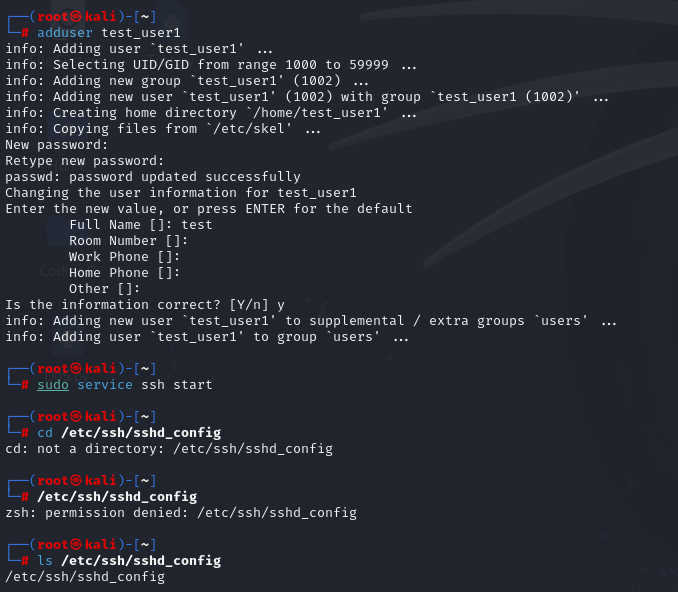
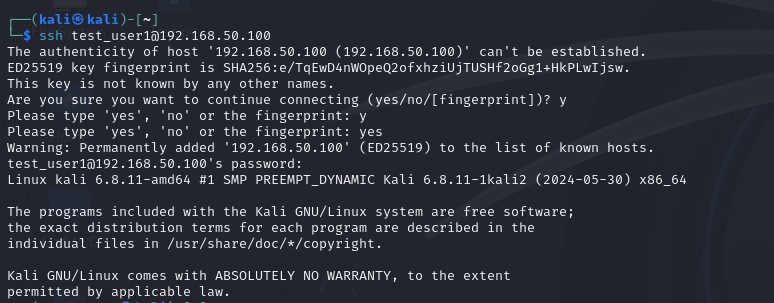
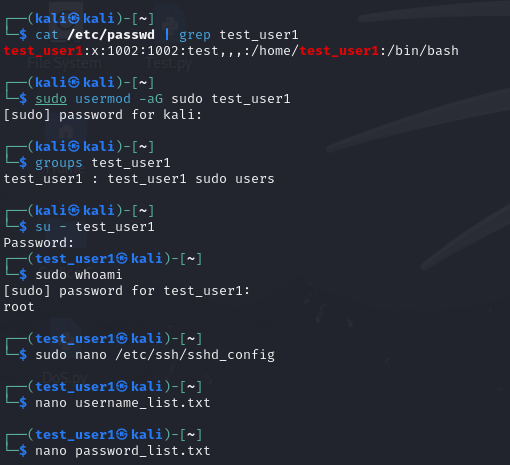
**Progetto S6L5 Valentina Rubina Tempesta**

**Authentication cracking con Hydra:**

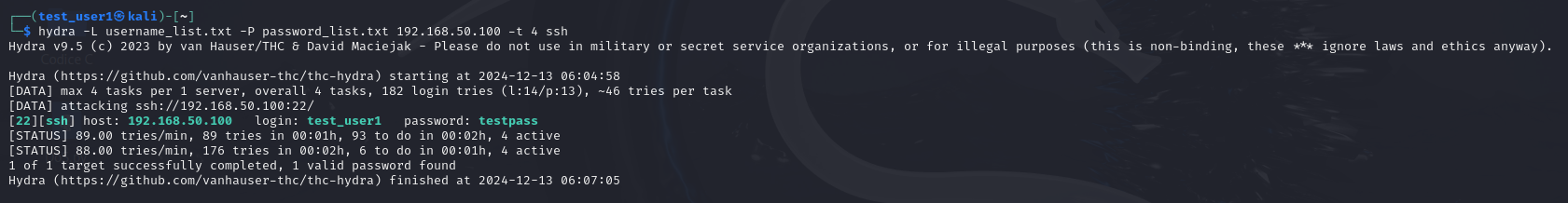
Sono andata a creare un nuovo utente sulla Kali chiamandolo **test\_user1** con password **testpass** e successivamente avviato il servizio di ssh ed esplorato il path /**etc/ssh/sshd\_config** senza apportare alcuna modifica al file.   


