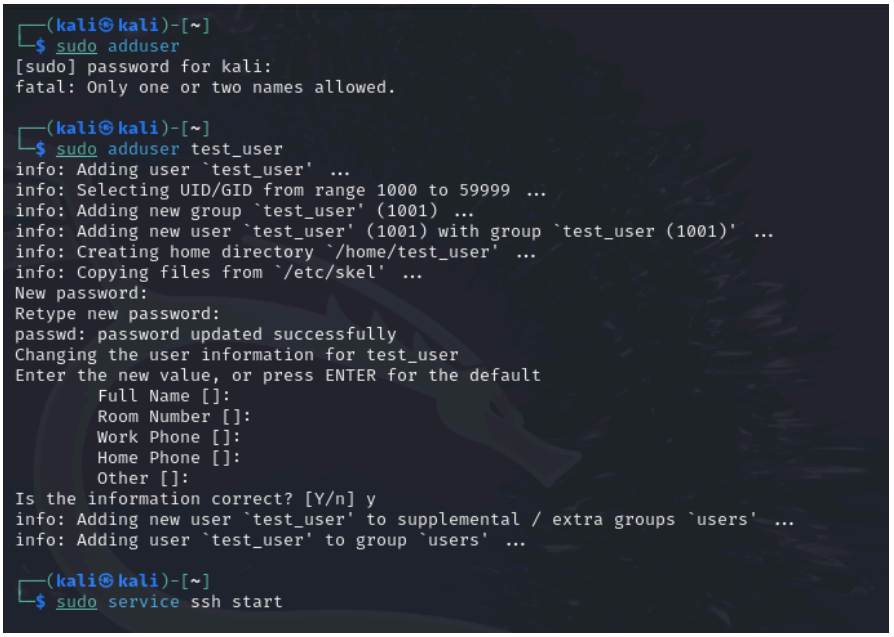
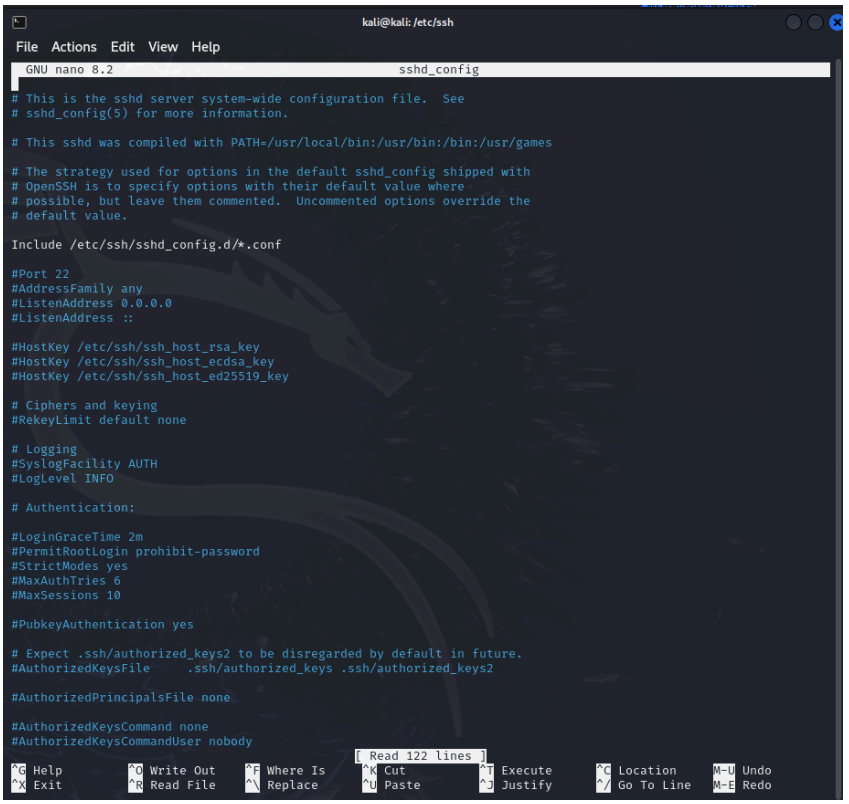
Esercitazione S6-L5 - Test Hydra su diversi servizi e macchine

- **SSH su user kali**

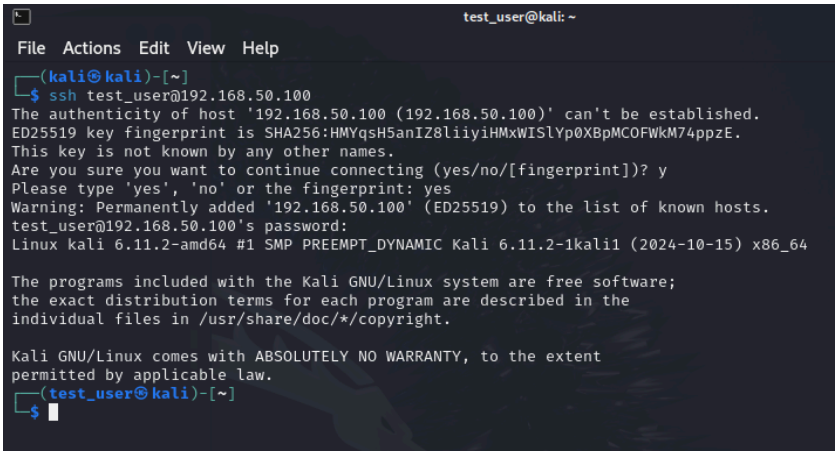
Creazione nuovo user **test_user** su kali e avvio **SSH**



