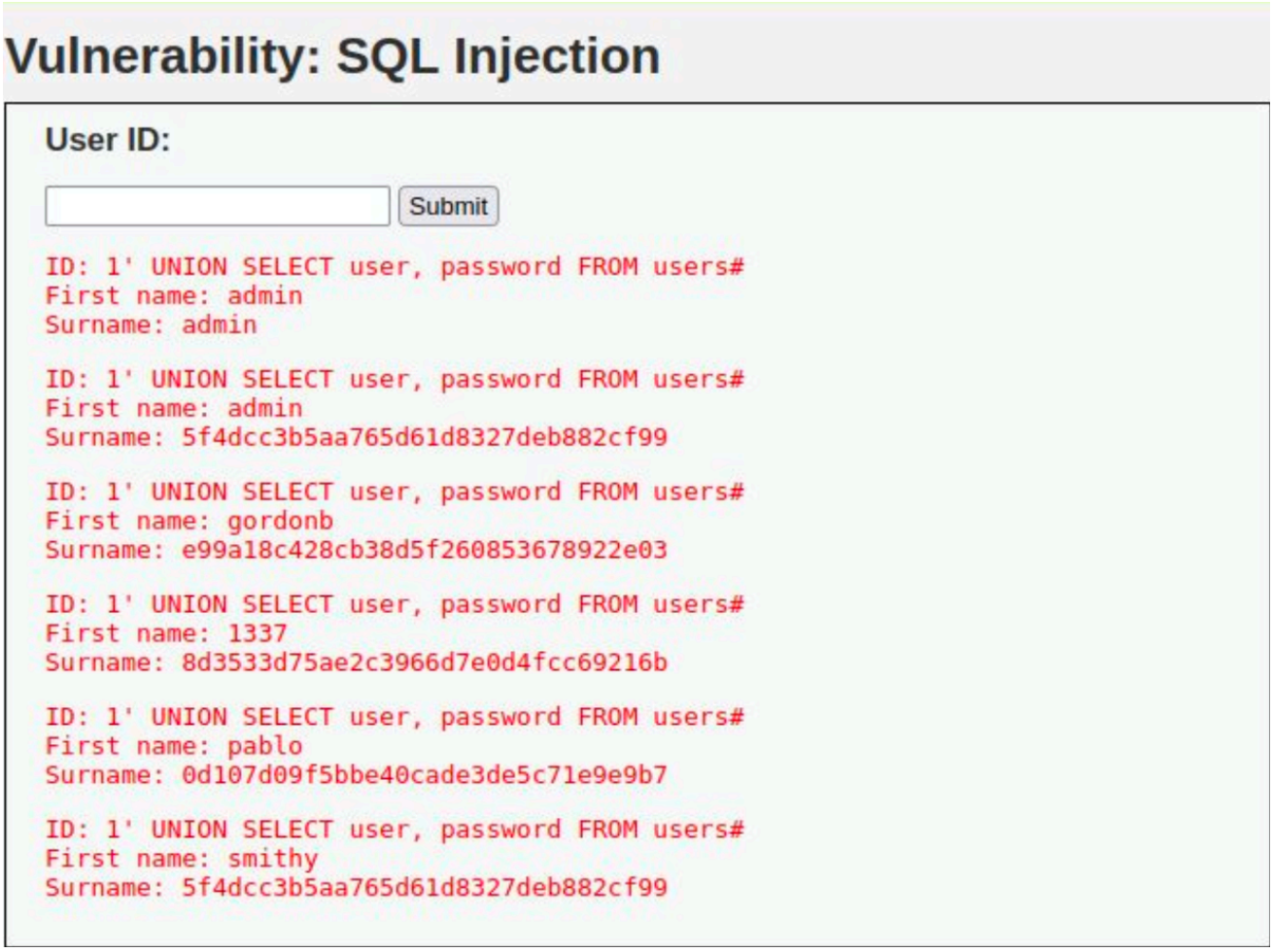
REPORT -TROUBLESHOOTING DI HASH CRACKING CON JTP - S6/L4

Target: Crack Passwords DVWA
Autore: Francesco Fontana
Data: 08/05/2025
Strumenti utilizzati: Kali Linux - Metaspoitable 2 - JTP (John the Ripper)
Obbiettivo: L'obiettivo in questa sessione è stato il crack passwords in DVWA sfruttando JTP nel terminale di Kali Linux e la wordlists (Rockyou)

