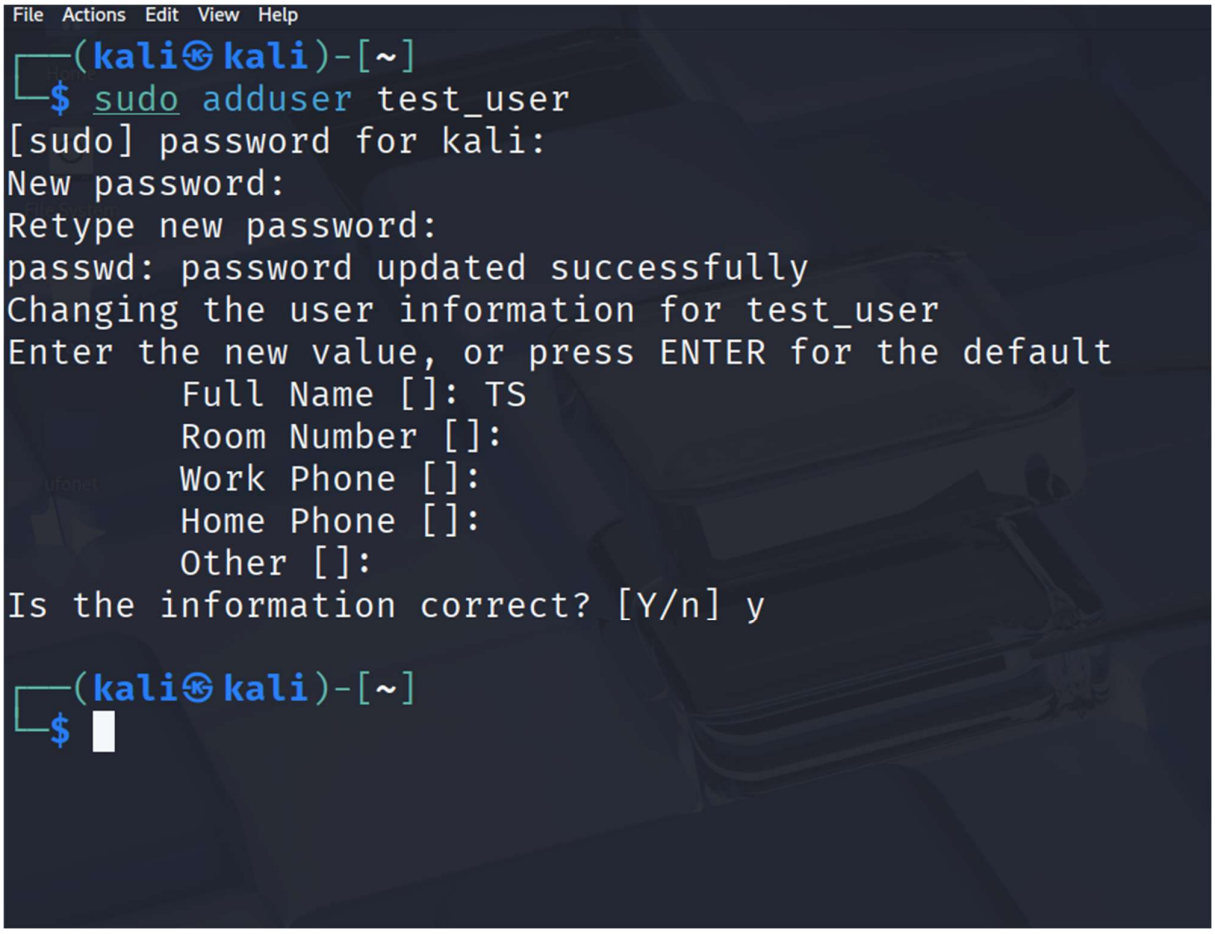
Esercizio S6L5

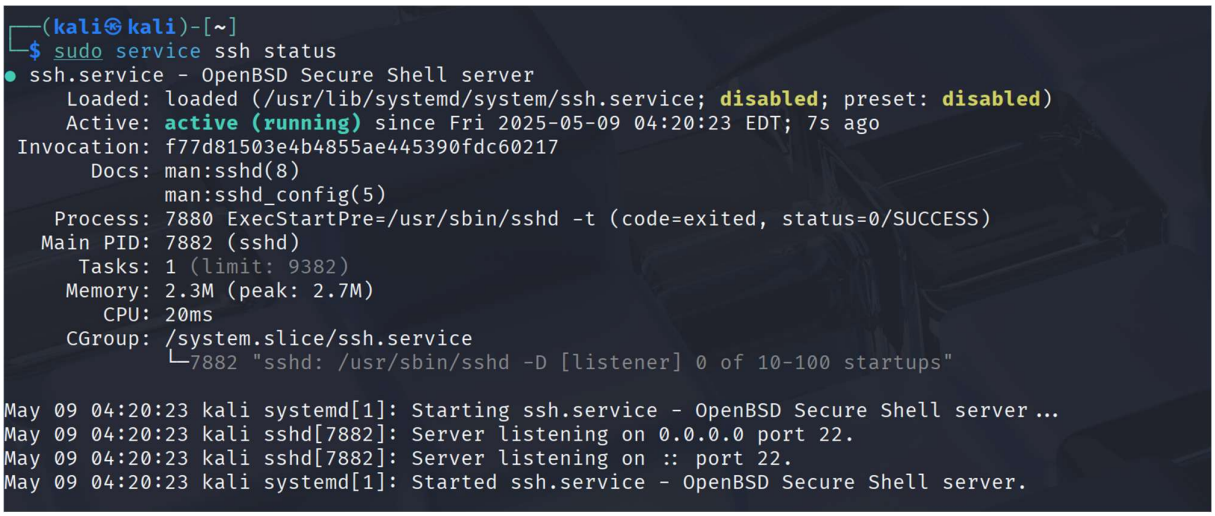
CONFIGURAZIONE E CRACKING SSH

Creiamo un nuovo utente su