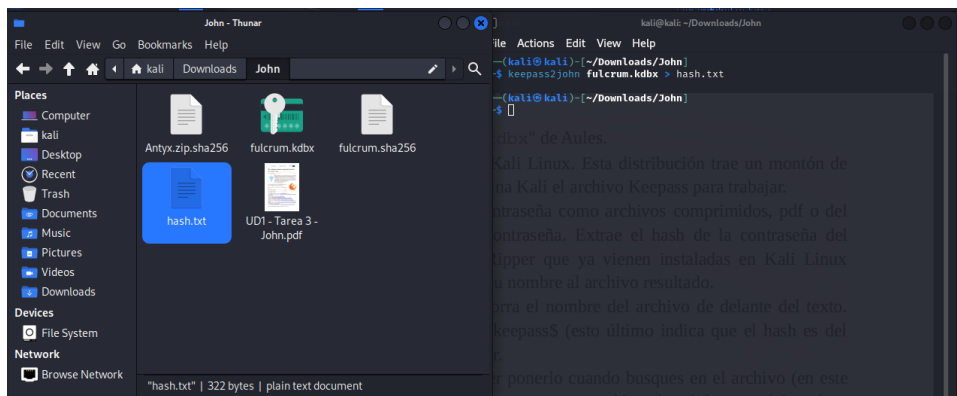
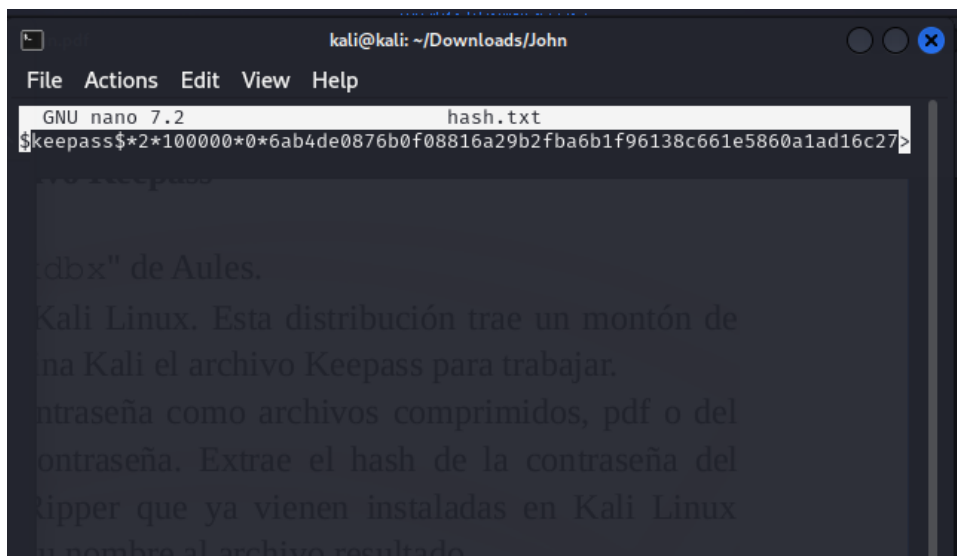


# Usamos john para sacar hash.txt

keepass2john file.bdbx > hash.txt



Eliminamos la palabra fullcrum del archivo hash.txt



Ejecutamos el comando (el diccionario tiene que estar descomprimido)

[illegible]

```
[john@kali] ~/Downloads/John
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt.gz hash.txt > prueba.txt
Using default input encoding: UTF-8
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:04 0.31k (ETA: 05:05:09) 0g/s 91.93p/s 91.93c/s 91.93C/s **H*
N
L***e**9R***o*$?~j+c*xl%*xxt+*o+h*o*o*Q*|*|c#NB=**q
Warning: UTF-16 BOM seen in wordlist. File may not work properly unless you re-encode it
0g 0:00:24:58 DONE (2023-09-25 05:08) 0g/s 91.66p/s 91.66c/s 91.66C/s H*-||*|*|*;*E!S*****x.....R...o*o*R...)-----lQ*{*(AC*****
Session completed.
```



```
[kali@kali] (~/.Downloads/John)
└─$ john --format=KeepAss --wordlist=/usr/share/wordlists/rockyou.txt.gz hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeepAss [SHA256 AES 32/64])
Cost 1 (iteration count) is 100000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00.09 1.29% (ETA: 05:35:48) 0g/s 176.6p/s 176.6c/s 176.6C/s _hw!(♦Q2-♦#0..1l!Rt♦♦♦daX♦♦♦`a<♦Zy|FPD♦
BE65
```

