**Trama:**

L’esercizio di oggi ha un duplice scopo:

● Fare pratica con **Hydra** per craccare l’autenticazione dei servizi di rete.

● Consolidare le conoscenze dei servizi stessi tramite la loro configurazione. L’esercizio si svilupperà in due fasi:

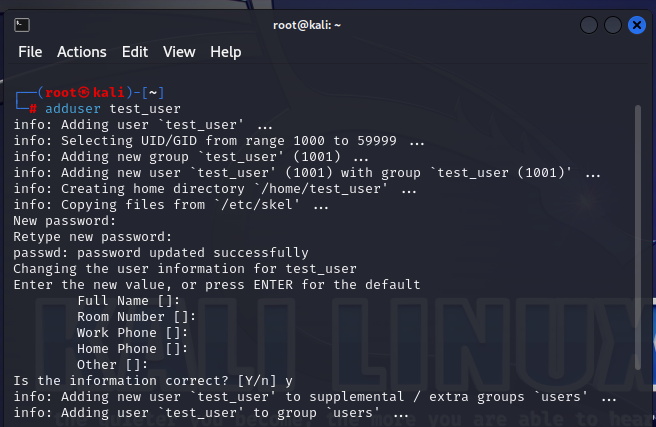
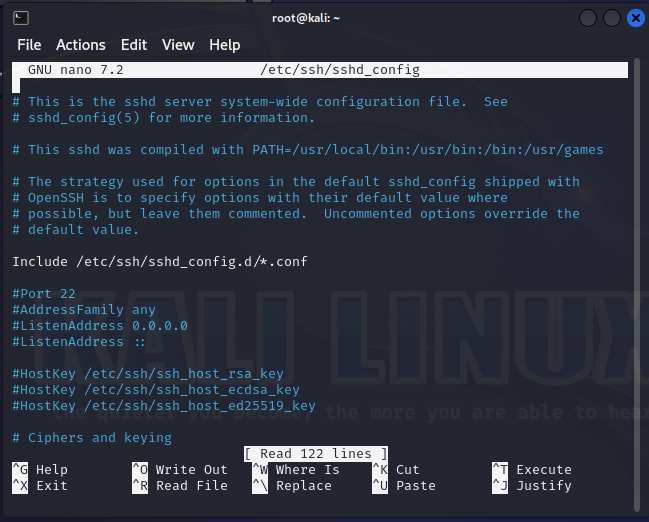
● Una prima fase dove insieme vedremo l’abilitazione di un servizio SSH e la relativa sessione di cracking dell’autenticazione con Hydra.

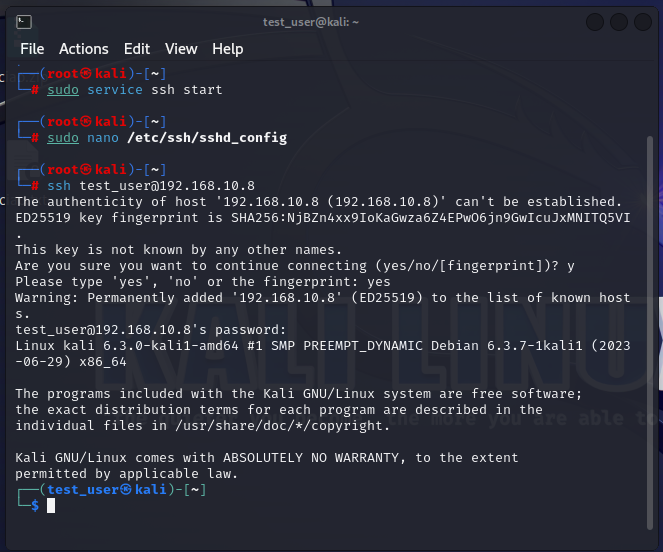
● Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

Per iniziare creiamo un nuovo utente su Kali Linux, con il comando «adduser», il nome utente sarà **test\_user**, e la password **testpass**.

