

# REPORT S6/L5

---

- Obiettivo:
- abilitazione di un servizio SSH e la relativa sessione di cracking dell'autenticazione con Hydra.
  - configurare e craccare un qualsiasi servizio di rete tra quelli disponibili, ad esempio ftp, rdp, telnet, autenticazione HTTP.

## SVOLGIMENTO

### FASE 1

Ho creato un nuovo utente su Kali Linux con il comando «*adduser*» mettendo come nome utente *test\_user* e come password *testpass*.

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

Ho poi il servizio ssh con il comando *sudo service ssh start*.

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

Successivamente ho testato la connessione in SSH dell'utente appena creato sul sistema eseguendo il comando `ssh test_user@127.0.0.1`

```
(kali㉿kali)-[~]
$ ssh test_user@127.0.0.1
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ED25519 key fingerprint is SHA256:Cpjz2teJdQzEpc0VSU0mEUdWnp19Ux5BSm9jzI07ViQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '127.0.0.1' (ED25519) to the list of known hosts.
test_user@127.0.0.1's password:
Linux kali 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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, avendo verificato l'accesso, configuro Hydra per tentare di individuare username e password dell'utente appena creato, utilizzando il dizionario SecLists.

```
(kali㉿kali)-[~]
$ sudo apt-get install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 2006 not upgraded.
Need to get 526 MB of archives.
After this operation, 2,082 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 seclists all 2024.4-0kali1 [526 MB]
Fetched 526 MB in 18s (30.0 MB/s)
Selecting previously unselected package seclists.
(Reading database ... 395823 files and directories currently installed.)
Preparing to unpack .../seclists_2024.4-0kali1_all.deb ...
Unpacking seclists (2024.4-0kali1) ...
Setting up seclists (2024.4-0kali1) ...
Processing triggers for kali-menu (2024.3.1) ...
Processing triggers for wordlists (2023.2.0) ...

(kali㉿kali)-[~]
$ █
```

Utilizzo il comando *hydra -L*

*/usr/share/seclists/Username/xato-net-10-million-username.txt -P*  
*/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt*  
per trovare username e password.

```
(kali@kali)-[~]
$ hydra -L /usr/share/seclists/Username/xato-net-10-million-username.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt 127.0.0.1 -t4 ssh -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).

[ATTEMPT] target 127.0.0.1 - login test_user - pass testpass - 8 of 8295465295457 [child 2] (0/0)
[22][ssh] host: 127.0.0.1 login: test_user password: testpass
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 1000002 of 8295465295457 [child 2] (0/0)
```

## FASE 2:

Per forzare l'autenticazione con Hydra di un servizio scelgo un servizio FTP.

Installo il servizio con il comando *sudo apt-get install vsftpd* e lo avvio con il comando *service vsftpd start*

```
(kali@kali)-[~]
$ sudo apt-get 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 2002 not upgraded.
Need to get 142 kB of archives.
After this operation, 352 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 vsftpd amd64 3.0.3-13.1 [142 kB]
Fetched 142 kB in 2s (84.1 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 402325 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.3-13.1_amd64.deb ...
Unpacking vsftpd (3.0.3-13.1) ...
Setting up vsftpd (3.0.3-13.1) ...
/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 (2.12.1-2) ...
Processing triggers for kali-menu (2024.3.1) ...

(kali@kali)-[~]
$ service vsftpd start
```

Successivamente utilizzo il comando *hydra -L*

*/usr/share/seclists/Username/xato-net-10-million-username.txt -P*  
*/usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt*  
*ftp://127.0.0.1* per craccare l'autenticazione dell'utente.

```
(kali㉿kali)-[~]  
└─$ hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/P  
asswords/xato-net-10-million-passwords-1000000.txt ftp://127.0.0.1  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret serv  
ice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics any  
way).  
  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-17 08:07:10  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previo  
us session found, to prevent overwriting, ./hydra.restore  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 8295465295457 login tries (l:8295457/p:1000001),  
~518466580967 tries per task  
[DATA] attacking ftp://127.0.0.1:21/  
[21][ftp] host: 127.0.0.1 login: test_user password: testpass  
[STATUS] 1000274.00 tries/min, 1000274 tries in 00:01h, 8295464295183 to do in 138219:52h, 16 active
```