Authentication Cracking con Hydra

Obbiettivi:

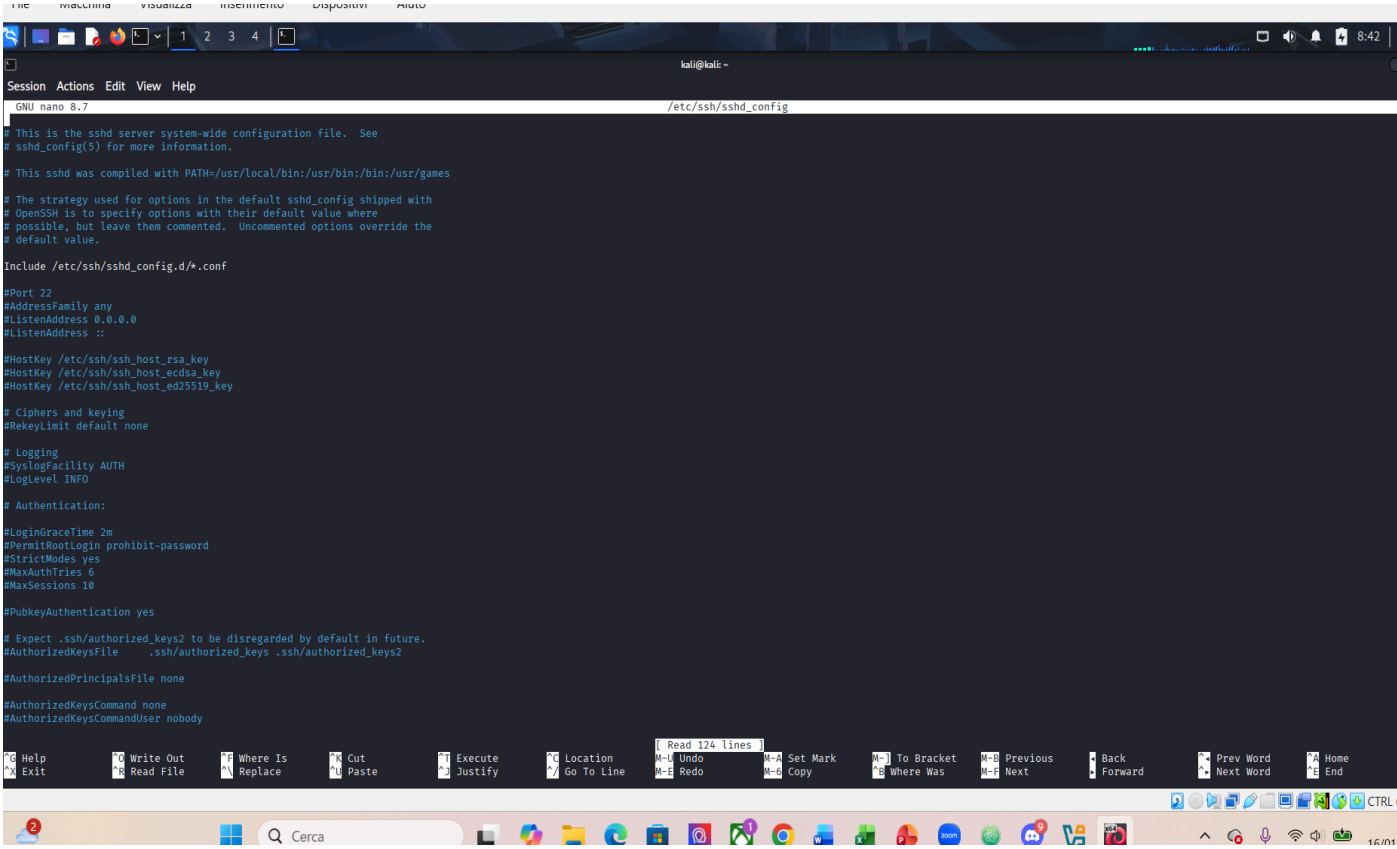
- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.

- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

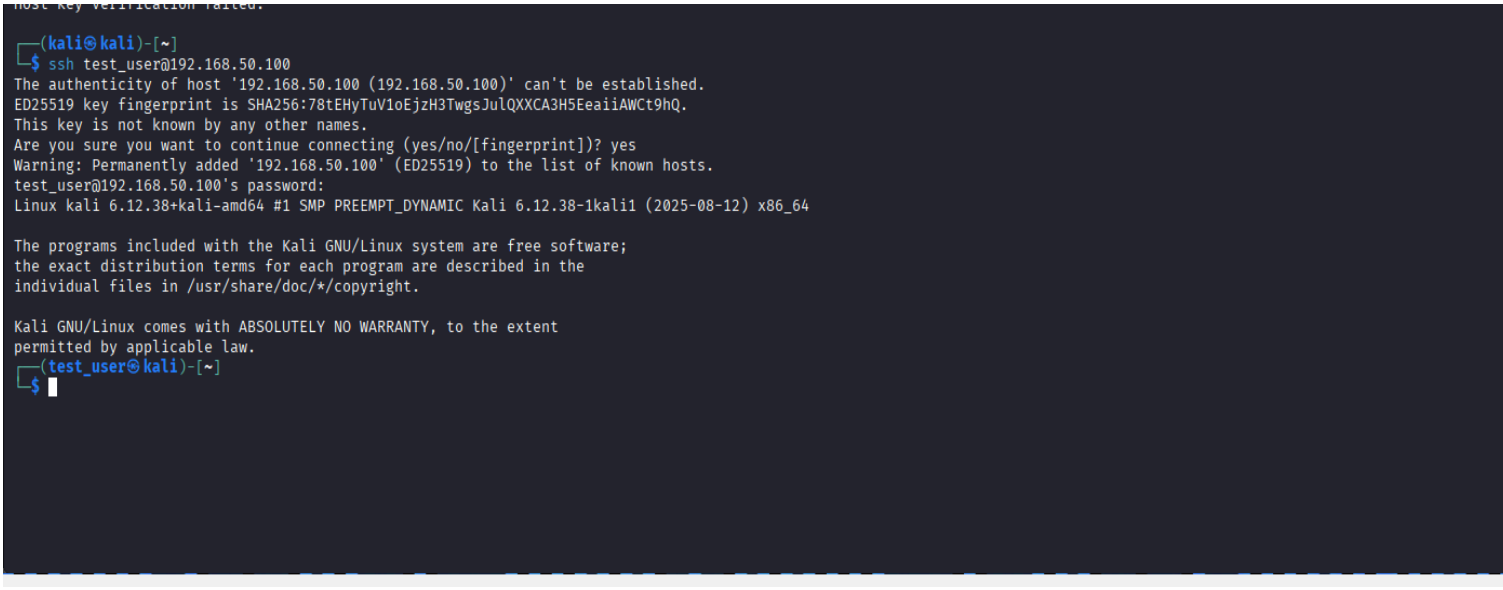
Fase 1 - Configurazione e Cracking SSH

SSH (Secure Shell) è un protocollo di rete che consente l'accesso remoto sicuro a sistemi informatici tramite una connessione cifrata.
Permette di eseguire comandi, amministrare server e trasferire file a distanza.
Utilizza meccanismi di autenticazione come password o chiavi crittografiche.
È uno standard fondamentale per la gestione dei sistemi e la sicurezza informatica.

Creiamo un nuovo utente su Kali Linux che avrà le seguenti credenziali:
username: test_user
password: testpass
Attiviamo il servizio **ssh** con il comando **sudo service ssh start**
Nel path **/etc/ssh/sshd_config** troviamo il file di configurazione del demone sshd e abilitiamo l'accesso all'utente root in ssh



Testiamo la connessione in ssh dell'utente appena creato, come di seguito:



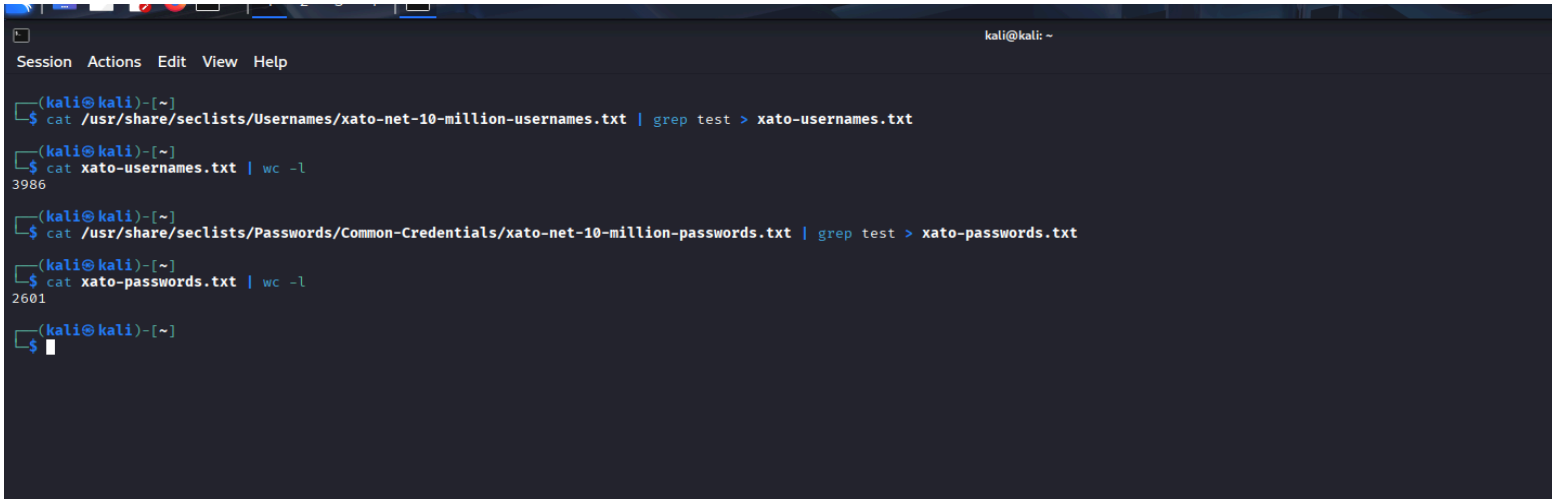
Dopo aver verificato l'accesso configuriamo Hydra per iniziare la sessione di cracking.

Hydra (THC Hydra) è uno strumento di sicurezza informatica utilizzato per testare la resistenza dei sistemi di autenticazione.
Consente di simulare attacchi di forza bruta o a dizionario su diversi servizi di rete.
È impiegato in contesti di penetration testing e audit di sicurezza autorizzati.
Aiuta a individuare password deboli e configurazioni vulnerabili.

Prima di iniziare la sessione di cracking scarichiamo delle wordlists di username e password installando **seclists** che contiene elenchi di username e password piuttosto vasti.

Per installare seclists: '**sudo apt install seclists**'

Le liste scaricate come anticipato contengono elenchi di user e password molto vasti e quindi li andremo a ridurre per una questione di tempi e risorse, come di seguito:



I comandi inviati ci permettono di leggere le wordlists con milioni di user e password con il comando ‘cat’ , tramite il comando ‘grep’ filtriamo le parole all’interno della lista che contengono ‘test’ e salviamo la nuova lista > su un file xato.txt

Una volta ridotte le nostre liste procediamo con l’attaccare l’autenticazione SSH con Hydra come di seguito.

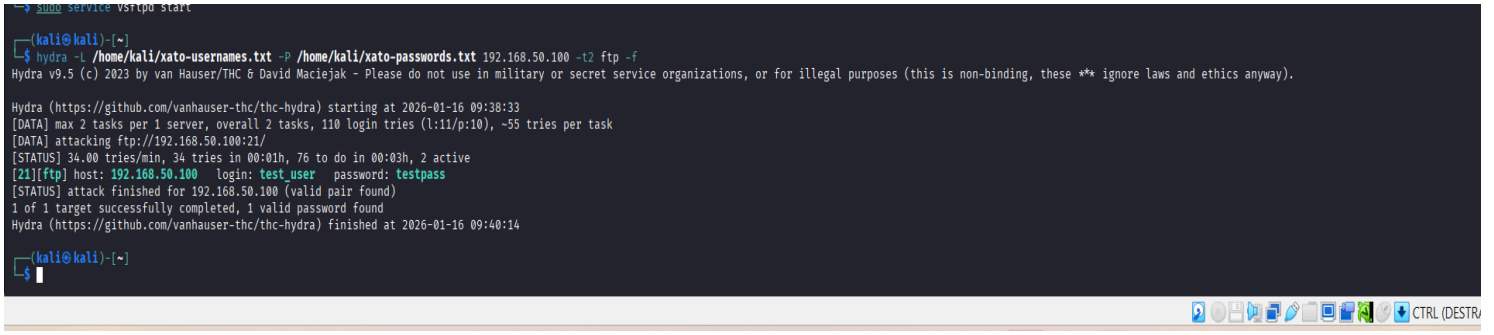
Il cracking SSH è andato a buon fine siamo riusciti ad ottenere user e password dell’utente creato.

