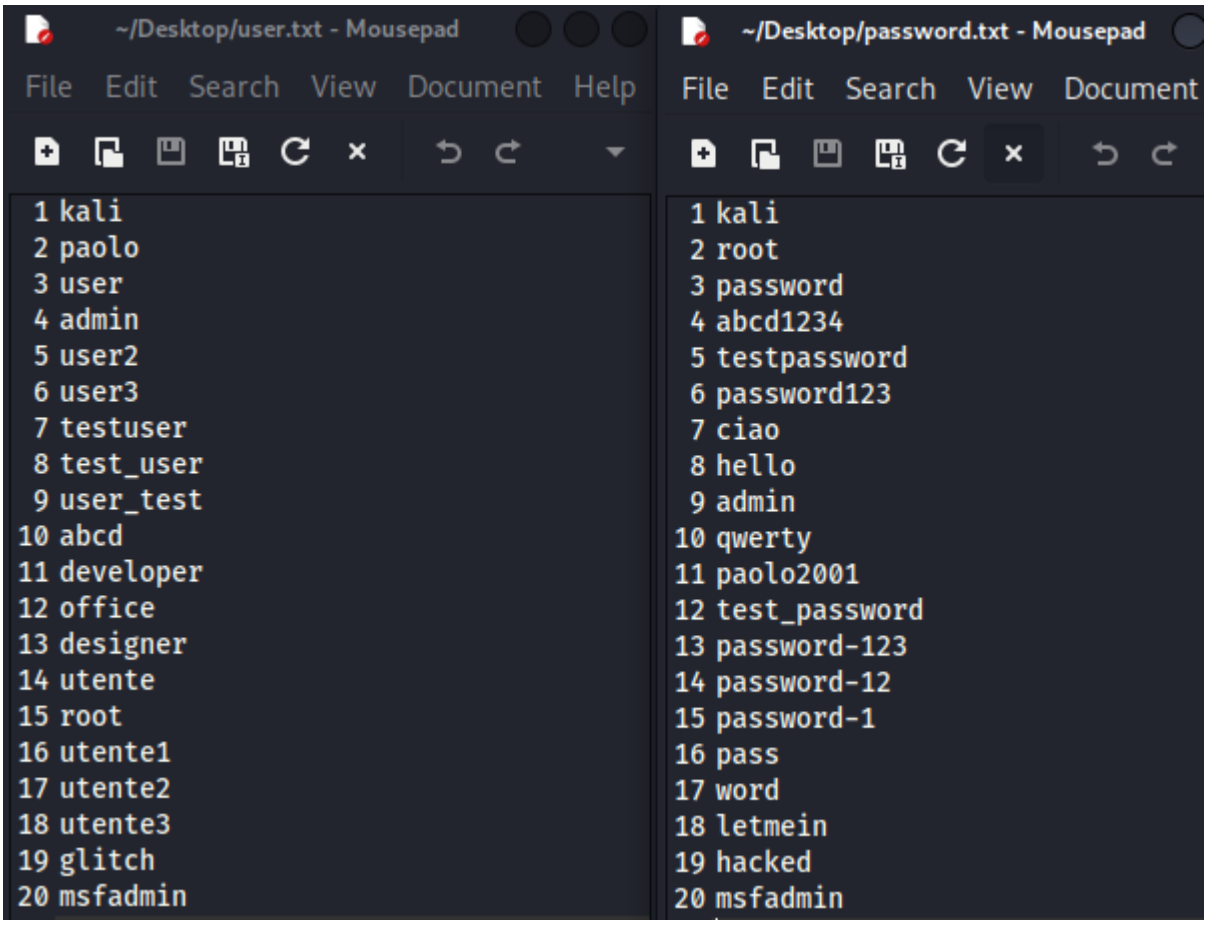
Authentication cracking con Hydra

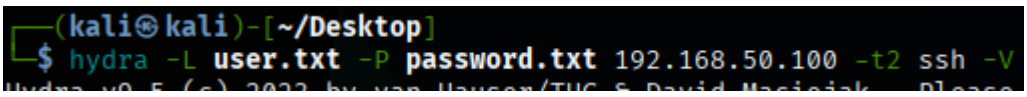
L'esercizio di oggi consiste nel crackare le password degli utenti nella macchina kali per accedere a vari servizi. I servizi che testato sono ssh, ftp e telnet.