Kali Linux, con il comando «adduser».

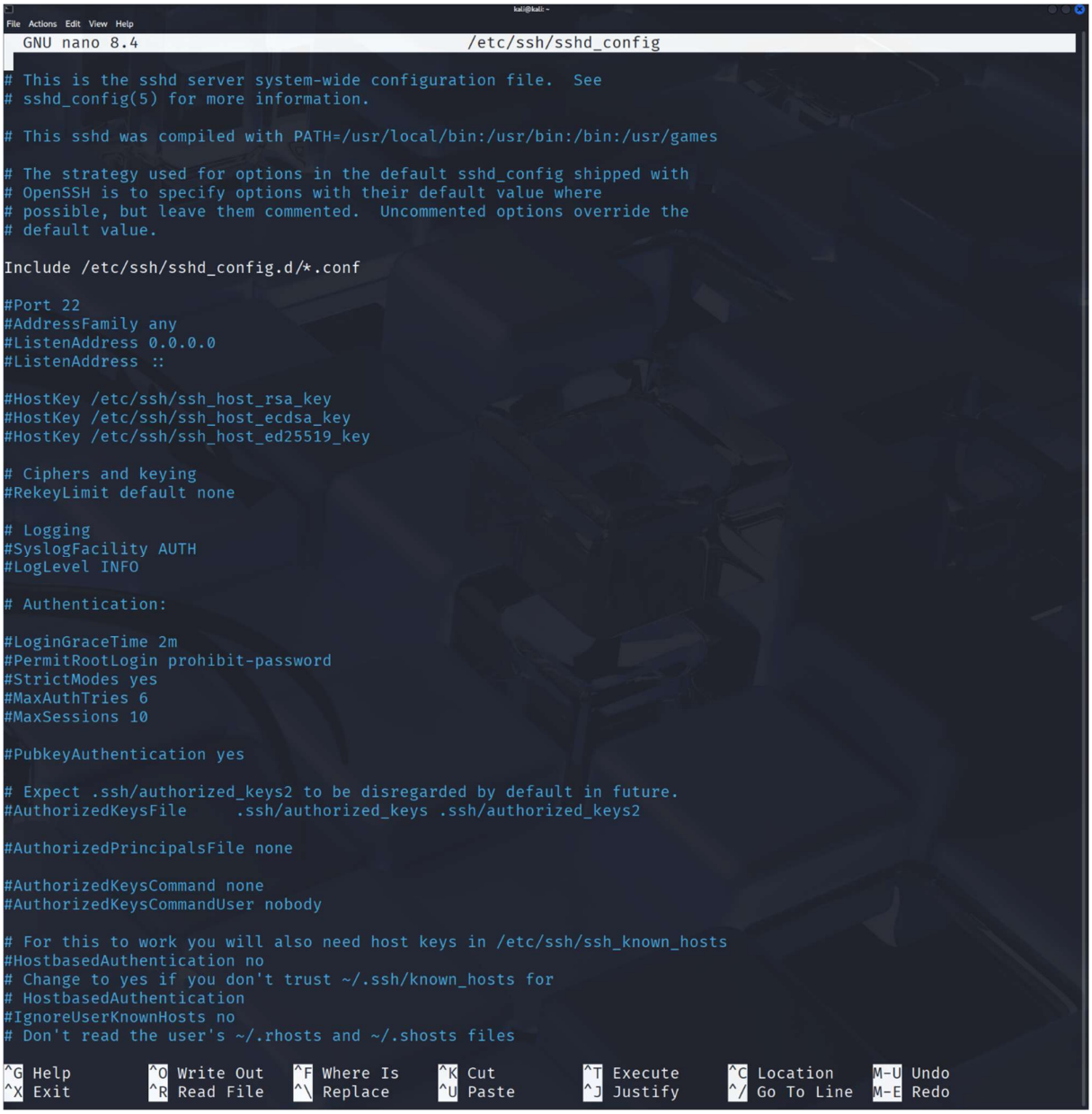
Chiamiamo l'utente test_user, e configuriamo una password iniziale testpass