Successivamente ho testato la connessione SSH inserendo il nome user e l’ip della mia kali, ricevendo il prompt corretto.   


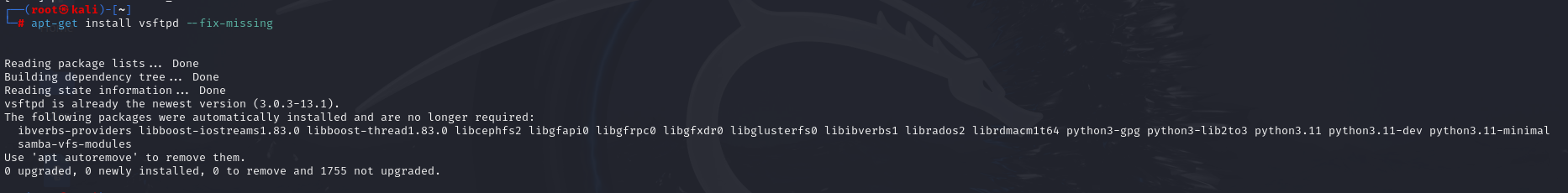
Da qui ho cominciato la fase di cracking con Hydra.   
Ho prima di tutto dato i privilegi di root a user\_test1 così da poter permettere la creazione di file di testo. Di seguito ho creato due file di testo con user e password (**username\_list** e **password\_list**) contenenti le due credenziali veritiere dell’account insieme ad altre fasulle.



Ho mandato il comando per l’avvio della ricerca hydra in modalità non verbosa inserendo l’ip di kali e dopo pochi minuti ho avuto il risultato sperato, hydra ha scoperto password e nome utente.

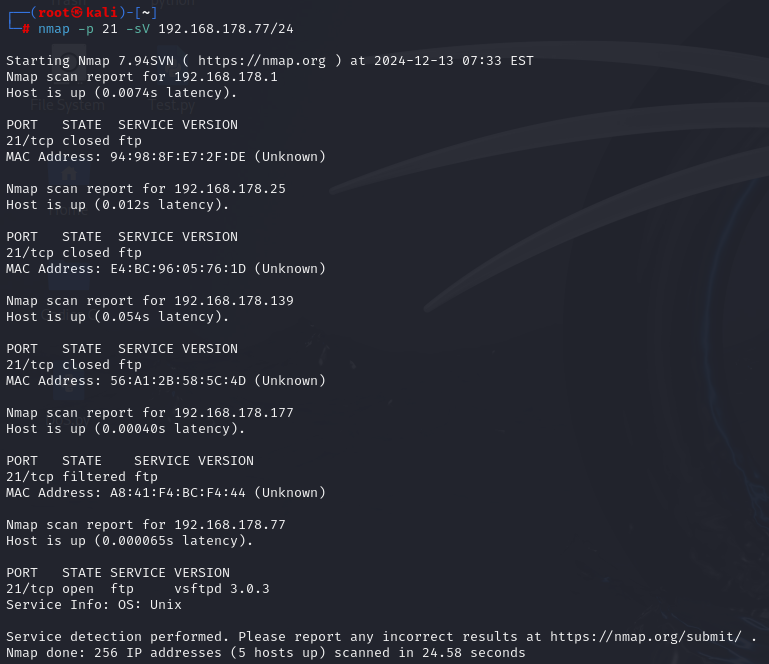


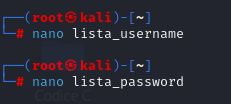
Per la seconda parte dell’esercizio ho deciso di craccare il servizio ftp, installandolo ed avviandolo.



