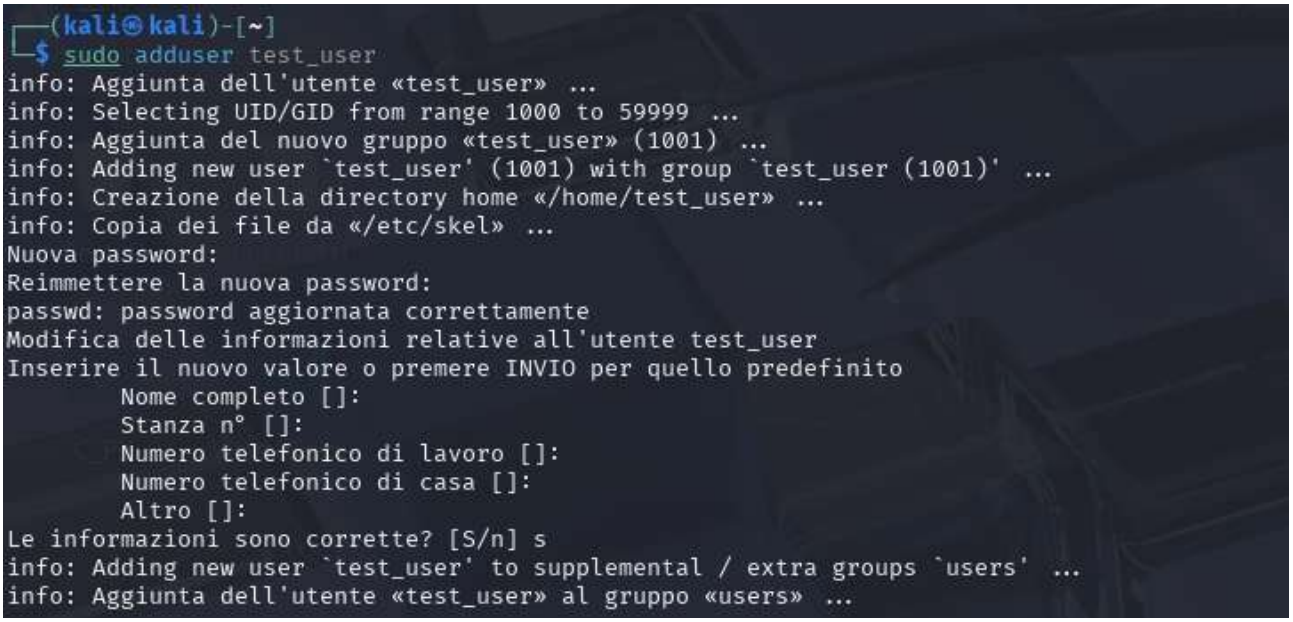
PROGETTO S6L5

Authentication cracking con Hydra

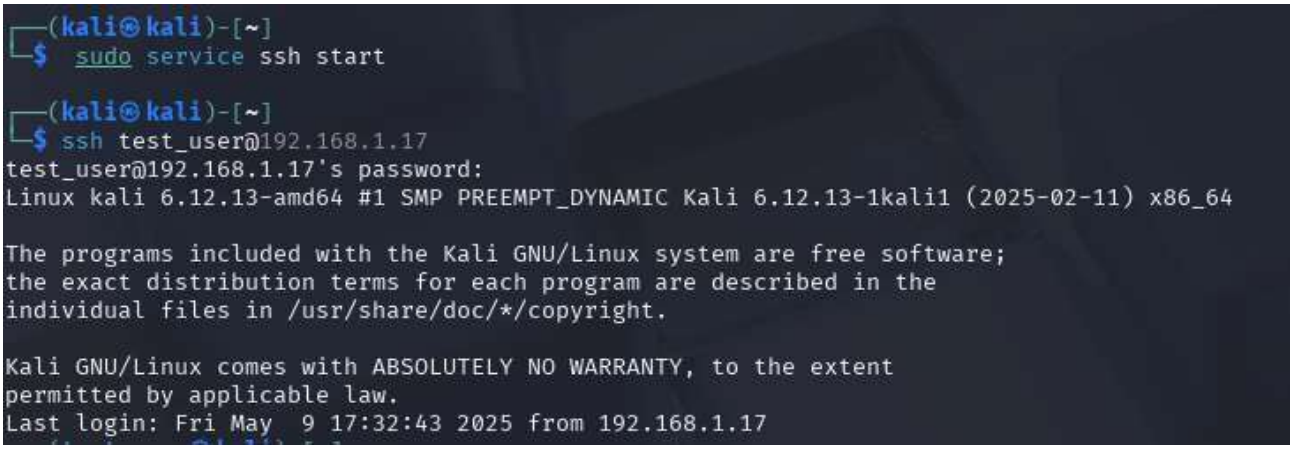
1.

