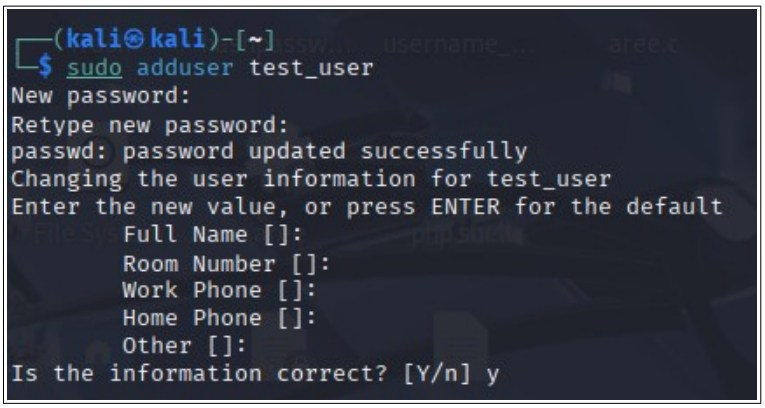
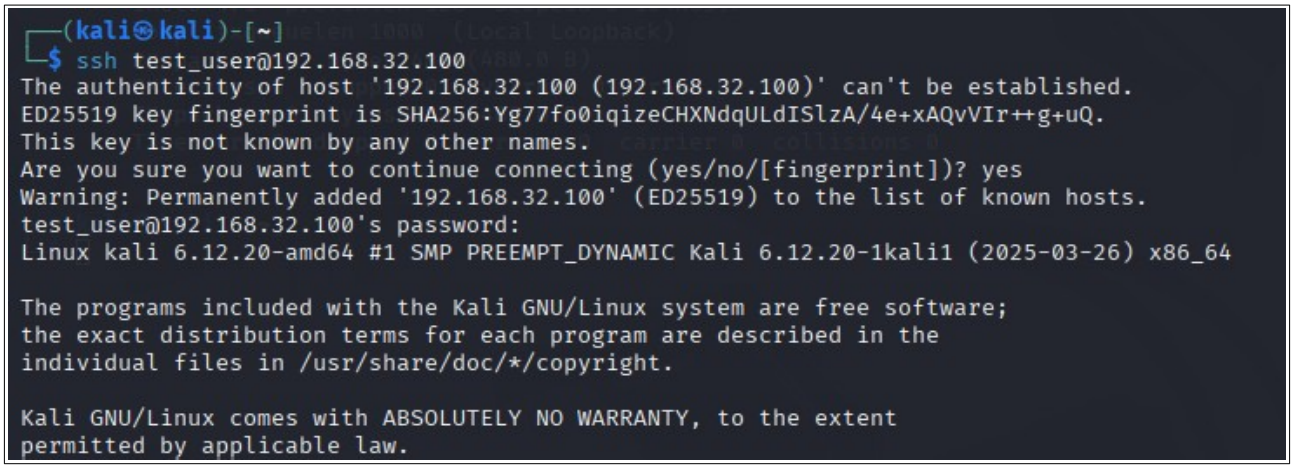
Report Authentication cracking con Hydra W14D4

In questo esercizio andremo ad effettuare il cracking delle password tramite Hydra.

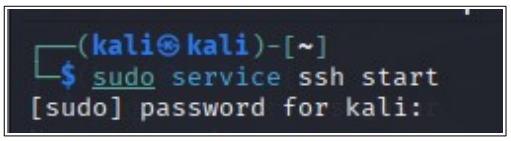
Step 1 Creiamo un nuovo user su Kali Linux con username: test_user e password: testpass.



Step 2 Abilitiamo il servizio SSH per l'user test_user e aggiungiamo l'IP di Kali tra gli IP trusted dal servizio.