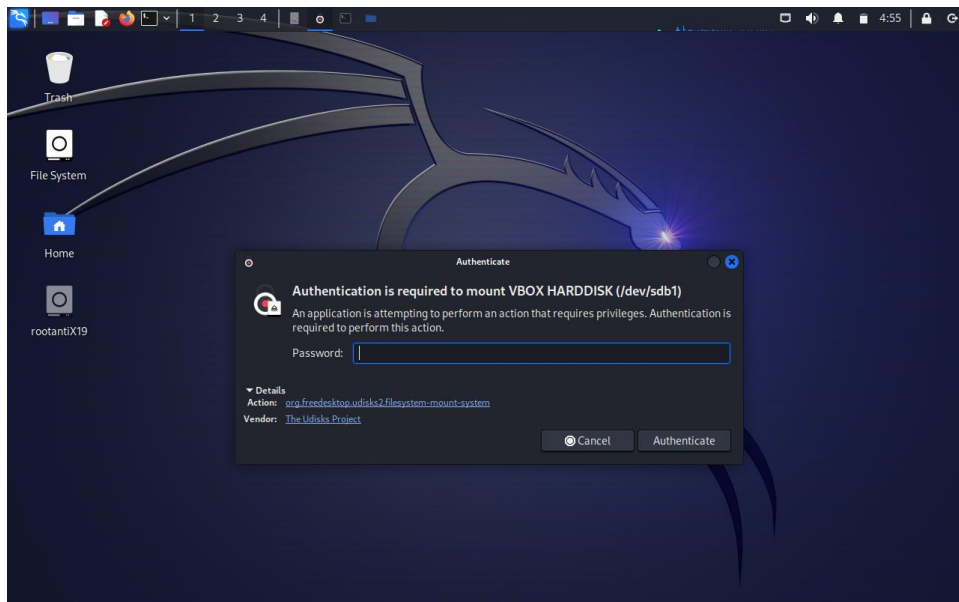
Terminara y con `-show` sacaremos la contraseña

```
(kali㉿kali)-[~/Downloads/John]
$ john --show hash.txt
?:mindgame
1 password hash cracked, 0 left
(kali㉿kali)-[~/Downloads/John]
$
```

Volcamos la unidad descargada en la maquina virtual de kali

Controlador: SATA

-  kali-linux-23-24-disk001.vdi
-  Antyx.vdi



Vamos a comprobar `/etc/passwd` y `/etc/shadow`

Etc/passwd

```
GNU nano 7.2 passwd.txt
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
messagebus:x:101:101::/nonexistent:/usr/sbin/nologin
usbmux:x:102:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
_rpc:x:103:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:104:65534::/var/lib/nfs:/usr/sbin/nologin
joan:x:1000:1000::/home/joan:/bin/bash
maria:x:1001:1001::/home/maria:/bin/bash
jordi:x:1002:1002::/home/jordi:/bin/bash
kiko:x:1003:1003::/home/kiko:/bin/bash
albert:x:1004:1004::/home/albert:/bin/bash
felip:x:1005:1005::/home/felip:/bin/bash
oscar:x:1006:1006::/home/oscar:/bin/bash
```

Etc/shadow

```
GNU nano 7.2 shadow.txt
root:$6$MmNTxZgy7aF5$ZHeZLXCcbQg[eUsHXyZb1m5j7jPkSpzdTDHdJMw1xTuBjHT7a9Jb3xEK3TVvq3z75khhIpcVx9x16mfh.4/:18892:0:99999:7:::
daemon:*:18767:0:99999:7:::
bin:*:18767:0:99999:7:::
sys:*:18767:0:99999:7:::
sync:*:18767:0:99999:7:::
games:*:18767:0:99999:7:::
man:*:18767:0:99999:7:::
lp:*:18767:0:99999:7:::
mail:*:18767:0:99999:7:::
news:*:18767:0:99999:7:::
uucp:*:18767:0:99999:7:::
proxy:*:18767:0:99999:7:::
www-data:*:18767:0:99999:7:::
backup:*:18767:0:99999:7:::
list:*:18767:0:99999:7:::
irc:*:18767:0:99999:7:::
gnats:*:18767:0:99999:7:::
nobody:*:18767:0:99999:7:::
_apt:*:18767:0:99999:7:::
messagebus:*:18767:0:99999:7:::
usbmux:*:18767:0:99999:7:::
_ftp:*:18767:0:99999:7:::
statd:*:18767:0:99999:7:::
joan:$6$X8lGwZLDJ13s3J7w5/q07sb0GgLCqfa22aM/TsHMGvYuketjSTuZMAewmMtw0NA9Vz320e.umPeLLg3fcpwGhno0cJ5EY152n/qVX0:18892:0:99999:7:::
maria:$6$5bhpP.rnkv8qQm4q1W51K3jhw3jeh2APKz1NhiwE37upp7KHG.jbaMtd5XMAAhtdzQg5fnaBmhlld31ln1SHdE.ph0y0eFVPR0C/:18892:0:99999:7:::
jordi:$6$z1z5JwW877PSYrB5LH0oLUTnCGrp81HF0HML5n1fmHaHn8joaGmwyv16359j6.NkL2CsyeLvgQtUJfBa2Urze1QHrY71VoOX138.:18892:0:99999:7:::
kiko:$6$11FyhInPFTIHdV/T$5iMt1Jx/y5vX04Y8Q59.ofSTLfp567EdvWYQpvdBMrLwUufm6otZzr1cN9m0vY77Q.dKzALFN/201PzzB3/:18892:0:99999:7:::
albert:$6$Z3Zv6EzUzUpJN6E57usqCZUFmD96E12xEUmGy0THdhJeyVvSU2dMuhzpgNHJfzu5.0WwAG8Tm6m1XCv7a964cf8zx1Sgyxtgv01:18892:0:99999:7:::
felip:$6$uPFb2IDqoW0jZn5f0wcAwG3r.f480IR3rShjnt0QJyaNBZaym3w3J5lnKs3/XJ1LbCLpCXA0eSml7vlt0h0pc77Z4p2LT9bcy.:18892:0:99999:7:::
oscar:$6$FirdJ7e84LEhWt$asiwMIUwGceKEoYsaqgn0sQu4uvM9zFZtj5ew7TpaT.NgX5TTRRHly1QwFogwfsUueBcrsyJr47qr/mCIYub20:18892:0:99999:7:::
Wrote 30 lines
```

Usamos el “unshadow”

```
kali@kali: ~/trabajo_john
File Actions Edit View Help
kali@kali: /media/kali/rootant0X19/etc x kali@kali: ~/trabajo_john x kali@kali: ~/trabajo_john x
(kali@kali)~(~/trabajo_john)
$ unshadow passwd.txt shadow.txt > passwords
(kali@kali)~(~/trabajo_john)
$ ls
passwd.txt passwords shadow.txt
(kali@kali)~(~/trabajo_john)
$ cat passwords
root:$6$MmNTxZgy7aF5$ZHeZLXCcbQg[eUsHXyZb1m5j7jPkSpzdTDHdJMw1xTuBjHT7a9Jb3xEK3TVvq3z75khhIpcVx9x16mfh.4/:18892:0:99999:7:::
daemon:*:18767:0:99999:7:::
bin:*:18767:0:99999:7:::
sys:*:18767:0:99999:7:::
sync:*:18767:0:99999:7:::
games:*:18767:0:99999:7:::
man:*:18767:0:99999:7:::
lp:*:18767:0:99999:7:::
mail:*:18767:0:99999:7:::
news:*:18767:0:99999:7:::
uucp:*:18767:0:99999:7:::
proxy:*:18767:0:99999:7:::
www-data:*:18767:0:99999:7:::
backup:*:18767:0:99999:7:::
list:*:18767:0:99999:7:::
irc:*:18767:0:99999:7:::
gnats:*:18767:0:99999:7:::
nobody:*:18767:0:99999:7:::
_apt:*:18767:0:99999:7:::
messagebus:*:18767:0:99999:7:::
usbmux:*:18767:0:99999:7:::
_ftp:*:18767:0:99999:7:::
statd:*:18767:0:99999:7:::
joan:$6$X8lGwZLDJ13s3J7w5/q07sb0GgLCqfa22aM/TsHMGvYuketjSTuZMAewmMtw0NA9Vz320e.umPeLLg3fcpwGhno0cJ5EY152n/qVX0:18892:0:99999:7:::
maria:$6$5bhpP.rnkv8qQm4q1W51K3jhw3jeh2APKz1NhiwE37upp7KHG.jbaMtd5XMAAhtdzQg5fnaBmhlld31ln1SHdE.ph0y0eFVPR0C/:18892:0:99999:7:::
jordi:$6$z1z5JwW877PSYrB5LH0oLUTnCGrp81HF0HML5n1fmHaHn8joaGmwyv16359j6.NkL2CsyeLvgQtUJfBa2Urze1QHrY71VoOX138.:18892:0:99999:7:::
kiko:$6$11FyhInPFTIHdV/T$5iMt1Jx/y5vX04Y8Q59.ofSTLfp567EdvWYQpvdBMrLwUufm6otZzr1cN9m0vY77Q.dKzALFN/201PzzB3/:18892:0:99999:7:::
albert:$6$Z3Zv6EzUzUpJN6E57usqCZUFmD96E12xEUmGy0THdhJeyVvSU2dMuhzpgNHJfzu5.0WwAG8Tm6m1XCv7a964cf8zx1Sgyxtgv01:18892:0:99999:7:::
felip:$6$uPFb2IDqoW0jZn5f0wcAwG3r.f480IR3rShjnt0QJyaNBZaym3w3J5lnKs3/XJ1LbCLpCXA0eSml7vlt0h0pc77Z4p2LT9bcy.:18892:0:99999:7:::
oscar:$6$FirdJ7e84LEhWt$asiwMIUwGceKEoYsaqgn0sQu4uvM9zFZtj5ew7TpaT.NgX5TTRRHly1QwFogwfsUueBcrsyJr47qr/mCIYub20:18892:0:99999:7:::
```

```
(kali@kali)~(~/trabajo_john)
$ john passwords
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 instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 16 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
```

Y tendríamos la contraseña

```

--(kali@kali)-[~/Downloads/John]
└─$ john --wordlist=/home/kali/trabajo_john/rockyou.txt --rules /home/kali/trabajo_john/passwords
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 instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:03 0.00% (ETA: 2023-10-04 00:20) 0g/s 3221p/s 3221c/s 3221C/s 123
45b..iasshole
0g 0:00:00:05 0.00% (ETA: 2023-10-03 19:24) 0g/s 3500p/s 3500c/s 3500C/s bea
utyqueen..tanika
0g 0:00:00:07 0.00% (ETA: 2023-10-03 18:41) 0g/s 3600p/s 3600c/s 3600C/s joe
yl..carlos7
0g 0:00:00:11 0.01% (ETA: 2023-10-03 18:02) 0g/s 3706p/s 3706c/s 3706C/s los
er69..180993
0g 0:00:00:13 0.01% (ETA: 2023-10-03 17:52) 0g/s 3732p/s 3732c/s 3732C/s cal
tlynn..trudy
0g 0:00:00:14 0.01% (ETA: 2023-10-03 17:30) 0g/s 3742p/s 3742c/s 3742C/s amb
er101..spook
0g 0:00:00:15 0.01% (ETA: 2023-10-03 17:44) 0g/s 3749p/s 3749c/s 3749C/s sim
ple123..jacoble
0g 0:00:00:16 0.01% (ETA: 2023-10-03 17:26) 0g/s 3757p/s 3757c/s 3757C/s for
klift..215215
0g 0:00:00:17 0.01% (ETA: 2023-10-03 17:38) 0g/s 3762p/s 3762c/s 3762C/s jas
on77..bianchi
0g 0:00:00:18 0.01% (ETA: 2023-10-03 17:23) 0g/s 3770p/s 3770c/s 3770C/s mam
icuta..diferente
0g 0:00:00:19 0.01% (ETA: 2023-10-03 17:09) 0g/s 3773p/s 3773c/s 3773C/s 011
392..pootang
0g 0:00:00:21 0.01% (ETA: 2023-10-03 17:07) 0g/s 3785p/s 3785c/s 3785C/s Bry

```

```

--(kali@kali)-[~/trabajo_john]
└─$ john --show passwords
root:buster9:0:0:root:/root:/usr/bin/zsh
1 password hash cracked, 0 left

--(kali@kali)-[~/trabajo_john]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt --rules passwords-

```