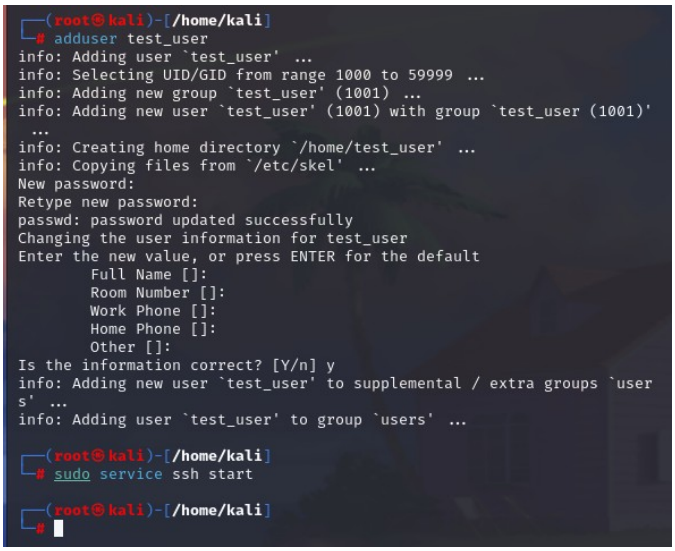
In questa esercitazione andrò a configurare un nuovo utente sulla macchina kali, abilitare il servizio SSH e infine Hydra per craccare le credenziali.

Come compito opzionale dove dobbiamo configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

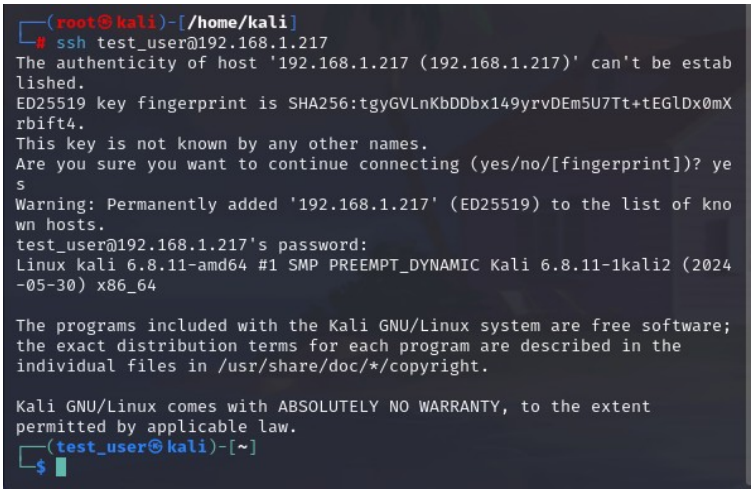
Come prima cosa creo un nuovo user su kali. Per farlo uso il comando “adduser” da terminale con i permessi di amministratore e assegno come user “test_user” e come password “testpass”

Successivamente attivo il servizio ssh con il comando
sudo service ssh start



Testo la connessione SSH dell’user appena creato con il comando ssh test_user@ip_kali.

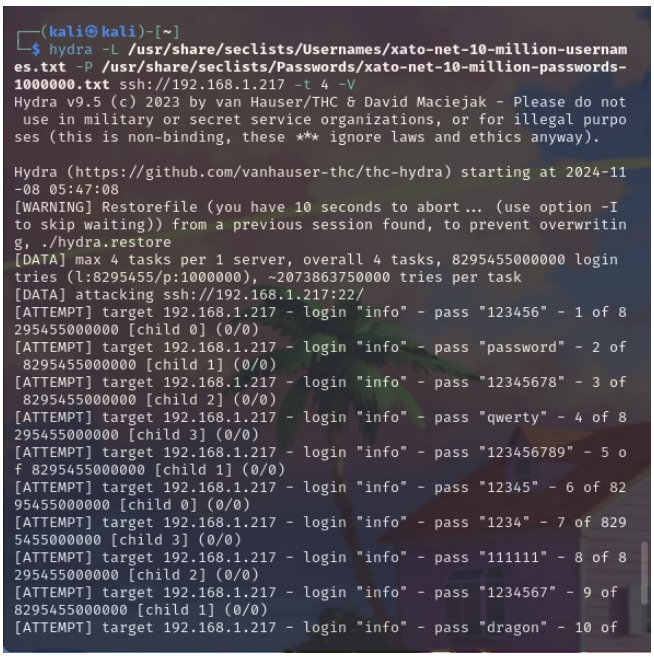
Si può notare come una volta terminato abbiamo effettuato la connessione a test_user al servizio SSH e ora che ho verificato l’accesso procedo con il cracking della password con Hydra



Ho scaricato una collezione di username e password di nome Seclists, contiene elenchi di username e password piuttosto vasto. Con il comando sudo apt-get install seclists ho eseguito l’installazione.

Apro un nuovo terminale e inserisco il comando hydra -L /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt ssh://192.168.1.217 -t4 -V

Come si può notare il processo potrebbe richiedere molto tempo



Nella seconda parte dell'esercizio eseguo gli stessi passaggi ma per un altro servizio, ftp,
lo installo con il comando
sudo apt-get install vsftpd, poi avvio il servizio con service vsftpd start

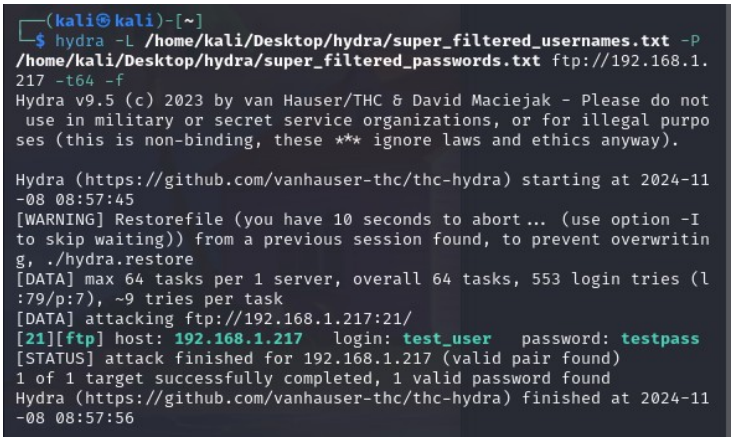
Un altro metodo che aiuta a velocizzare è quello di dividere la lista in liste piu piccole usando grep, creo dei file di testo filtrati con una o più parole chiave per ridurre la grandezza della lista.

Per gli user ho usato
grep -i "test" /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt > filtered_usernames.txt

Per la password
grep -i "test" /usr/share/wordlists/seclists/Passwords/xato-net-10-million-passwords-1000000.txt > filtered_passwords.txt

Infine uso il comando hydra con il path del nuovo file
hydra -L /home/kali/Desktop/hydra/super_filtered_usernames.txt -P /home/kali/Desktop/hydra/super_filtered_passwords.txt ftp://192.168.1.217 -t64 -f

Questo metodo riduce i tempi di attesa che, in base alla macchina che si sta usando, potrebbe richiedere molto più tempo di quanto noi ne abbiamo a disposizione



Hydra:
-L indica che vogliamo fare piu di un sigolo tentativo (-l) per gli user e gli diamo una lista.txt
-P stessa cosa ma con le password
-t64 sono i threads che vogliamo aprire, indica quante task vogliamo fare eseguire contemporaneamente alla macchina
-f che il comando si ferma subito dopo avere avuto un riscontro positivo
-V stampa su terminal i tentativi che si effettuano in realtime