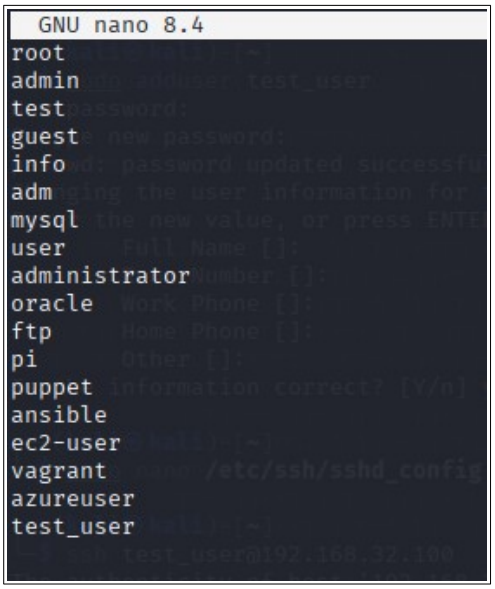


Step 3 Avviamo il servizio SSH tramite il comando sudo service ssh start.



Step 4 Mediante il comando wget -c https://github.com/danielmiessler/SecLists/archive/master.zip -O SecList.zip && unzip SecList.zip && rm -f SecList.zip scarichiamo Seclist e lo unzippiamo automaticamente.
Seclist contiene liste di username e password comuni che potremo passare ad Hydra ed utilizzarle per il password cracking.
N:B.: Kali dovrà essere in bridged con DHCP per poter eseguire il download.

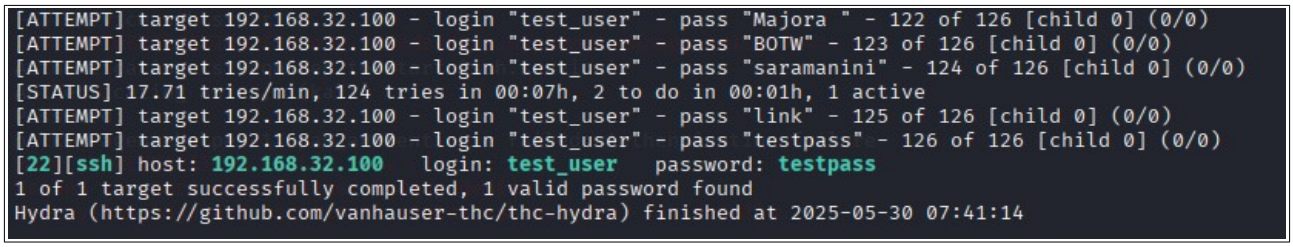
Step 5 Individuiamo due liste, una per gli username e una per le password da poter utilizzare. Nel mio caso ho scelto la lista top-usernames-shortlist.txt ed ho aggiunto l'username test_user per avere un esito positivo. Per la password ho creato una lista personalizzata che conteneva anche la password assegnata a test_user, cioè: testpass.
È bene notare che la password testpass era già contenuta nella lista Most-Popular-Letter-Passes.txt di Seclist, ma vista la mole di password contenute nel file, si è preferito crearne uno ad hoc più ristretto.



Step 6 Tramite il comando hydra -V -L ~/SecLists-master/Usernames/top-usernames-shortlist.txt -P ~/SecLists-master/Passwords/PasswordsSARA 192.168.32.100 -t1 ssh iniziamo il password cracking.
La sintassi del comando è la seguente:

- -V: verbose, stampa a schermo ogni tentativo di combinazione username e password che effettua;
- -L <file.txt path>: passiamo ad Hydra un file.txt di username da provare con relativo path del file;
- -P <file.txt path>: passiamo ad Hydra un file.txt di password da provare con relativo path del file;
- <IP macchina>: IP della macchina a cui verrà diretto l'attacco a dizionario;
- -t1: numero thread da utilizzare, in questo caso è uguale ad uno;
- <servizio>: servizio su cui viene effettuato il password cracking.

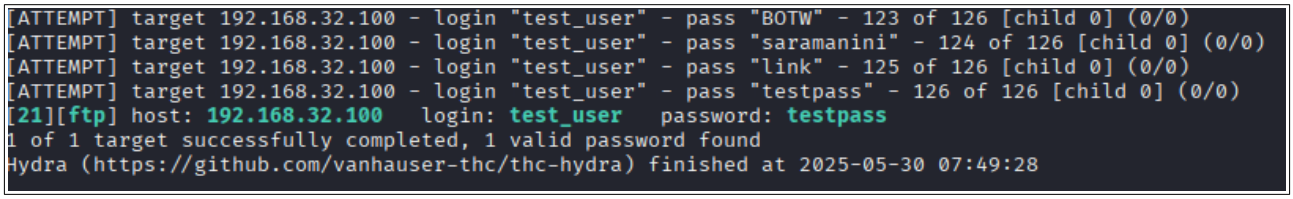
Come possiamo vedere dallo screenshot sottostante, l'attacco è andato a buon fine.



