Authentication Cracking con Hydra

Descrizione dell'esercizio

La prima parte dell'esercizio di oggi è guidata quindi provvederò a fornire degli screenshot dei vari step eseguiti da me.

Creiamo un nuovo utente su Kali Linux, con il comando «adduser».

Chiamiamo l'utente test_user, e configuriamo una password iniziale testpass

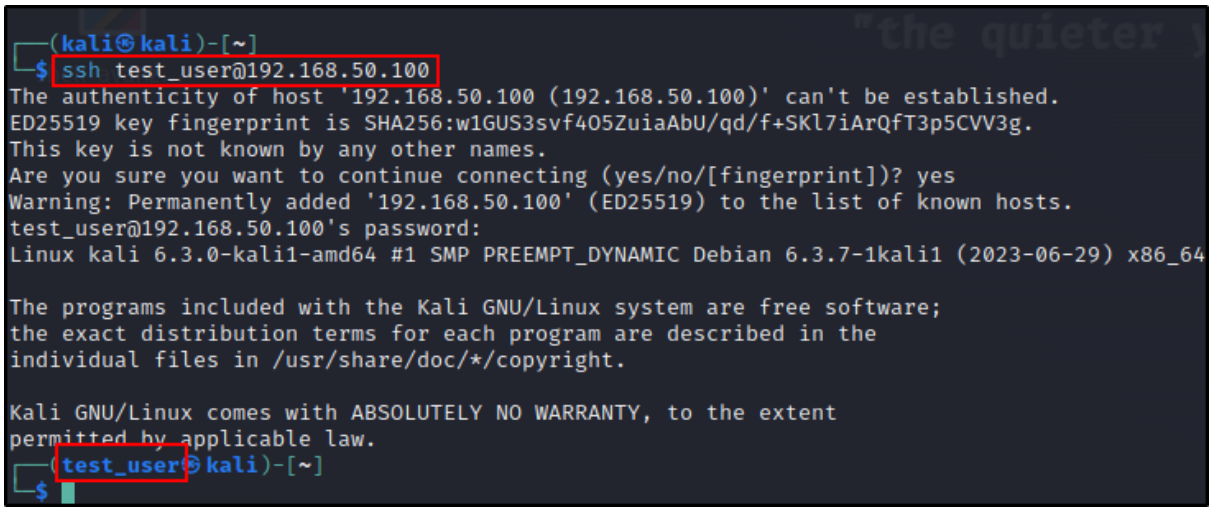
```
┌──(kali㉿kali)-[~]
└─$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1002) ...
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []: Test User
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Attiviamo il servizio ssh con il comando sudo service ssh start

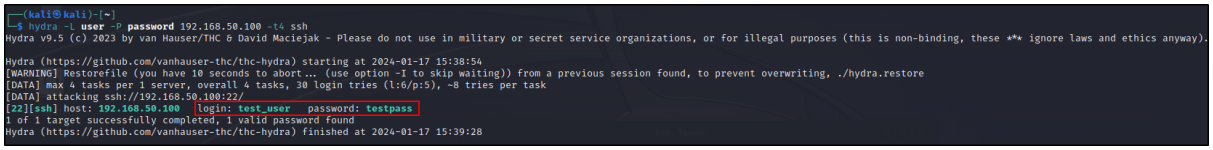
```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh start
```

Testiamo la connessione in SSH dell'utente appena creato sul sistema, eseguendo il comando seguente: ssh test_user@ip_kali, sostituite Ip_kali con l'ip della vostra macchina.

Se le credenziali inserite sono corrette, dovreste ricevere il prompt dei comandi dell'utente test_user sulla nostra Kali.



Possiamo attaccare l'autenticazione SSH con Hydra con il seguente comando, dove –l, e –p minuscole si usano se vogliamo utilizzare un singolo username ed una singola password. Ipotizziamo di non conoscere username e password ed utilizziamo invece delle liste per l'attacco a dizionario. Useremo gli switch –L, -P (notate che sono entrambe in maiuscolo).



Per la seconda parte dell'esercizio, scegliete un servizio da configurare e poi provate a craccare l'autenticazione con Hydra.

In questa fase ho deciso di attaccare il servizio Telnet della macchina Metasploitable presente all'indirizzo IP 192.168.50.101