

## S6.L3 Le fasi di Exploit

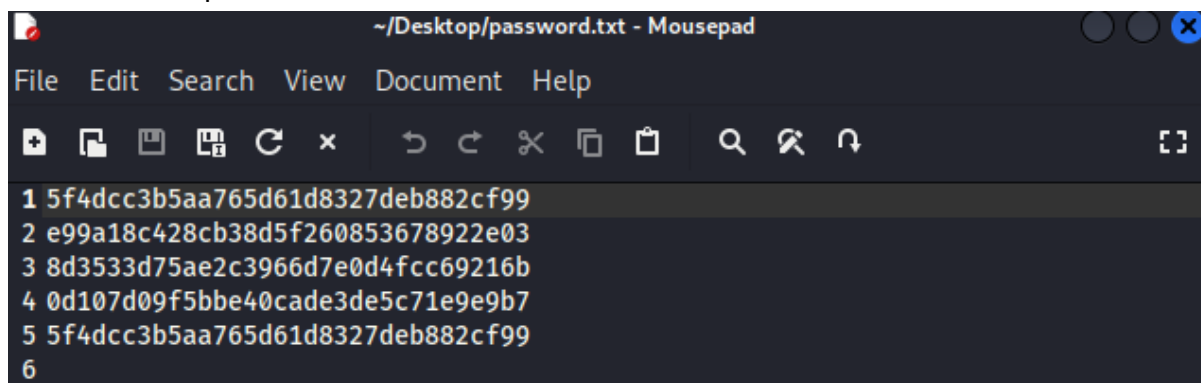
Se osserviamo meglio le password dalla lezione precedente, notiamo che non sembrano essere in chiaro, ma piuttosto degli hash di password MD5.

Recuperate le password dal database e provate a effettuare sessioni di cracking per ottenere la versione in chiaro delle password. Potete utilizzare qualsiasi strumento che è stato discusso nella lezione teorica.

L'obiettivo dell'esercizio di oggi è riuscire a decifrare tutte le password.

### Fase 1: Creazione file di testo con password formato ash

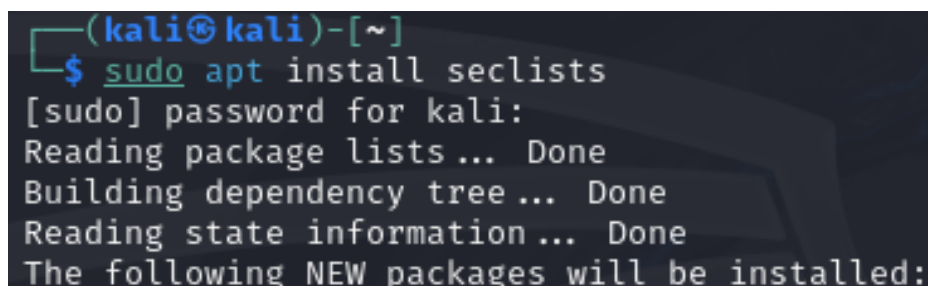
per prima cosa vado a creare un editor di testo che nomineremo password.txt dove andremo ad inserire le 5 password in formato hash



```
~/Desktop/password.txt - Mousepad
File Edit Search View Document Help
1 5f4dcc3b5aa765d61d8327deb882cf99
2 e99a18c428cb38d5f260853678922e03
3 8d3533d75ae2c3966d7e0d4fcc69216b
4 0d107d09f5bbe40cade3de5c71e9e9b7
5 5f4dcc3b5aa765d61d8327deb882cf99
6
```

### Fase 2: lista password

successivamente vado a scaricare i dizionari per sfruttare la ricerca delle password:



```
(kali@kali)-[~]
$ sudo apt install seclists
[sudo] password for kali:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
```

### Fase 3: John the ripper

Ho eseguito un attacco di password cracking utilizzando John the Ripper per decifrare gli hash di password MD5 presenti nel file password.txt. Ecco una spiegazione tecnica e dettagliata del processo:

### Navigazione alla directory Desktop:

cd ~/Desktop

mi sono spostato nella directory Desktop dove si trova il file password.txt.