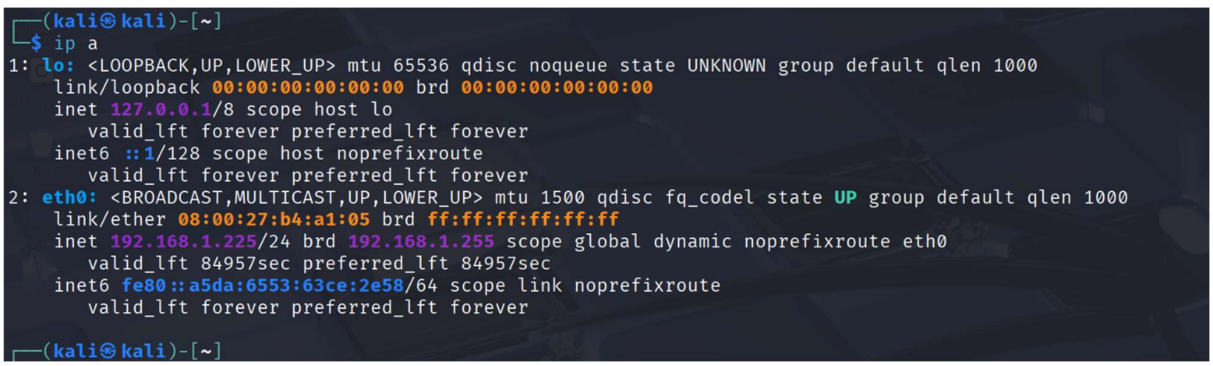
Attiviamo il servizio ssh con il comando sudo service ssh start e controlliamo che il servizio sia attivo



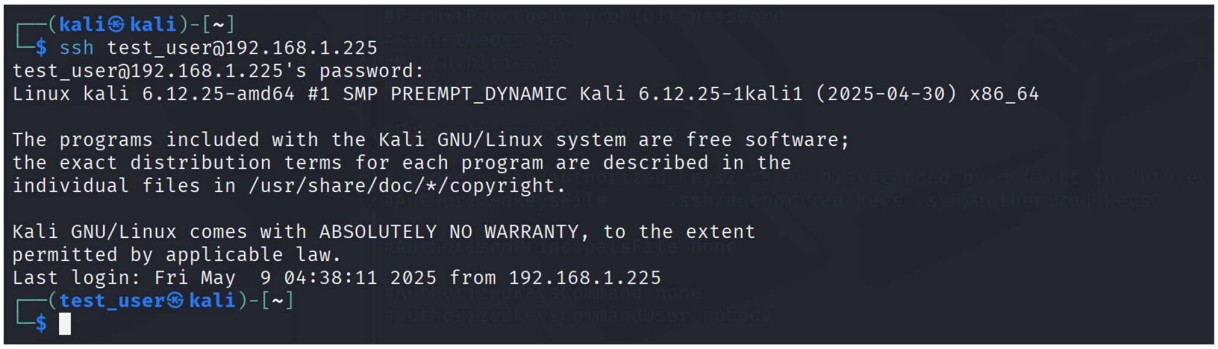
Apro il file di configurazione usando “sudo nano /etc/ssh/sshd_config”