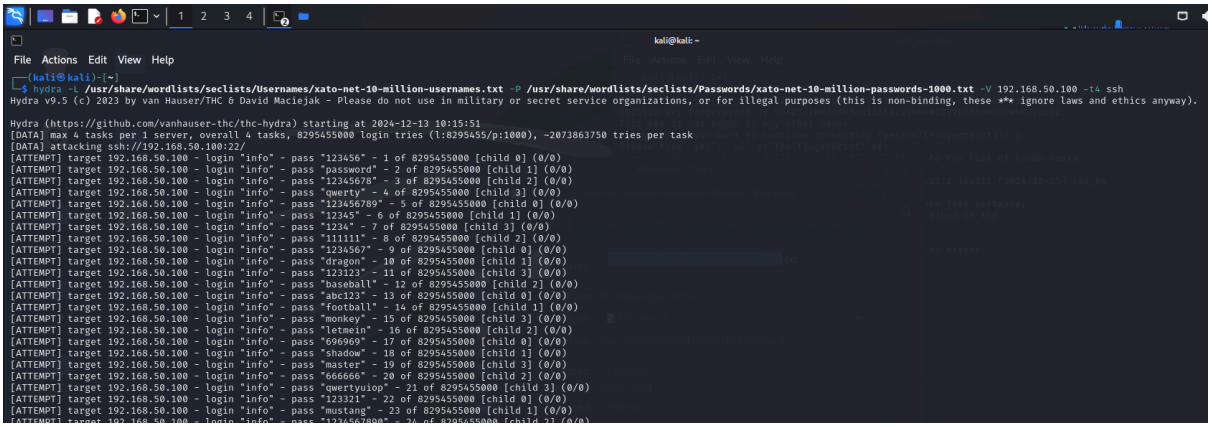
Apertura e studio file **config SSH**



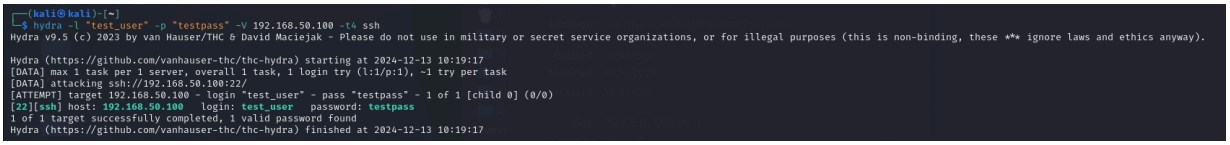
Apertura sessione **SSH** su **test_user** (indirizzo 192.168.50.100)



Avvio **hydra** inserendo in input una lista di username (**-L**) presa da **seclists**, una lista password (**-P**,anch'essa da **seclists**), l'indirizzo IP target (192.160.50.100) e il servizio preso in esame (**SSH**).
Altri parametri sono: **-V** che permette di visualizzare l'operato di Hydra
-t4 parametro per l'aggressività di hydra (16 default)



Viste le tempistiche, ho optato per un approccio differente. Ho inserito nome utente e password in **hydra** per accellerare la ricerca, limitandomi a verificarne il funzionamento



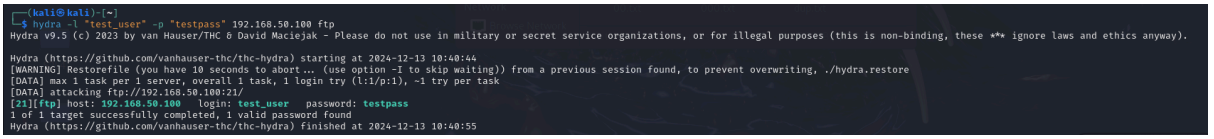
Come possiamo notare, **hydra** ha individuato i dati richiesti servendosi della porta **22** (**SSH)**.

- **FTP su user kali**

Installazione e avvio **vsftpd**

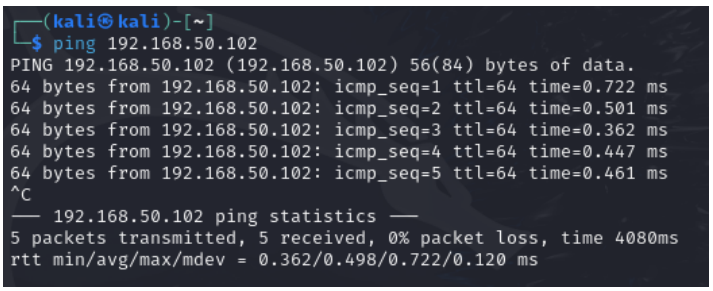
Avvio **hydra** su macchina kali (192.168.50.100) sfruttando il servizio **ftp**