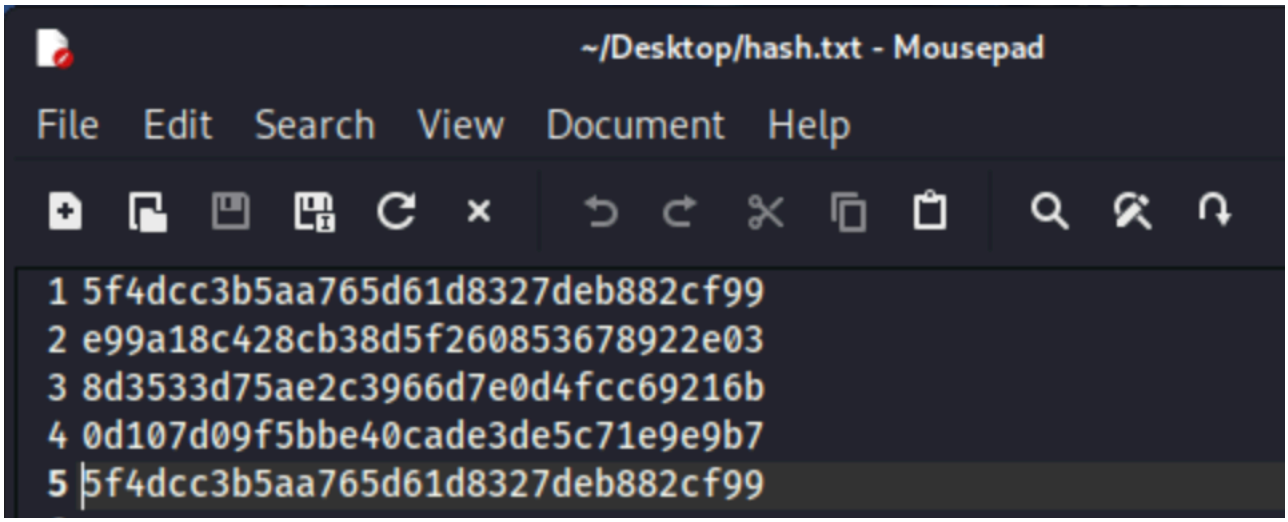
PANORAMICA DELL'ATTIVITÀ

1) Tramite un **SQL Injection** all'interno di DVWA, ho ottenuto le seguenti password da craccare inserendo questo comando:

1' UNION SELECT user, password FROM users#



2) Per craccare gli hash delle password MD5 utilizziamo JTR, ho creato un file.txt posto sul Desktop di Kali Linux, dove ho inserito tutti gli hash delle password:



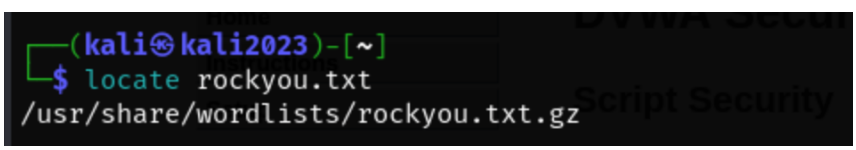
RISOLUZIONI

Risoluzione al Problema 1: Trovare e preparare una Wordlist

Per risolvere il problema della wordlist mancante, è stato necessario diverse soluzioni:

1. **Decomprimere il file rockyou.txt** presente in formato compresso:
   sudo gunzip /usr/share/wordlists/rockyou.txt.gz

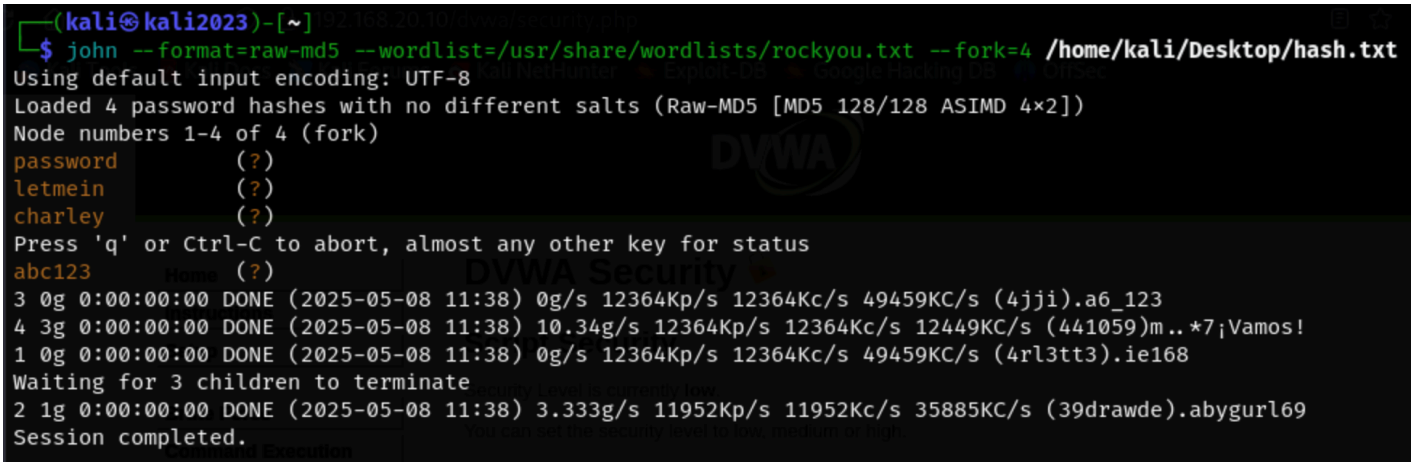
2. **Cercare il file nel sistema**:
   locate rockyou.txt



