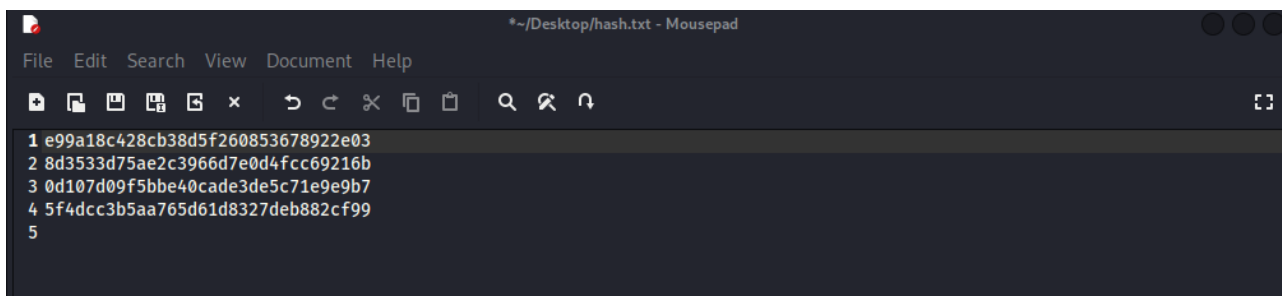


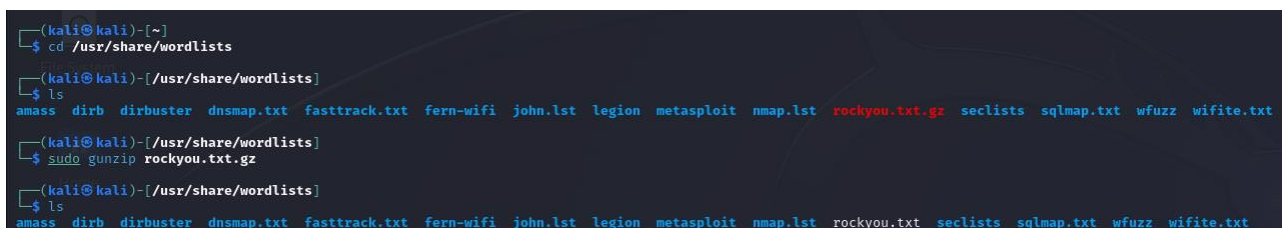
S6L3

L'esercizio di oggi consiste nel craccare le password ottenute tramite un attacco SQL injection sulla DVWA della macchina Metasploitable. Le password sono state salvate su un file chiamato "hash.txt".



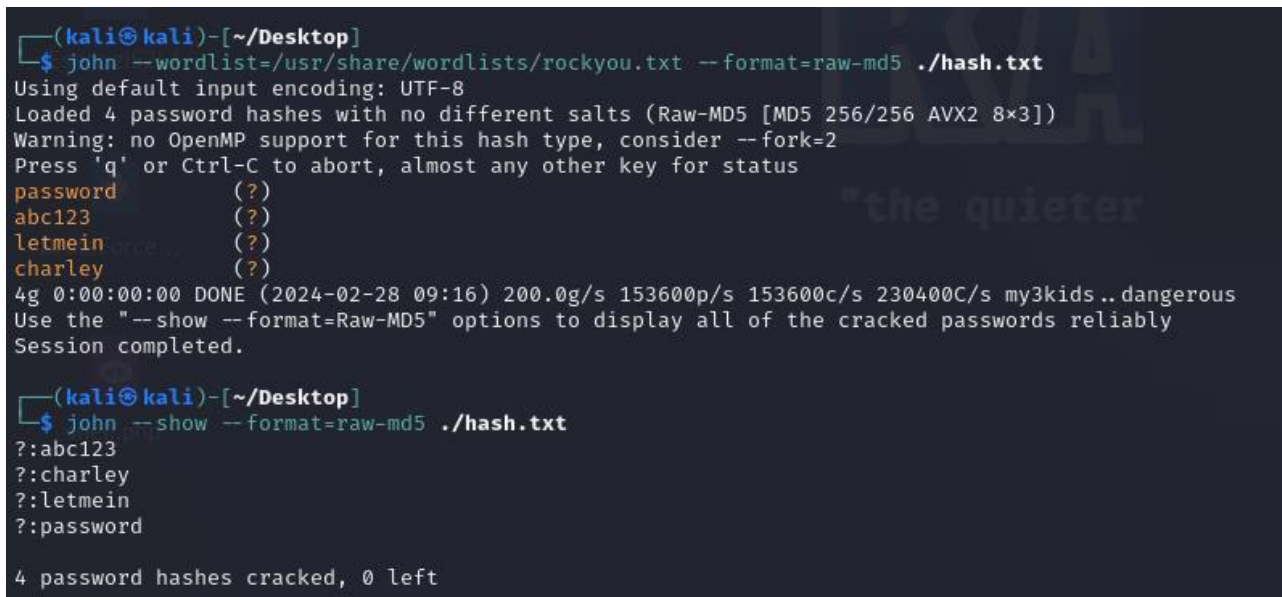
```
*~/Desktop/hash.txt - Mousepad
File Edit Search View Document Help
1 e99a18c428cb38d5f260853678922e03
2 8d3533d75ae2c3966d7e0d4fcc69216b
3 0d107d09f5bbe40cade3de5c71e9e9b7
4 5f4dcc3b5aa765d61d8327deb882cf99
5
```

Di conseguenza, dopo aver installato le liste tramite il comando "sudo apt install seclists", ho controllato che esistesse il file "rockyou.txt", e ho dovuto estrarre il file come mostrato nell'immagine.



```
(kali@kali)-[~]
$ cd /usr/share/wordlists
(kali@kali)-[/usr/share/wordlists]
$ ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt.gz seclists sqlmap.txt wfuzz wifite.txt
(kali@kali)-[/usr/share/wordlists]
$ sudo gunzip rockyou.txt.gz
(kali@kali)-[/usr/share/wordlists]
$ ls
amass dirb dirbuster dnsmap.txt fasttrack.txt fern-wifi john.lst legion metasploit nmap.lst rockyou.txt seclists sqlmap.txt wfuzz wifite.txt
```

Dopo ho reso il file "rockyou.txt" come lista delle chiavi di criptazione delle password del file "hash.txt"



```
(kali@kali)-[~/Desktop]
$ john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 ./hash.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
password (??)
abc123 (??)
letmein (??)
charley (??)
4g 0:00:00:00 DONE (2024-02-28 09:16) 200.0g/s 153600p/s 153600c/s 230400C/s my3kids..dangerous
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

(kali@kali)-[~/Desktop]
$ john --show --format=raw-md5 ./hash.txt
?:abc123
?:charley
?:letmein
?:password

4 password hashes cracked, 0 left
```