Ai fini dell’esercizio lasciamo il file così e procediamo controllando l’indirizzo IP della Kali digitando “ip a”



Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: ssh test_user@192.168.1.255

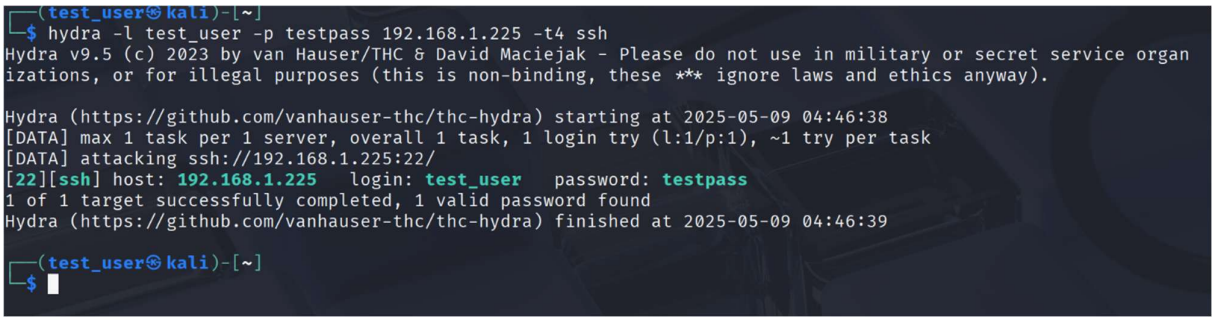


la connessione SSH è andata a buon fine. Sono stato in grado di autenticarmi come utente test_user con indirizzo IP 192.168.1.225.

Il prompt dei comandi è cambiato da kali@kali a test_user@kali, il che indica che ora sono loggato come test_user

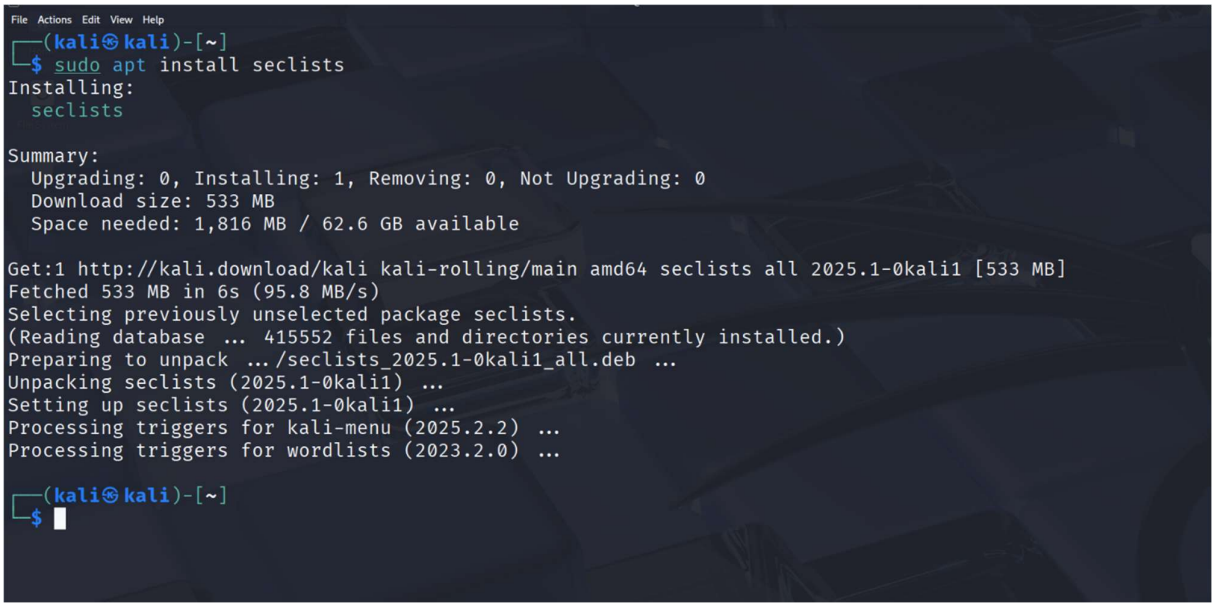
Questo dimostra che Il servizio SSH è attivo e funzionante, l'utente test_user è stato creato correttamente ed è abilitato per l'accesso tramite SSH, la password impostata è corretta.