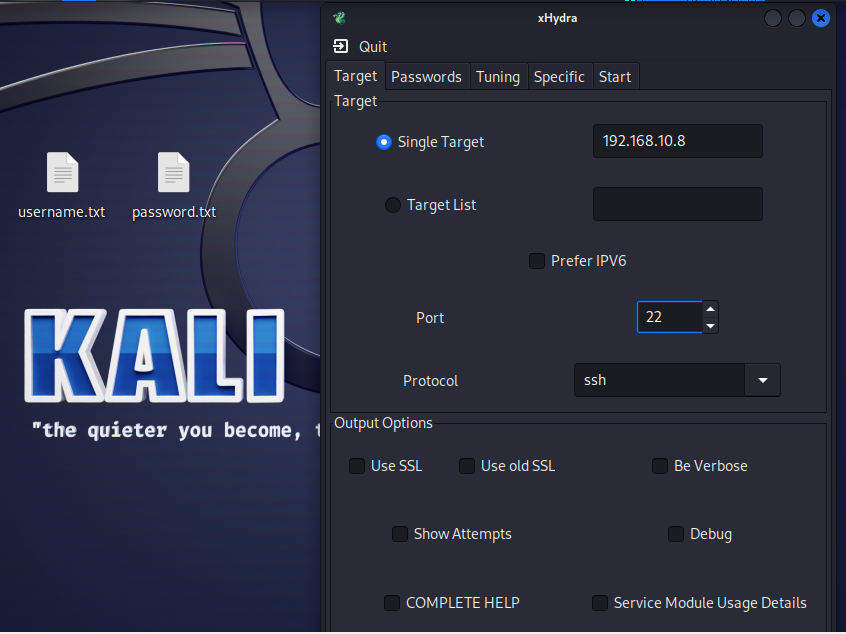
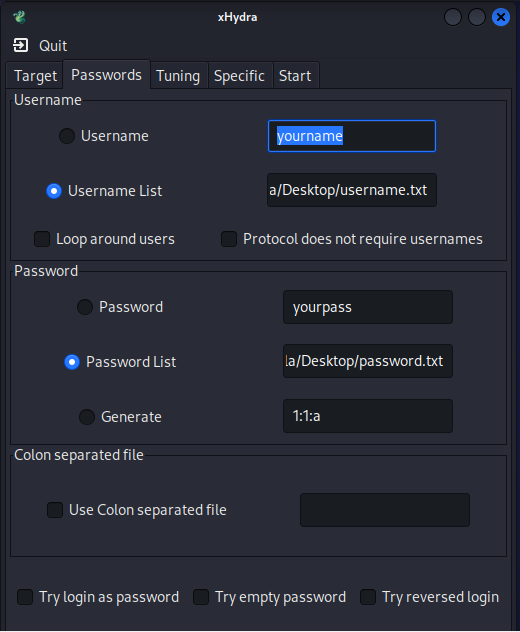
Attiviamo il servizio ssh con il comando **sudo service ssh start** e lo configuriamo con il path **/etc/ssh/sshd\_config** per abilitare l’accesso all’utente root in ssh.

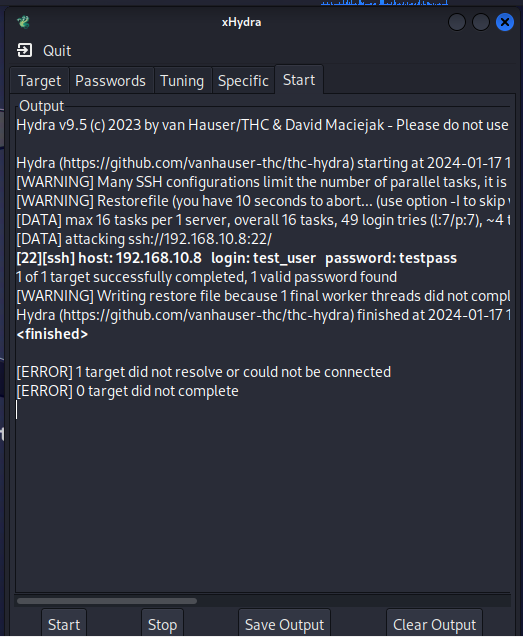
Stiliamo un paio di liste, rispettivamente di username e di password, e siamo pronti per aprire Hydra.



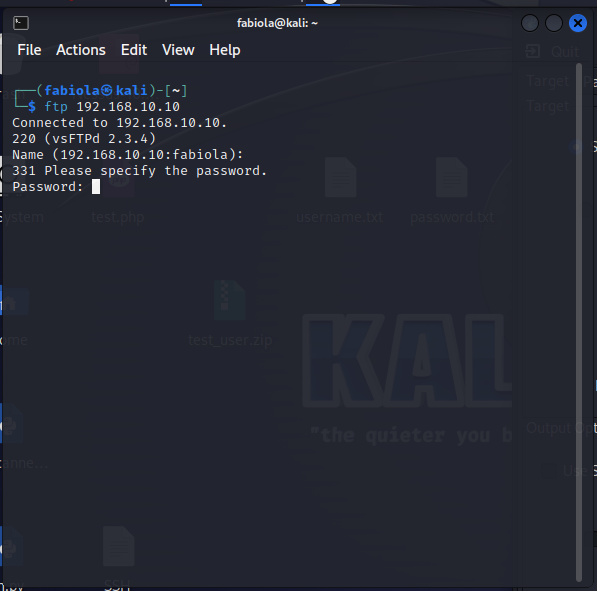
Una volta aperto Hydra, impostiamo il target (in questo caso l’IP di Kali), la porta e il protocollo (SSH su porta 22), nella sezione Passwords andiamo a richiamare le liste create sia per la sezione username che per password e startiamo il programma:

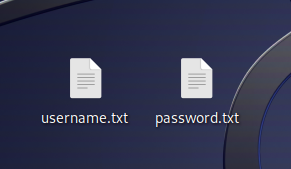
 



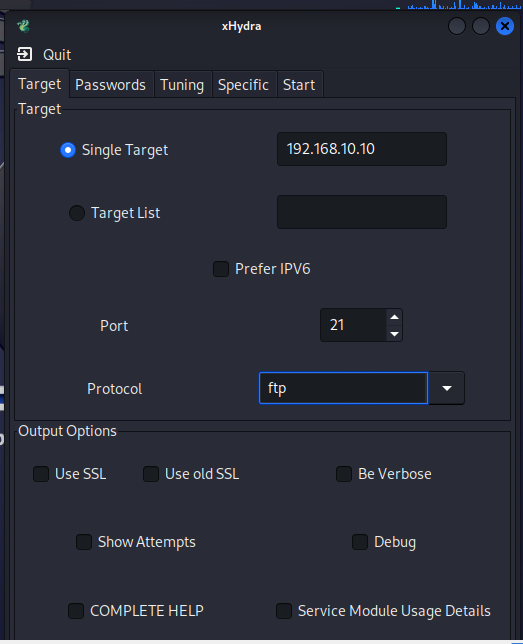
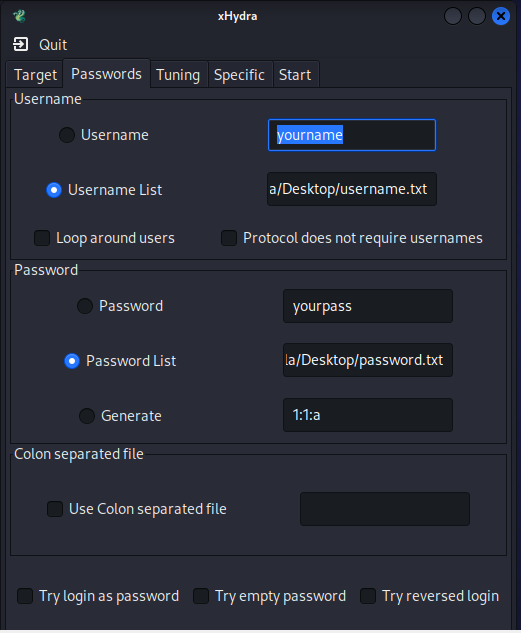
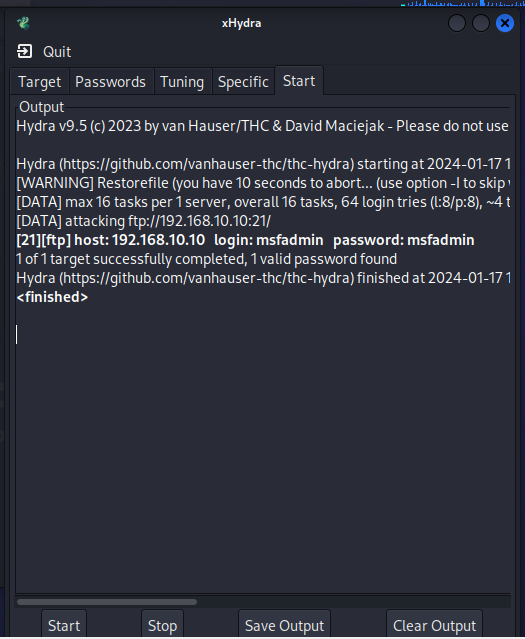
Come possiamo vedere, Hydra è riuscito ad estrapolare la username (test\_user) e la password (testpass).

Ora proviamo a craccare un altro servizio di rete, ad esempio FTP.

Il principio di base è lo stesso, dobbiamo estrapolare le credenziali di ftp di Metasploitable2, per fare ciò utilizzeremo le liste fatte in precedenza.



Impostiamo Hydra come abbiamo visto per l’SSH ma cambiando protocollo e porta:

Hydra ha trovato la username e la password, verificandone la veridicità possiamo renderci conto che siamo riusciti ad entrare e possiamo agire a piacimento:

