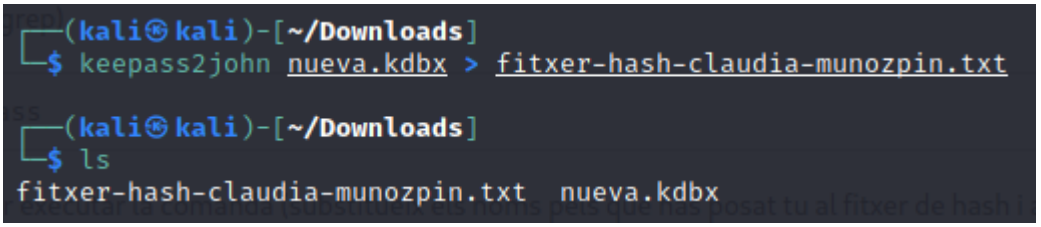
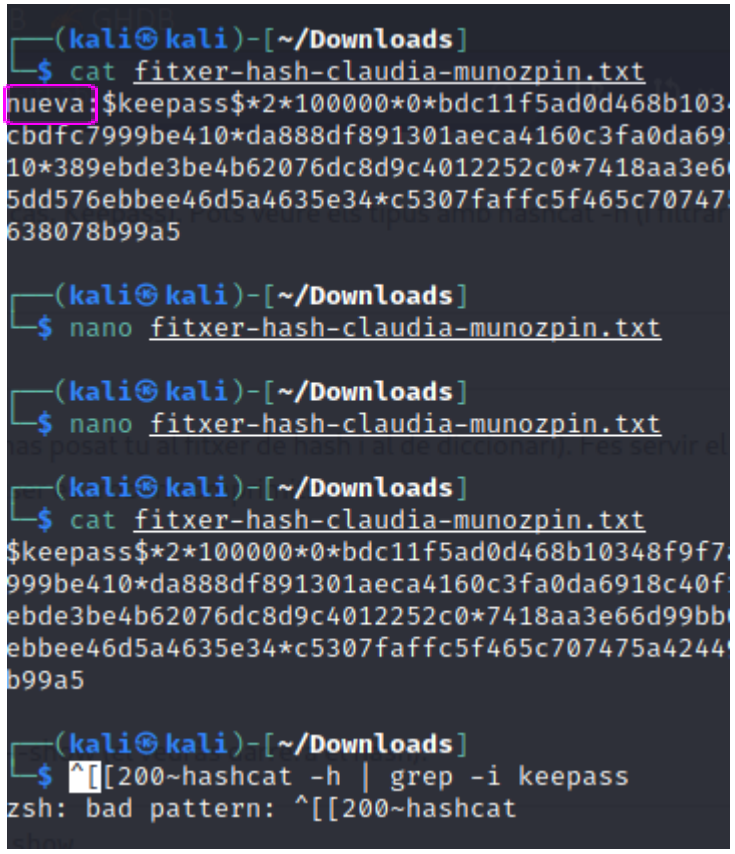
Claudia Fu Muñoz Pin

Gestor de contrasenyes

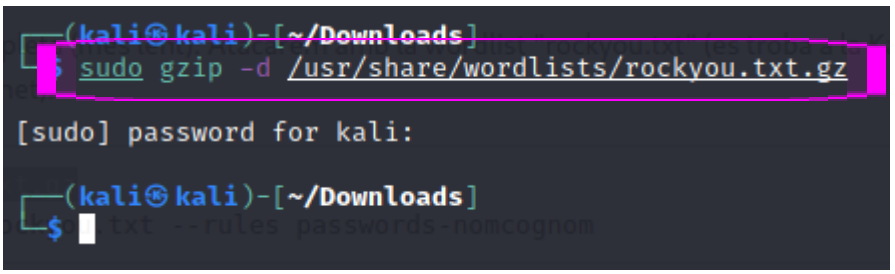
Primer descarreguem el nueva.kdbx. A continuació al convertirem en un arxiu .txt



Després li farem un nano per borrar el nueva: que té [rectangle rosa]



Un cop ja fet descomprimir amb la següent [Quadre rosa] comanda el diccionari rockyou.txt



Un cop l'hem descomprimit instal·larem el keepassx.

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install keepassx
[sudo] password for kali:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
keepassx is already the newest version (2.0.3+git20190121.1682ab9-2.2).
The following packages were automatically installed and are no longer require
d:
```

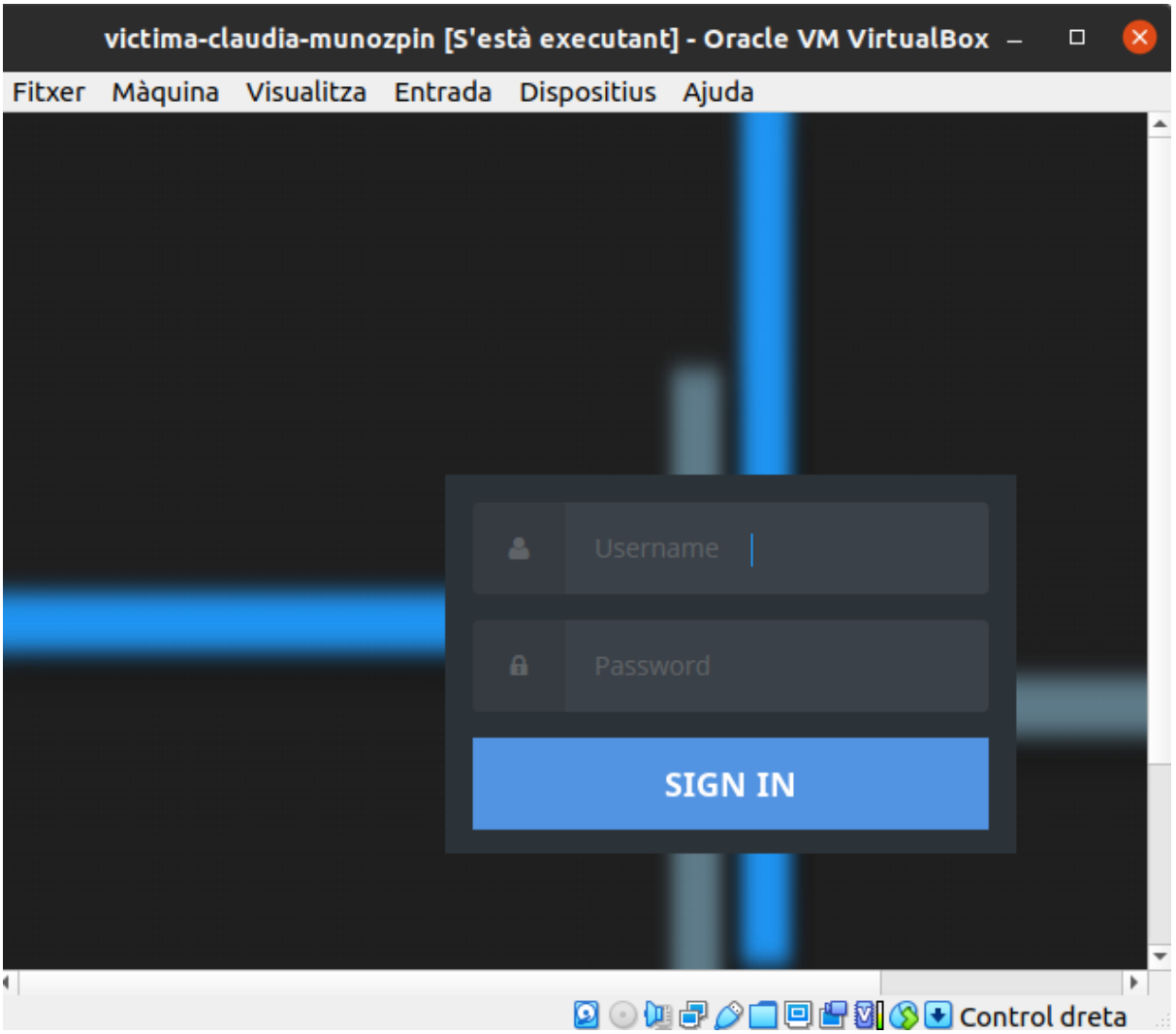
Després mirarem quin codi hashcat té el nostre keepass amb la següent comanda. Després agafarem el nostre codi i comprovarem amb el diccionari quina contrasenya té l'arxiu de keepass.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -h |grep -i keepass                                        255 ×
  13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES)      | Password Manager
s

┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -m 13400 -a 0 fitxer-hash-claudia-munozpin.txt /usr/share/wordlis
ts/rockyou.txt
hashcat (v6.1.1) starting ...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DIST
RO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================
* Device #1: pthread-Intel(R) Core(TM) i5-4460  CPU @ 3.20GHz, 1423/1487 MB (
512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
```

Un cop ha acabat el procés al final de la comanda posarem --show i ens mostrarà la contrasenya.

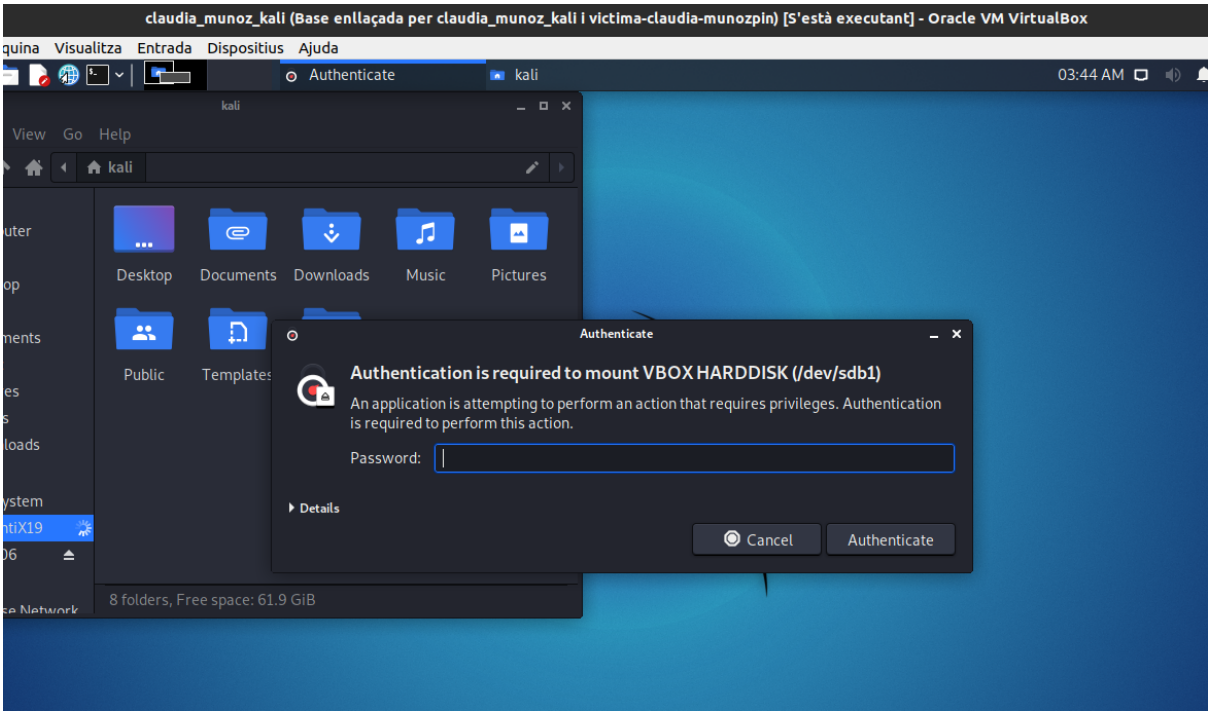
```
┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -m 13400 -a 0 fitxer-hash-claudia-munozpin.txt /usr/share/wordlis
ts/rockyou.txt -show
The specified parameter cannot use 'how' as a value - must be a number.

┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -m 13400 -a 0 fitxer-hash-claudia-munozpin.txt /usr/share/wordlis
ts/rockyou.txt --show
$keepass$*2*100000*0*bdc11f5ad0d468b10348f9f7adba6ff03585d6dce203bcb5bdcbdfc7
999be410*da888df891301aeca4160c3fa0da6918c40f173d75ffc9fa7a28075ae0c4e910*389
ebde3be4b62076dc8d9c4012252c0*7418aa3e66d99bb00c595498ddcfa244cbbac9cbf5dd576
ebbee46d5a4635e34*c5307faffc5f465c707475a424497549e8fd10c77f1e49059d75a638078
b99a5:mnbvcxz1
```

Segona Part

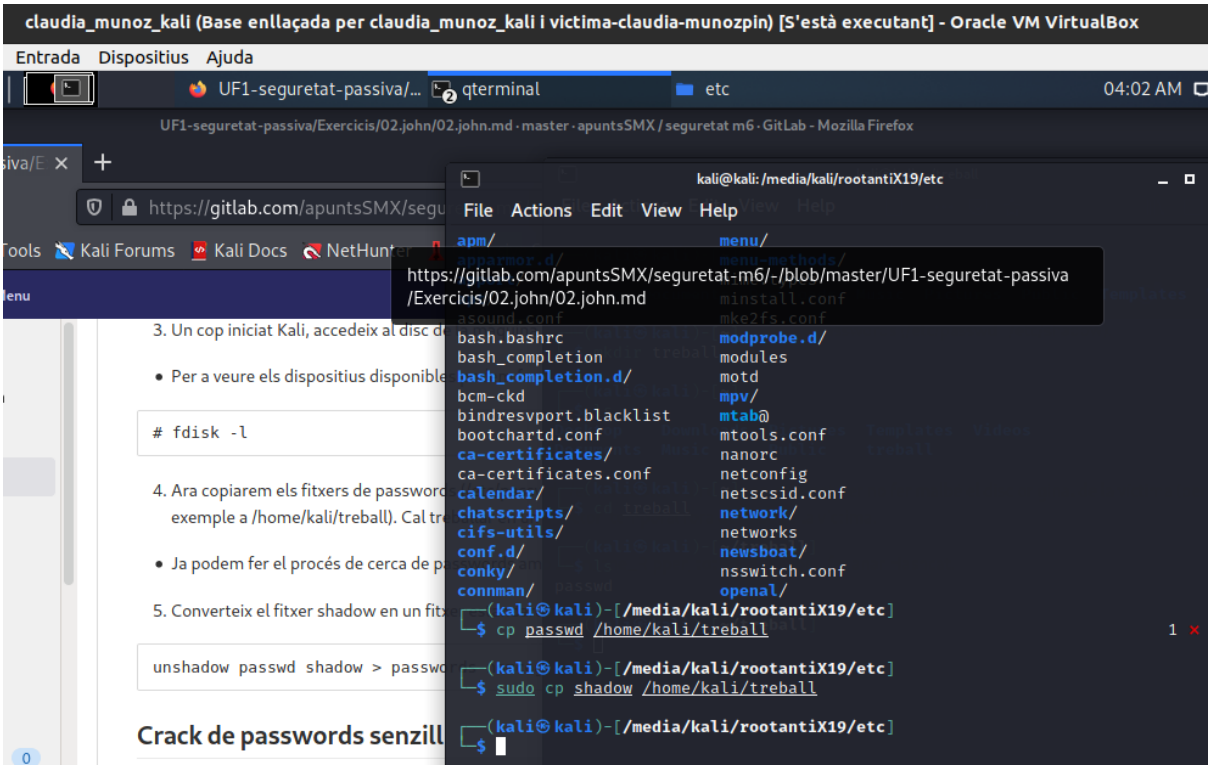


Com podem veure al intentar iniciar el disc dur del Keepassx no podrem ja que no tenim les contrasenyes ni els usuaris. Per tatn posarem aquest disc dur a la nostre maquina i desde allà el terminal buscarem les contrasenyes i els usuaris.

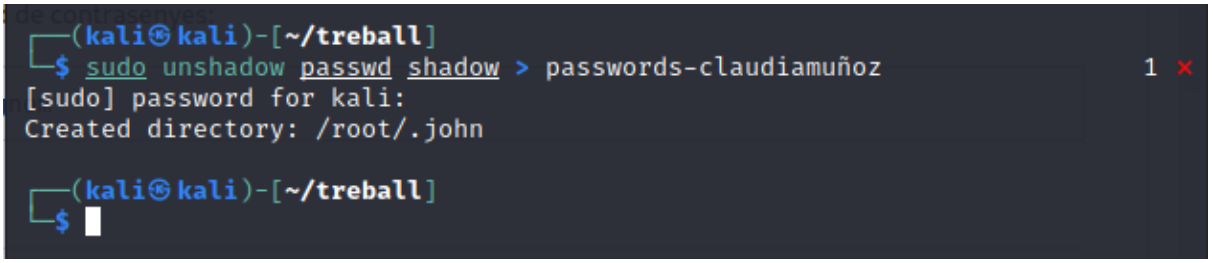
Un cop hem entrat al disc dur desde la nostre maquina kali ens demana-ra una contrasenya y haurem de posar kali.



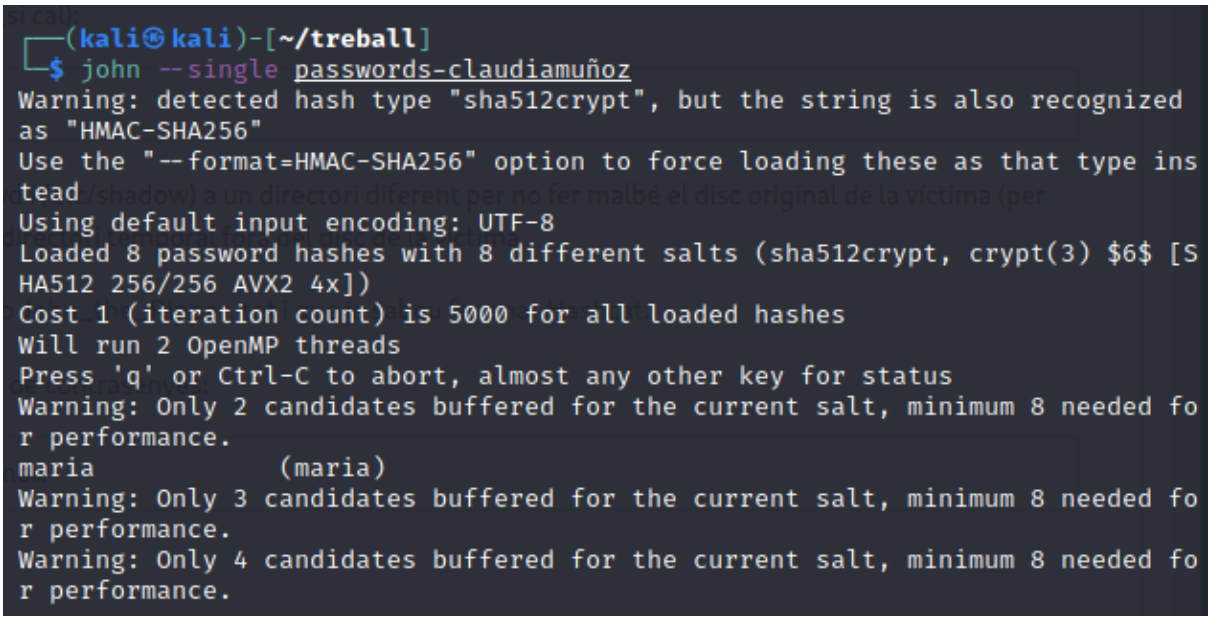
Després es anirem a la carpeta /etc/ i haurem de copiar el password a una carpeta externa del disc dur, en el meu cas en la nostre maquina. la comanda que utilitzarem serà cp passwd (directori don el volem copiar). Farem el mateix amb la carpeta shadow.



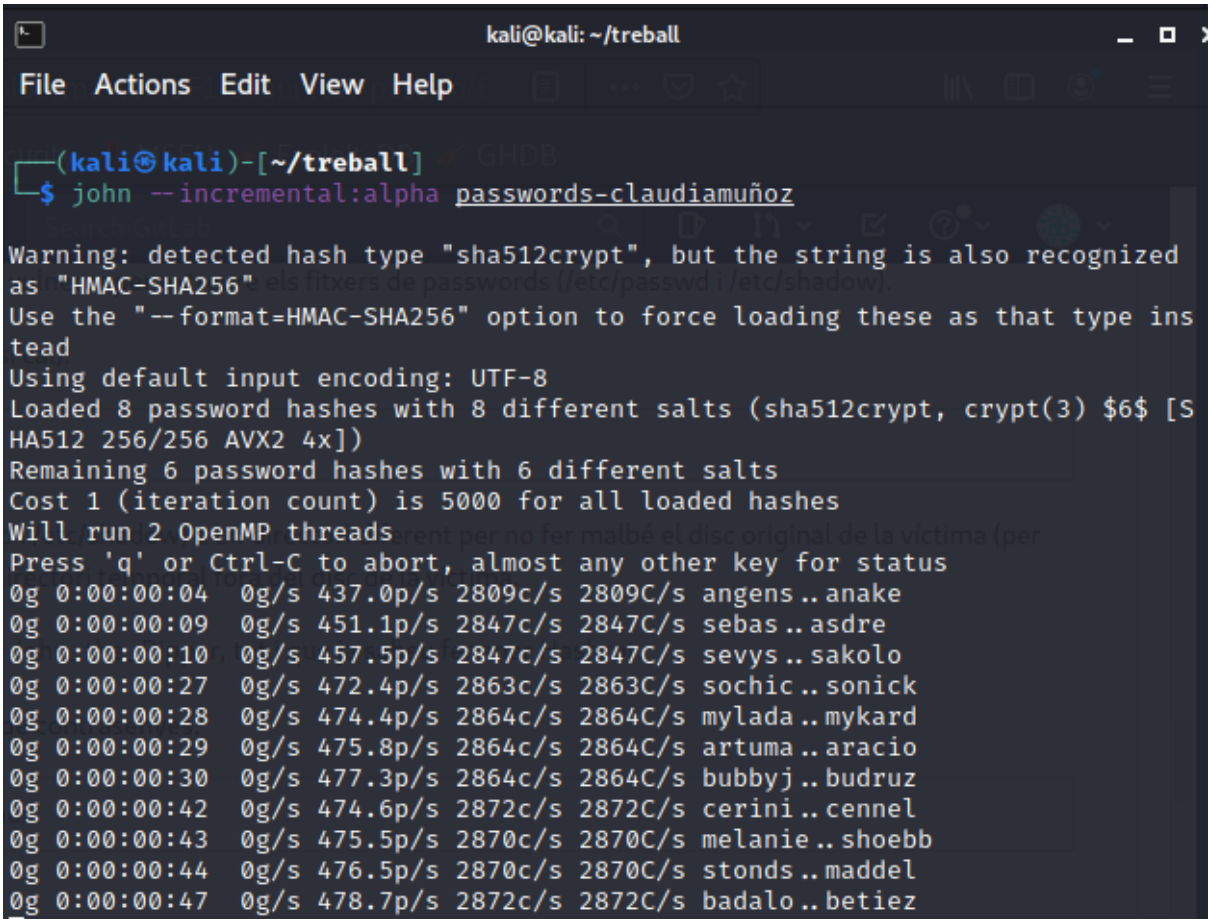
Quan l'hagim fet amb la següent comanda convertirem el fitxer shadow en un fitxer estàndard de contrasenyes:

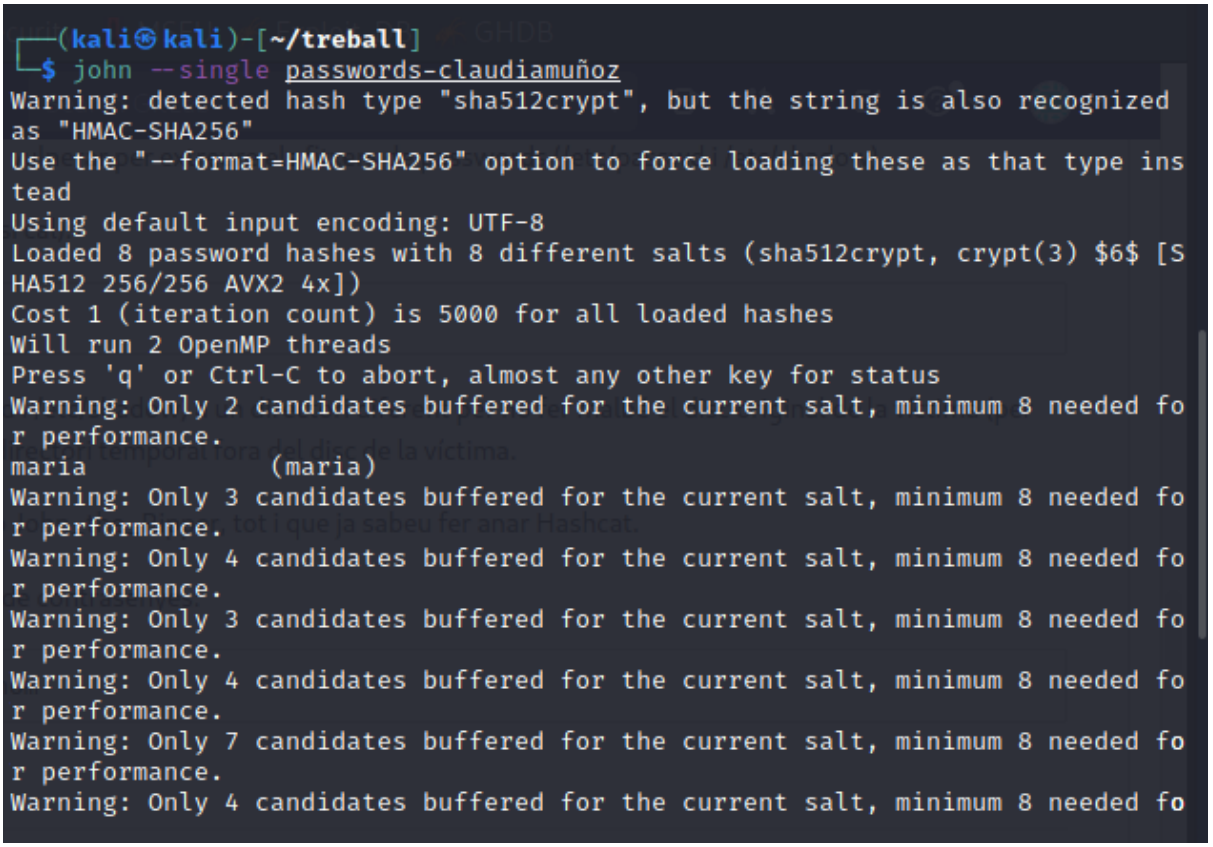


Després executarem la següent comanda què serà l'opció curt de buscar rapid els usuaris i les seves contrasenyes.



Amb aquesta comanda ho farem de la forma curta pero en el cas de no tindre diccionari. A mes a mes haurem de indicar-em quins caràcters ha de fer servir. com per ex: alpha.





Ara executem John amb un diccionari (wordlist) i li diem que generi variacions d'aquestes contrasenyes. Comanda a utilitzar: *# john --wordlist=/usr/share/wordlists/rockyou.txt --rules passwords-nomcognom*

```
┌──(kali㉿kali)-[~/treball]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --rules passwords-claudi
amuñoz
Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading these as that type ins
tead
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [S
HA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)
```

Un cop fet tot per aclarirme el que he fet ha sigut posar la següent contrasenya per a que em digui els usuaris i contrasenyes més organitzat.

```
┌──(kali㉿kali)-[~/treball]
└─$ john --show passwords-claudiamuñoz
root:buster69:0:0:root:/root:/bin/bash
joan:alexis15:1000:1000::/home/joan:/bin/bash
maria:maria:1001:1001:,,,:/home/maria:/bin/bash
jordi:jordi123:1002:1002:,,,:/home/jordi:/bin/bash
kiko:aabbcc:1003:1003:,,,:/home/kiko:/bin/bash
albert:packers1:1004:1004:,,,:/home/albert:/bin/bash
felip:homeandaway:1005:1005:,,,:/home/felip:/bin/bash
oscar:motorolav3:1006:1006:,,,:/home/oscar:/bin/bash

8 password hashes cracked, 0 left
```

```
motorolav3       (oscar)
4g 0:00:01:10 0.00% (ETA:
2007..gillespie
4g 0:00:01:11 0.01% (ETA:
69..colorada
4g 0:00:01:12 0.01% (ETA:
o1..091785
4g 0:00:01:13 0.01% (ETA:
T..021007
alexis15         (joan)
buster69         (root)
```

Usuari	Contrasenya
maria	maria
jordi	jordi123
albert	packers1
felip	homeandaway
kiko	aabbcc
oscar	motorolav3
joan	alexis15
root	buster69

A les imatges següents podem veure com hem pogut entra en el root sense cap problema i en un usari.