Qui sto aggiungendo un nuovo utente chiamato "test_user" al mio sistema Kali Linux. Ho impostato una password e inserito alcune informazioni di base. Alla fine, l'utente è stato creato e aggiunto al gruppo users.



2.

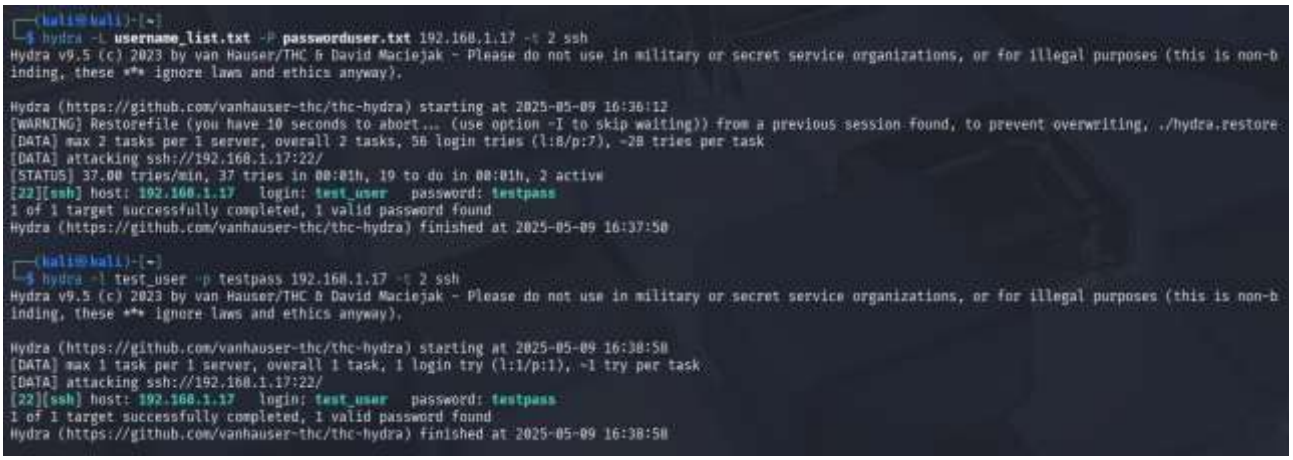
Qui sto avviando il servizio SSH sul mio Kali Linux con il comando sudo service ssh start. Questo mi permette di connettermi al mio computer in modo sicuro da remoto. Vedo anche l'indirizzo IP da cui ho effettuato l'ultimo accesso.



3.