Step 7 Ripetere l'operazione per il servizio ftp, per prima cosa scarichiamo il servizio tramite il comando sudo apt install vsftpd.
N:B.: Kali dovrà essere in bridged con DHCP per poter eseguire il download.

Step 8 Avviare il servizio con il comando sudo service vsftpd start.

Step 9 Ripetere il comando visto in precedenza, ma sostituire il servizio con ftp. Come prima avremo un esito positivo.

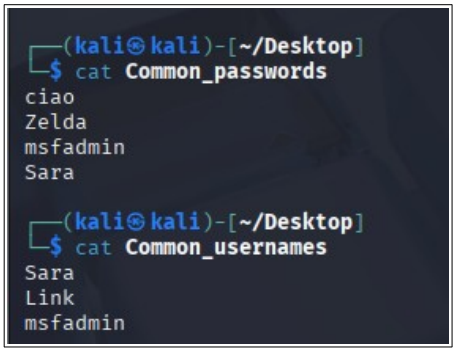


Facoltativo

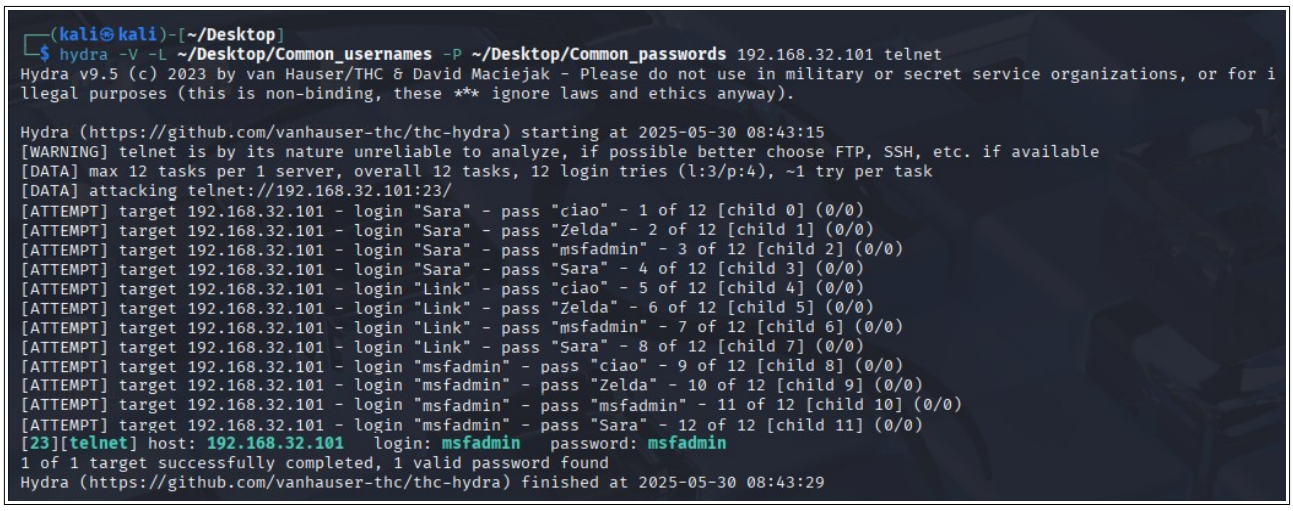
Eseguire il cracking delle password tramite un servizio a scelta di Metasploitable 2.

Step 1 Mettere entrambe le macchine (Kali e Metasploitable 2) su rete interna ed assicurarsi che possano comunicare tramite ping.

Step 2 Creare due file user e password, contenenti le credenziali di accesso di Metasploitable 2.



Step 3 Mediante il comando hydra -V -L ~/Desktop/Common_usernames -P ~/Desktop/Common_passwords 192.168.32.101 telnet , inizieremo il password cracking sul servizio telnet.
Come possiamo notare, avremo esito positivo.



Step 4 Proviamo il medesimo comando su un diverso servizio, ad esempio ftp.