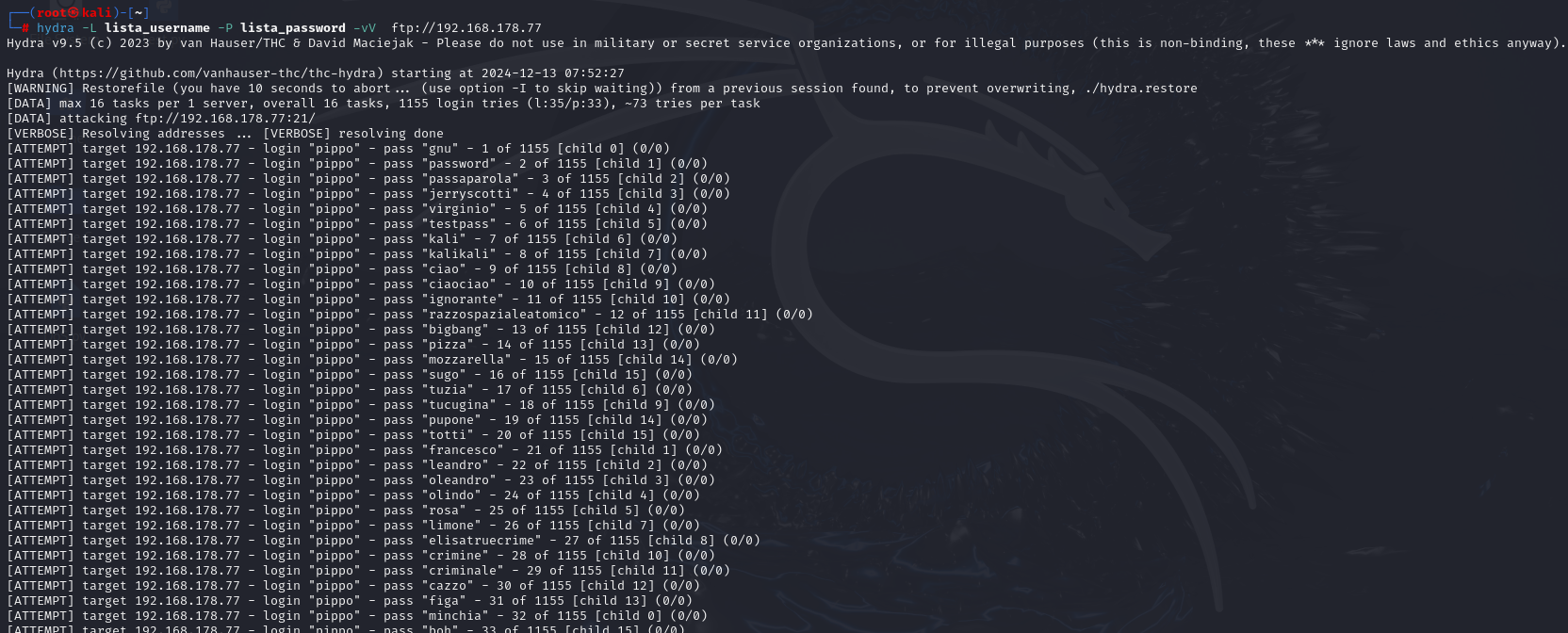


ho avviato una scansione della porta ftp (21) per avere la certezza dell’ip nel quale era aperta, confermando l’ip della mia kali.

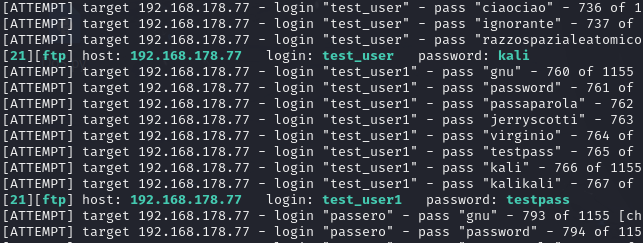


Ho ricreato due file differenti contenenti all’interno svariati user e password con anche la giusta combinazione per entrambi.   


Ed ho avviato la scansione in modalità verbosa per FTP:



Dopo svariati tentativi cercando di associare password ed user da entrambi i file dati, Hydra è riuscito a trovare la giusta combinazione.



🥳🥳🥳