A questo punto, avendo verificato l'accesso, non ci resta che configurare Hydra per una sessione di cracking. Ovviamente in questo esercizio conosciamo già l'utente e la password per accedere, ma soffermiamoci sulla sintassi di Hydra per ora:

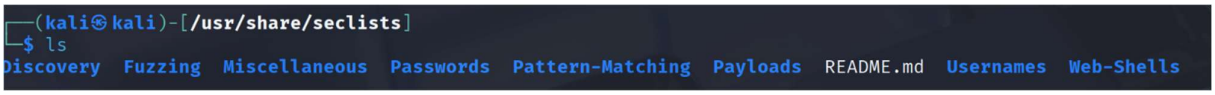


Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario.

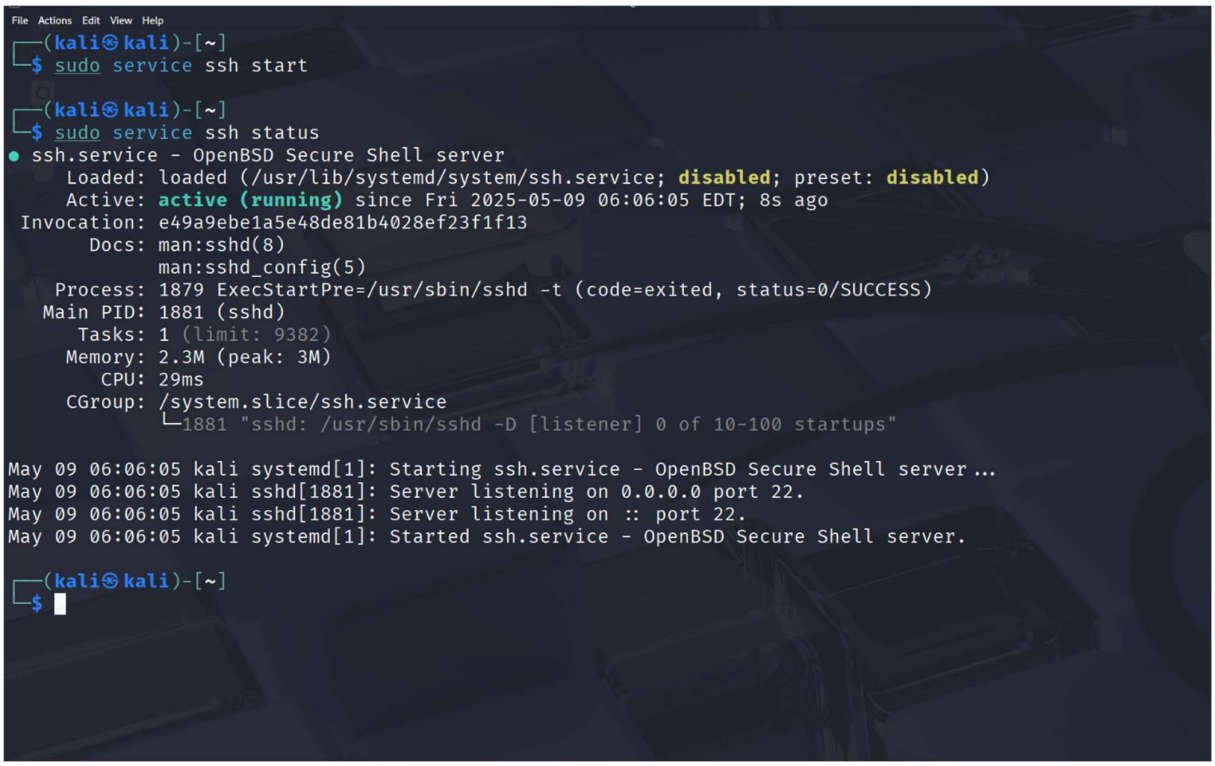
Installiamo seclist



Controllo le directory appena create



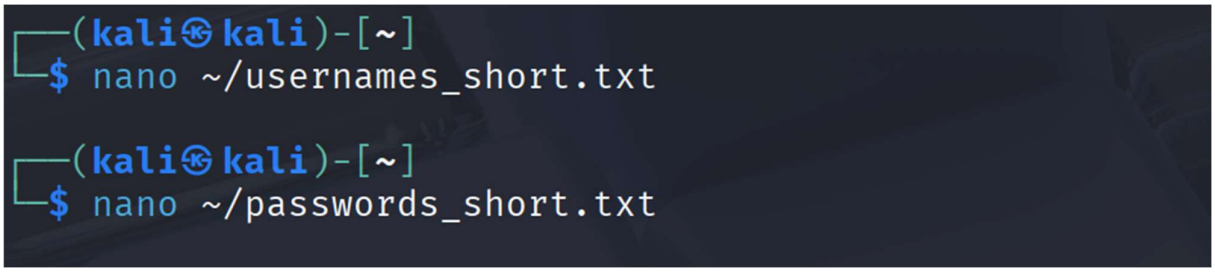