Verifica funzionamento inserendo nome utente e password già noti

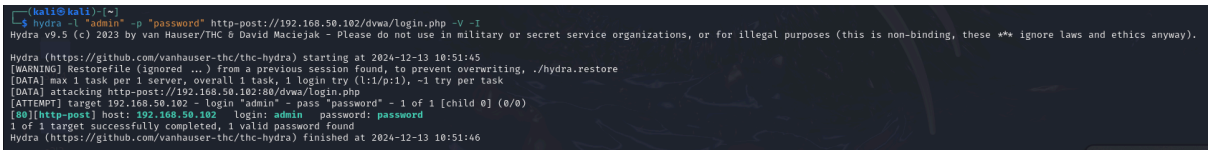


- **HTTP su macchina Metasploitable**

Collegamento macchina Metasploitable (192.168.50.102) su rete interna e verifica collegamento tramite **ping**

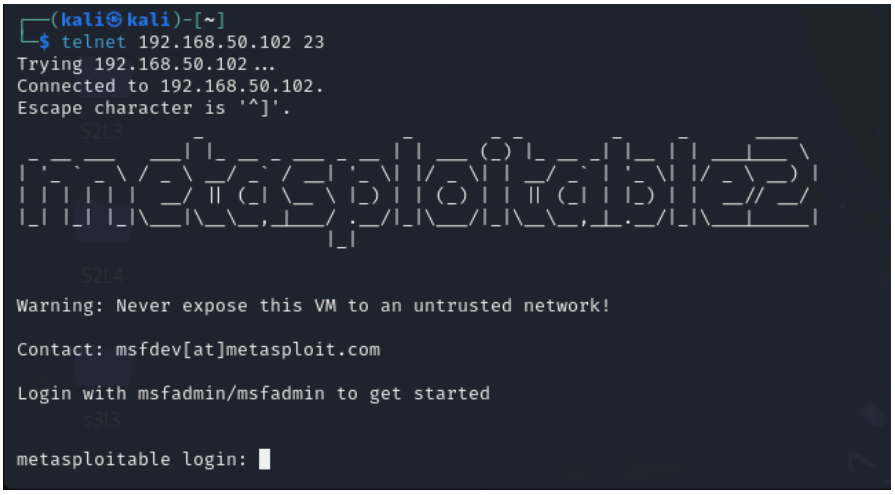


Test **hydra** su macchina Metasploitable sfruttando il verbo **POST** su servizio **HTTP**. Il test è stato effettuato sulla pagina di login della **DVWA**.

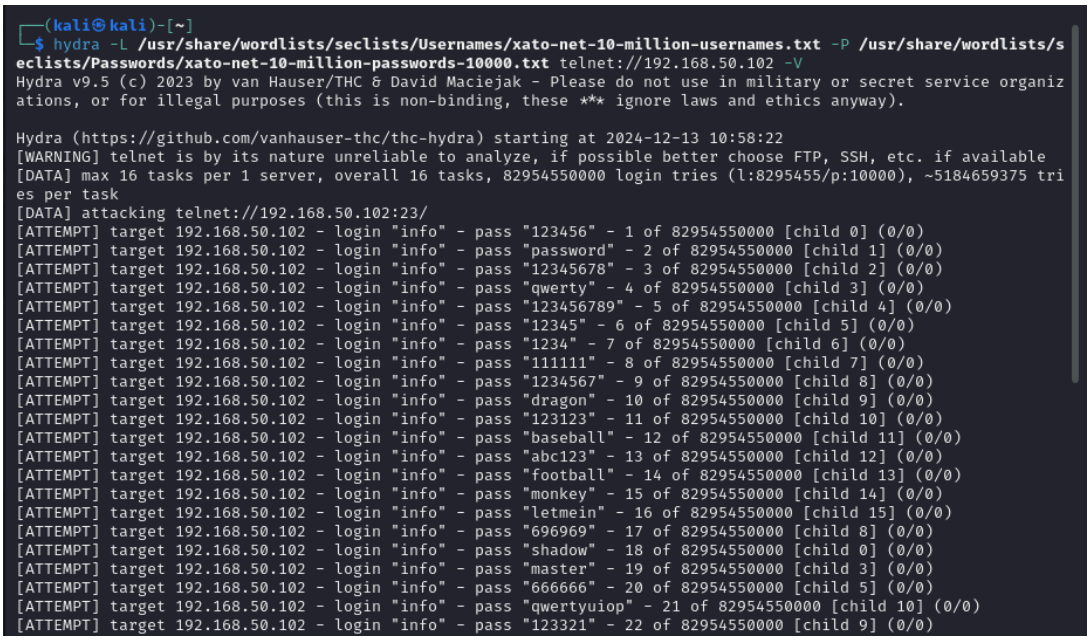


- **TELNET su Metasploitable**

Avvio connessione TELNET da kali (192.168.50.100) su Metasploitable (192.169.50.102)



Avvio **hydra** per ricerca di nome utente e password della Metasploitable sfruttando il servizio TELNET (**23**)



Verifica efficacia hydra tramite inserimento di nome utente e password noti