### Esecuzione di John the Ripper:

**john --incremental --format=raw-md5 password.txt**

- john: Comando per avviare John the Ripper.
- --incremental: Opzione che avvia un attacco di tipo incrementale, il quale prova tutte le combinazioni possibili di caratteri.
- --format=raw-md5: Specifica il formato degli hash nel file password.txt, in questo caso raw-md5 che indica hash MD5 non salati.
- password.txt: Il file di input contenente gli hash delle password da decifrare.

```
(kali@kali)-[~/Desktop]
$ john --incremental --format=raw-md5 password.txt

Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4x3])
Warning: no OpenMP support for this hash type, consider --fork=2
Press 'q' or Ctrl-C to abort, almost any other key for status
abc123      (?)
charley     (?)
password    (?)
letmein     (?)
4g 0:00:00:00 DONE (2024-05-16 08:32) 5.194g/s 3316Kp/s 3316Kc/s 3893KC/s letebru..letmish
Warning: passwords printed above might not be all those cracked
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

### Output del comando:

- John the Ripper ha caricato 4 hash di password differenti (Raw-MD5).
- È stato mostrato un avviso riguardante il supporto OpenMP per questo tipo di hash e una raccomandazione di usare l'opzione --fork=2 per migliorare le prestazioni.
- John the Ripper ha identificato le seguenti password:
  - abc123
  - charley
  - password
  - letmein
- La velocità di cracking è stata di 5.194k password al secondo.

### Conclusione dell'operazione:

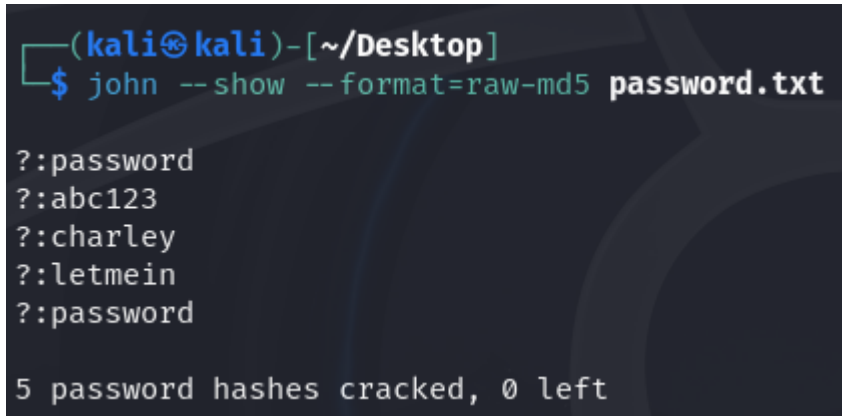
- John the Ripper ha completato la sessione di cracking e ha avvisato che le password mostrate potrebbero non essere tutte quelle decifrate.
- Raccomanda di usare l'opzione --show --format=Raw-MD5 per visualizzare tutte le password decifrate in modo affidabile.

In sintesi, ho utilizzato John the Ripper per decifrare hash di password MD5 presenti nel file password.txt attraverso un attacco incrementale. Le password decifrate sono state abc123, charley, password, e letmein.

## Fase 4: Stampa delle password

Ho utilizzato John the Ripper per visualizzare le password decifrate dagli hash MD5 nel file password.txt con il comando:

```
john --show --format=raw-md5 password.txt
```

A screenshot of a terminal window with a dark background. The prompt is '(kali@kali)-[~/Desktop]'. The command '\$ john --show --format=raw-md5 password.txt' has been executed. The output shows five lines, each starting with a question mark and a colon, followed by a password: '?:password', '?:abc123', '?:charley', '?:letmein', and '?:password'. At the bottom, it says '5 password hashes cracked, 0 left'.

```
(kali@kali)-[~/Desktop]
$ john --show --format=raw-md5 password.txt

?:password
?:abc123
?:charley
?:letmein
?:password

5 password hashes cracked, 0 left
```

**Le password decifrate sono:**

password  
abc123  
charley  
letmein  
password

John the Ripper ha confermato di aver decifrato con successo tutti e 5 gli hash di password presenti nel file, mostrando le versioni in chiaro delle password.