Modifico i file di username e password per essere più snelli limitandomi a 1001 righe ciascuno e facendo attenzione che in entrambi sia presente il corrispettivo dell'utente in oggetto di simulazione.



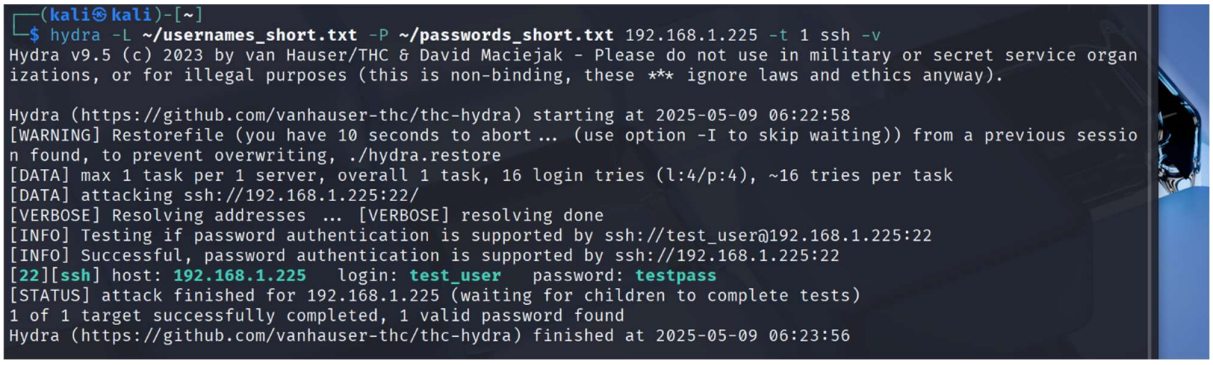
Hydra è ora in esecuzione e sta tentando le combinazioni di username e password.

I messaggi [STATUS] indicano che sta effettuando tentativi di login contro il servizio SSH su 192.168.1.225.

Per abbreviare i l tempo del test creo i file usernames_short.txt e passwords_short.txt con solo quattro variabili tra cui quella vera



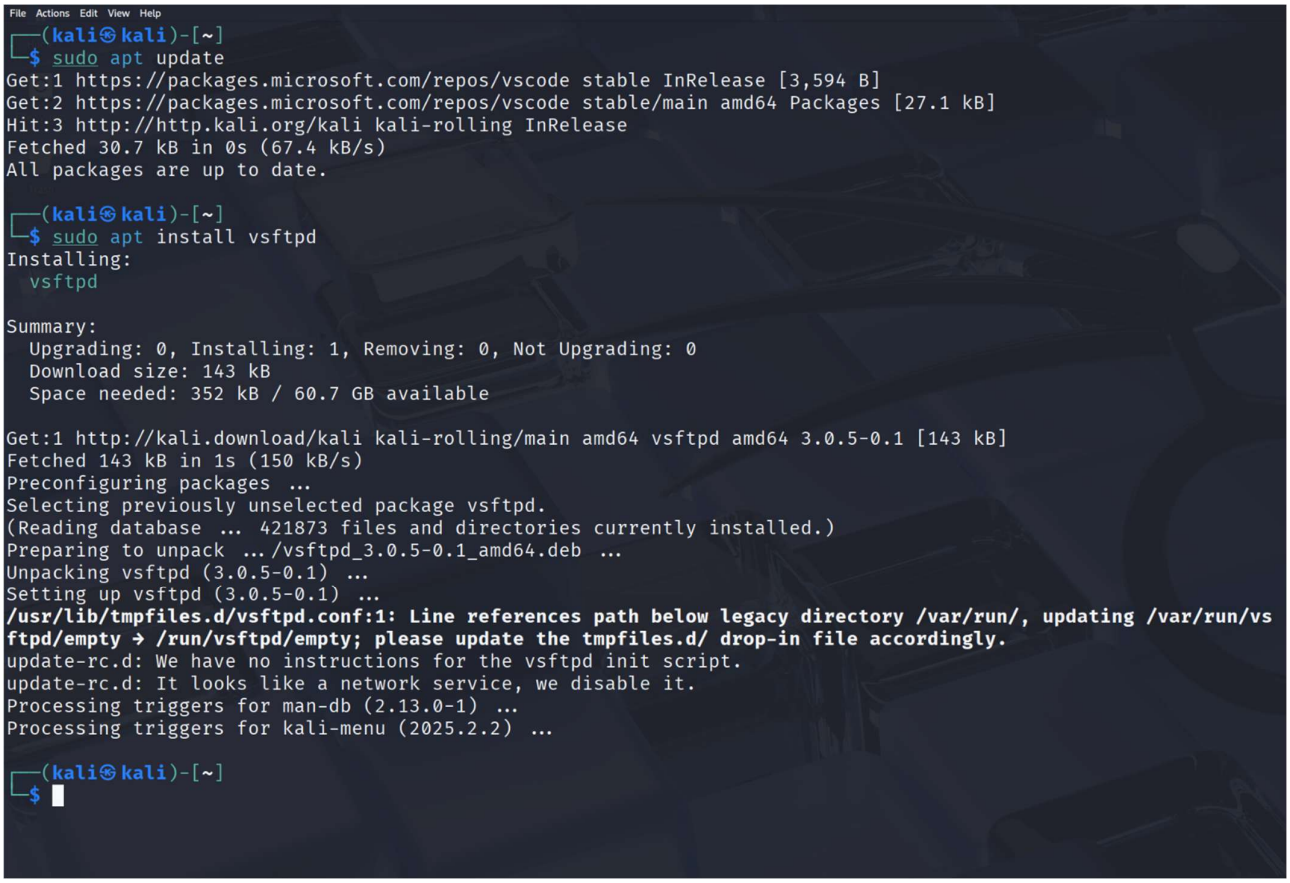
Avvio Nuovamente Hyda che, in un tempo accettabile, trova user e pass richieste



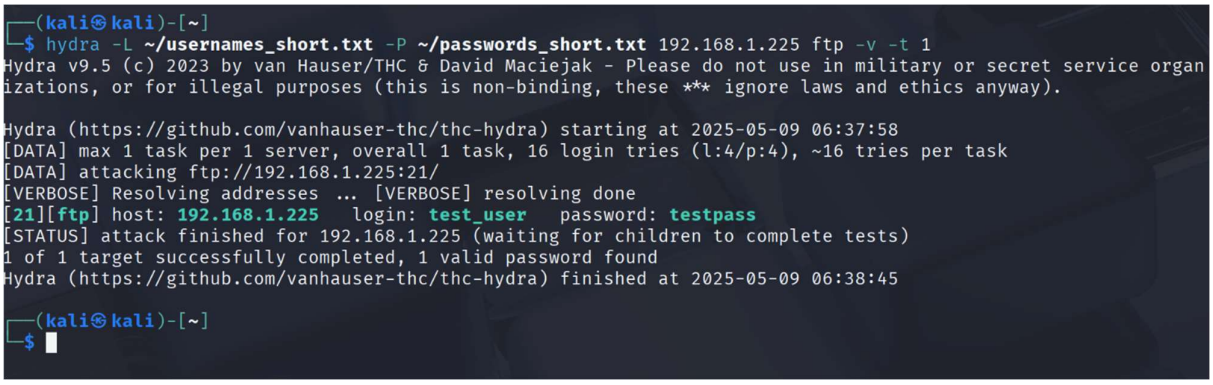
La prima parte dell’esercizio è quindi conclusa.

Per la seconda parte dell’esercizio, scelgo il servizio ftp, e poi provo a craccare l’autenticazione con Hydra.

Inizio con l'installare il servizio



Avvio il servizio e utilizzo Hydra con i dizionari di quattro parole usati in precedenza



Hydra ha trovato una corrispondenza per il servizio FTP ed è riuscito a autenticarsi al server FTP in esecuzione su 192.168.1.225 utilizzando l'username test_user e la password testpass.