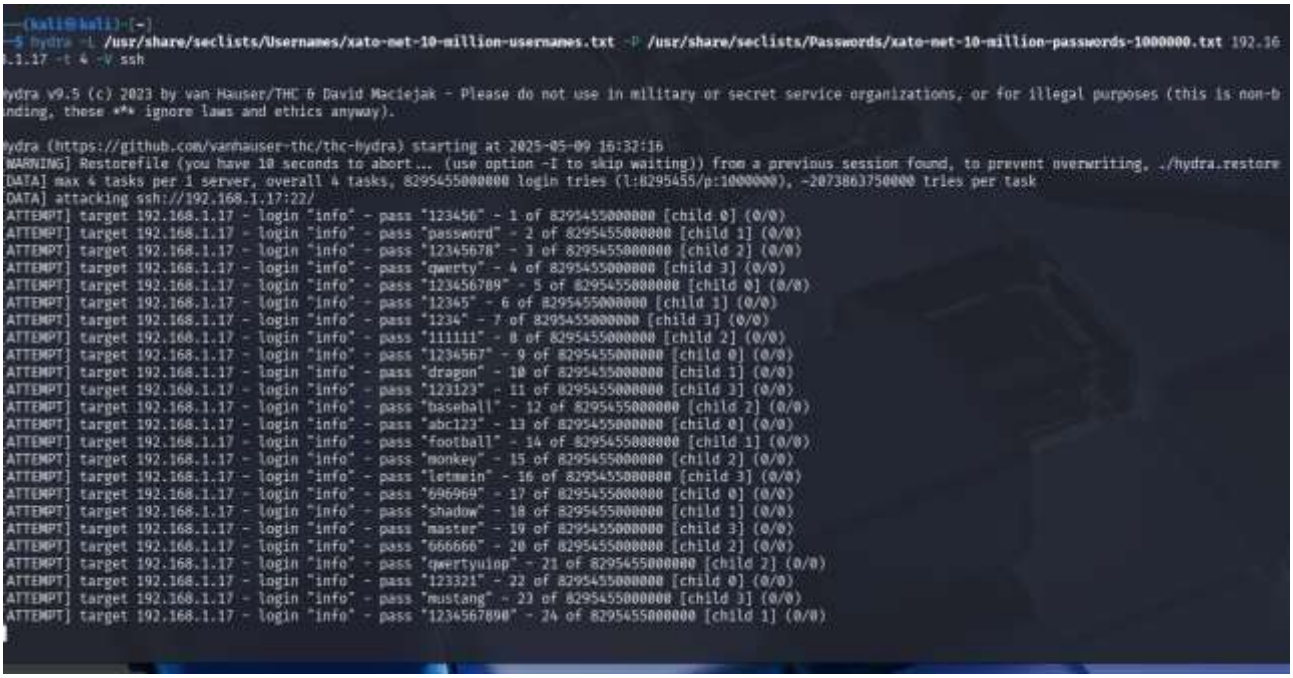
Sto usando Hydra per provare a indovinare le credenziali SSH per l'indirizzo 192.168.1.17.

Ho usato due comandi diversi: uno con liste di username e password e l'altro specificando direttamente le credenziali. In entrambi i casi, Hydra ha trovato la combinazione corretta -> test_user e testpass