Per prima cosa utilizzo il comando adduser e aggiungo un nuovo utente che chiamo testuser e imposto la password testpassword.

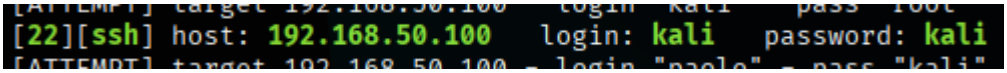
1. SSH
   Per iniziare il crack della password ho bisogno di due liste, una per gli utenti e una per le password. Ho creato queste liste da zero inserendo 20 possibili nomi utenti e 20 possibili password, in modo che poi hydra possa testare ogni utente con ogni password, arrivando quindi ad un totale di 400 combinazioni possibili.

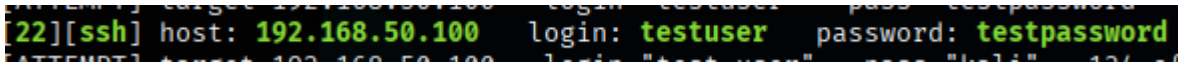


   Una volta create le liste posso iniziare l'attacco a forza bruta.
   Eseguo quindi il comando:



Grazie al parametro -V posso osservare in tempo reale tutti i tentativi per trovare le combinazioni giuste e ottengo:

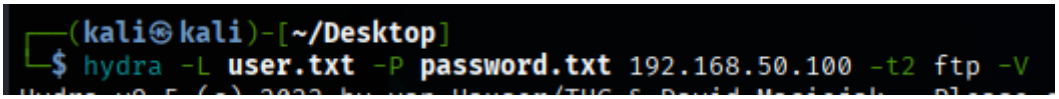




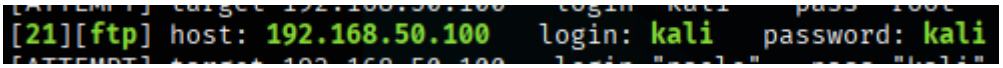
Alla fine del test abbiamo il messaggio di conclusione che specifica che il tool ha completato con successo il target impostato e ha trovato due password valide.

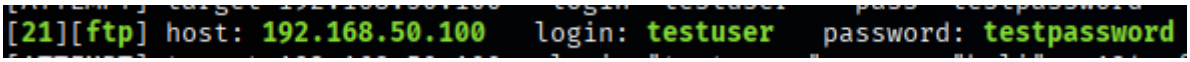
2. FTP
   Per craccare l'autenticazione su ftp con hydra dobbiamo prima installare il servizio. Eseguo quindi da terminale i comandi:
   1. sudo apt install vsftpd (per installare il servizio)
   2. service vsftpd start (per avviare il servizio)

   Una volta configurato il tutto eseguo l'attacco a forza bruta su ftp:



   I risultati sono gli stessi che trovavamo in precedenza:





3. Telnet
   Ho voluto testare anche sul servizio telnet (porta 23). Per prima cosa ho installato il servizio sulla mia macchina kali con il comando:

   sudo apt install telnet

   Successivamente ho installato openbsd-inetd con il comando:

   sudo apt install openbsd-inetd telnetd

   L'ho avviato con:

   sudo systemctl start inetd

   E ho avviato la comunicazione sulla porta 23 con:

   telnet 192.168.50.10 23 (ip metasploitable2)

Una volta avviata la comunicazione apro un terminale e avvio hydra con il comando:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L user.txt -P password.txt -t2 -d telnet://192.168.50.10 -V
```

Con il parametro -d attiviamo la modalità di debug. Dopo all'incirca 10 minuti la scansione termina e troviamo la corrispondenza.

```
[23][telnet] host: 192.168.50.10   login: msfadmin   password: msfadmin
fb 03ff fd01 fffd 1fff fb05 fffd 21    [ ..............!  ]
```