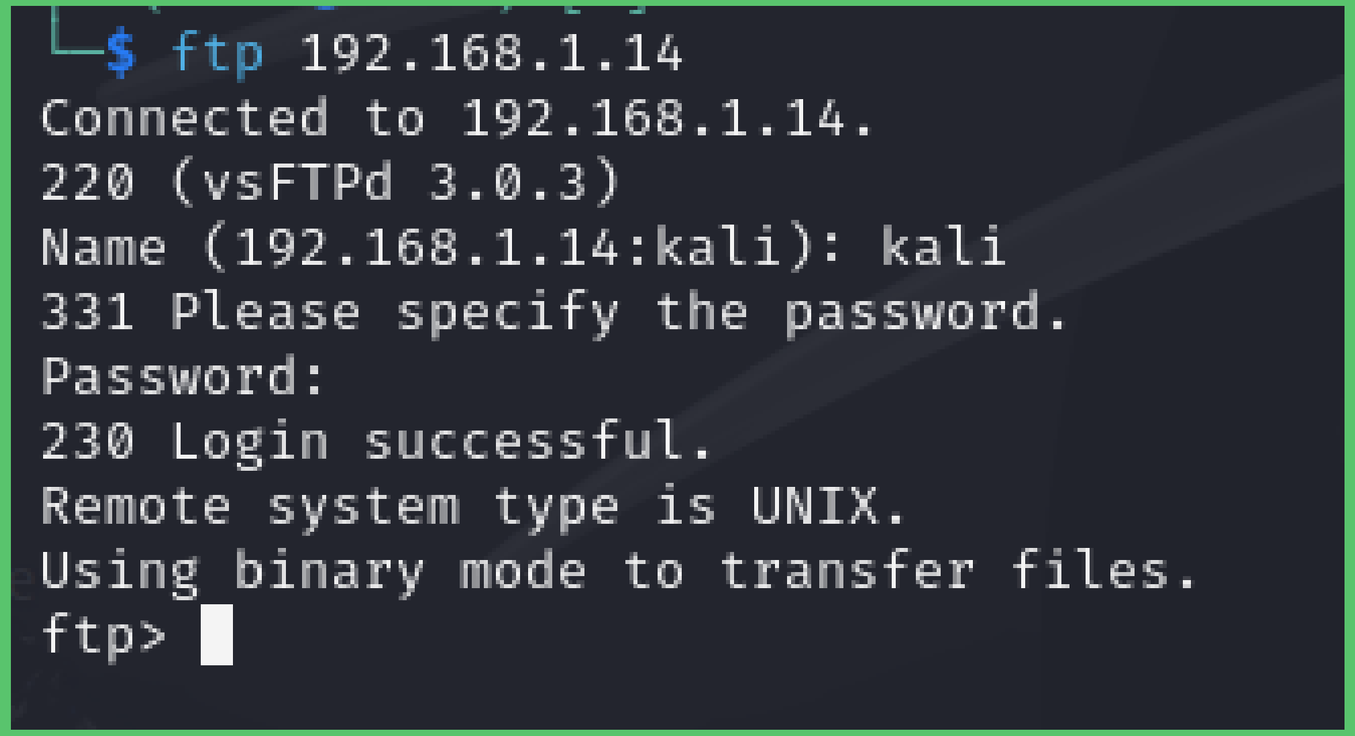
Output

```
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 2024-05-16 17:52:26
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
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 2024-05-16 17:52:34
[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, 108 login tries (l:12/p:9), ~7 tries per task
[DATA] attacking ftp://192.168.1.14:21/
[21][ftp] host: 192.168.1.14   login: kali   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 17:53:08
<finished>
```

dopo poco Hydra ci mostra in output l'user e la password



provando ad inserire le credenziali verifichiamo che effettivamente siano giuste