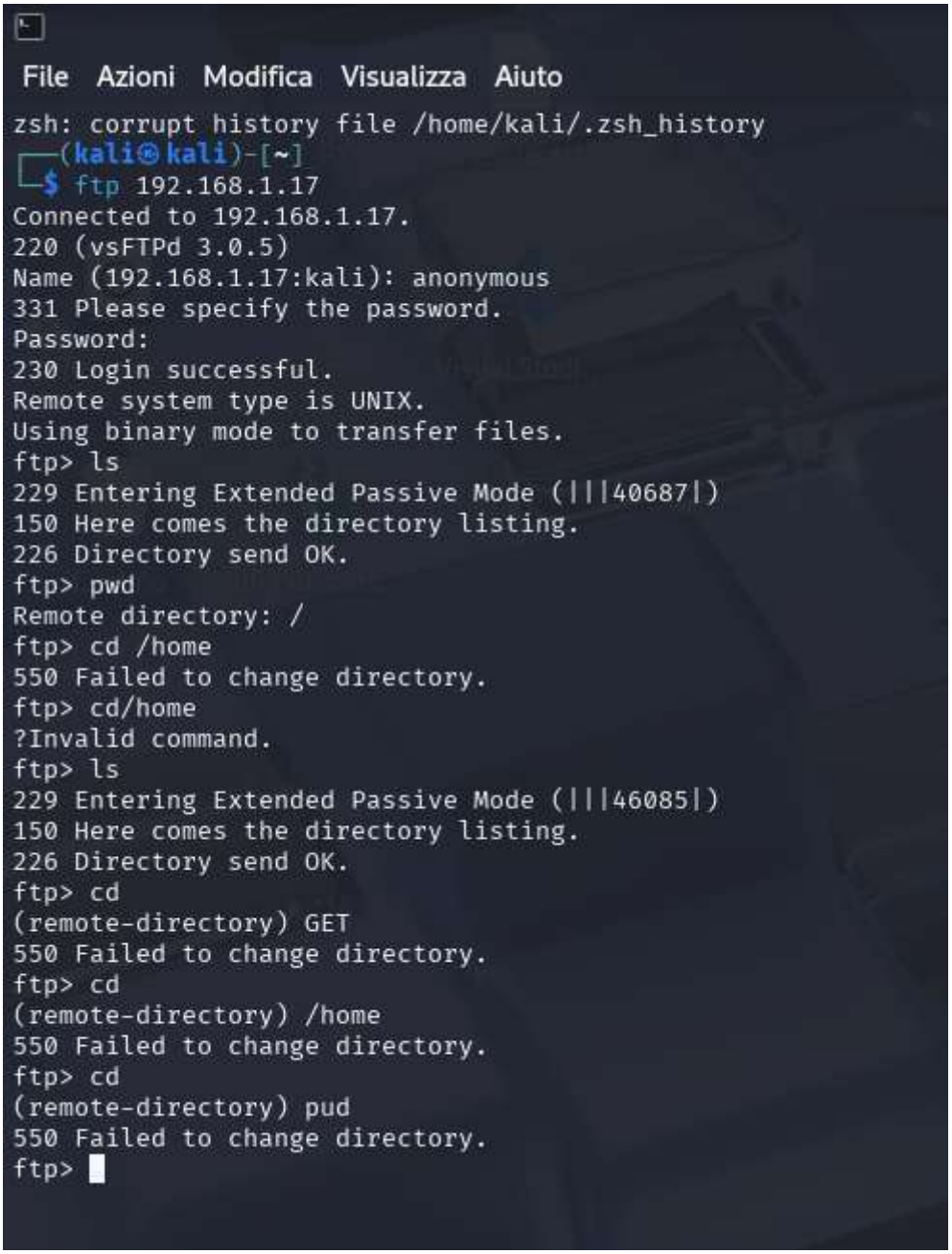
4.

Questa volta sto usando una lista di password molto grande per tentare l'accesso SSH all'indirizzo 192.168.1.17. Vedendo tanti tentativi falliti, dimostra come funziona un attacco di forza bruta.



5.

Qui mi sto connettendo a un server FTP all'indirizzo 192.168.1.17 usando il comando ftp.
Ho provato ad accedere come utente anonimo e il login è riuscito. quando ho provato a vedere nelle directory con comandi come cd, ho avuto degli errori.



Dopo tanti tentatvivi e qualche consiglio del prof, con il comando ‘pwd’ ho voluto sapere in quale cartella remota mi trovavo, e la risposta è stata la radice (slash).
Poi, ho dato ls -la per vedere tutti i file e le cartelle presenti lì, inclusi quelli nascosti, con i relativi permessi, proprietari, dimensioni e date. Ho visto due directory.
Successivamente, ho provato a spostarmi nella cartella public con cd public, ma purtroppo il server mi ha risposto con un errore "550 Failed to change directory.". Quindi, non sono riuscito a entrare in quella cartella.
Ho comunque provato a dare di nuovo ls -la, ma ovviamente la lista delle directory è rimasta la stessa, visto che non mi ero spostato.

Infine, ho tentato di scaricare il file users.txt.bk con il comando get users.txt.bk. Anche in questo caso, ho ricevutolo stesso errore, quindi non sono riuscito a scaricare il file.