Risoluzione al Problema 2: Abilitare il Multithreading

Ho implementato l'opzione **--fork=4** come suggerito da alcune documentazioni per migliorare le prestazioni con il seguente comando:

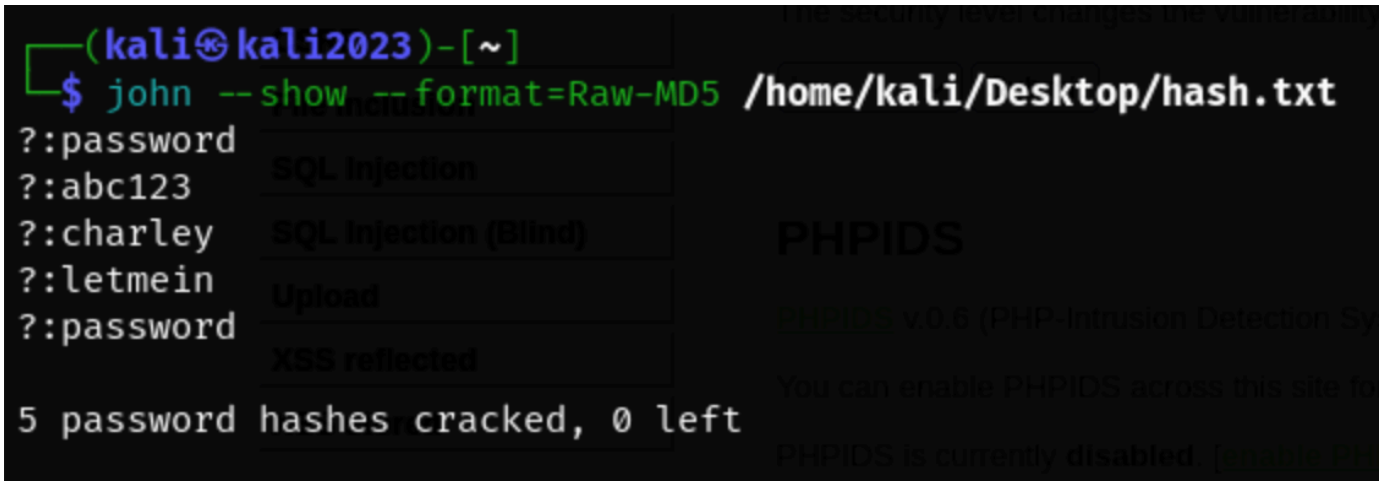
john --format=raw-md5 --wordlist=/home/kali/Desktop/mywordlist.txt --fork=4 /home/kali/Desktop/hash.tx



FASE FINALE

Una volta terminata la sessione di cracking, possiamo visionare le password craccate da JtR con il seguente comando:

john --show --format=Raw-MD5 /home/kali/Desktop/hash.txt



CONCLUSIONI E RACCOMANDAZIONI

Per un efficace cracking di hash MD5 con John the Ripper, si raccomanda di:

1. Utilizzare sempre file separati per wordlist e hash
2. Implementare l'opzione **--fork** su sistemi multi-core per migliorare le prestazioni
3. Verificare la disponibilità e l'integrità dei file wordlist prima di iniziare
4. Considerare l'utilizzo di wordlist più ampie per aumentare le probabilità di successo

Per sessioni future, potrebbe essere utile esplorare opzioni aggiuntive come regole di mangling o attacchi basati su maschere per migliorare l'efficacia del processo di cracking.