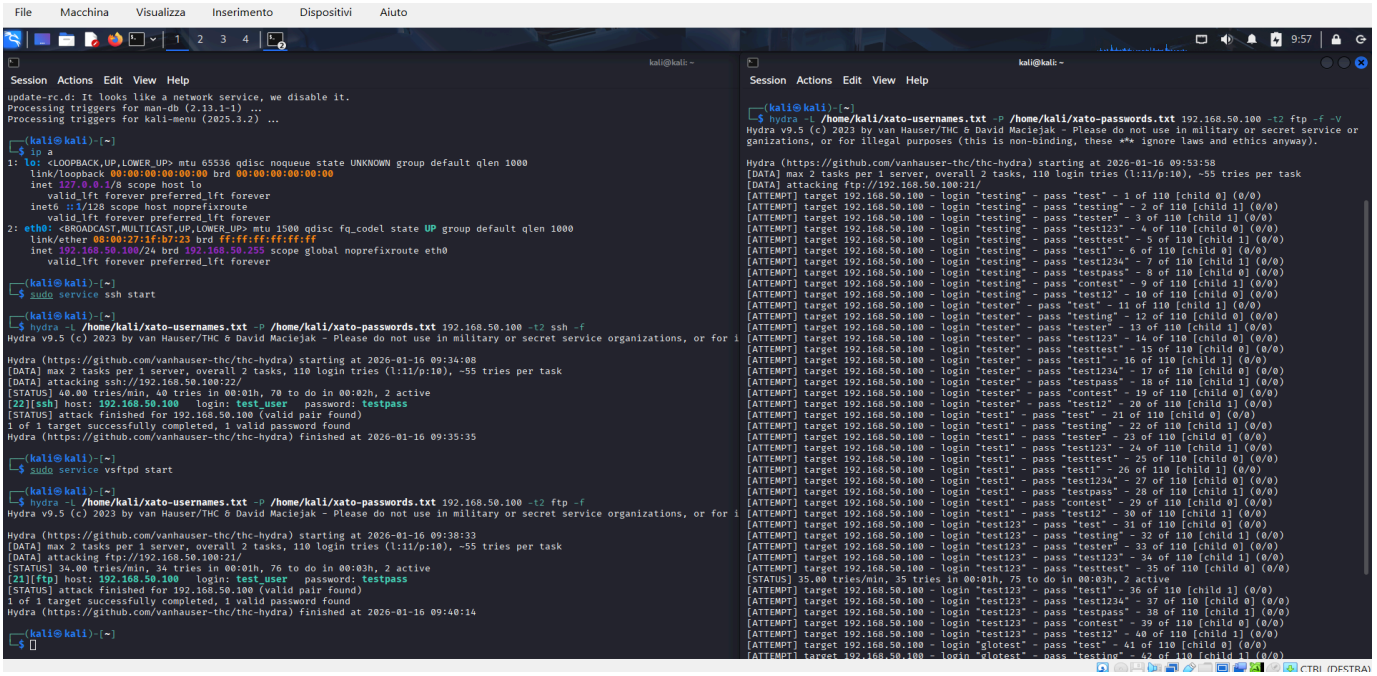
Fase 2 - Cracking servizio FTP

FTP (File Transfer Protocol) è un protocollo di rete usato per trasferire file tra un client e un server.
Permette operazioni di upload, download e gestione dei file da remoto.
Utilizza una connessione di rete standard senza cifratura dei dati.
Per questo motivo è considerato poco sicuro.
Oggi viene spesso sostituito da SFTP o FTPS.

Installiamo il servizio con il seguente comando
sudo apt install vsftpd
E poi avviare il servizio con: **sudo service vsftpd start**

Possiamo procedere tramite Hydra al cracking di ftp come di seguito:





Il cracking FTP è andato a buon fine siamo riusciti ad ottenere user e password dell'utente creato.