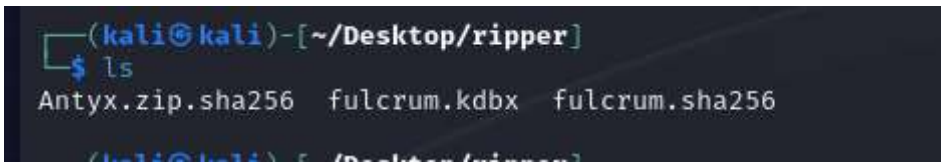
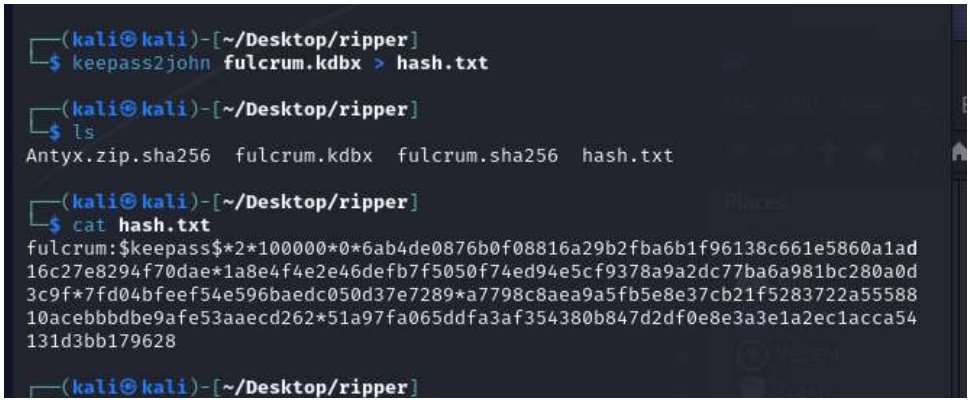
Primer paso: “Cómo obtener password del archivo Keepass”

• Descarga el archivo KeePass "fulcrum.kdbx" de Aules.



Extrae el hash de la contraseña del archivo con las utilidades de John The Ripper que ya vienen instaladas en Kali Linux (https://www.openwall.com/john/) y ponle tu nombre al archivo resultado.



Edita el archivo para ver el contenido y borra el nombre del archivo de delante del texto. Tienes que borrar lo que hay delante de $keepass$ (esto último indica que el hash es del programa Keepass). Si no, no va a funcionar.

Usa el diccionario rockyou.txt. Los diccionarios preinstalados en Kali se encuentran en /usr/share/wordlists y quizás se encuentran comprimidos y antes debas descomprimirlos.

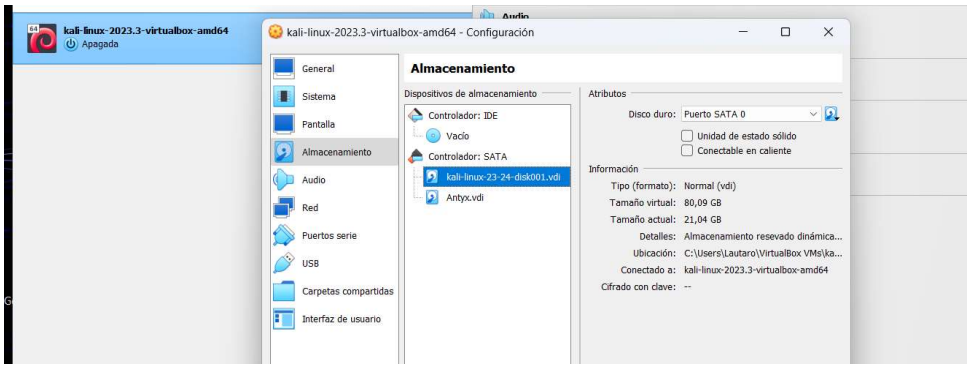
Ahora usamos el comando de john para obtener la contraseña del hash

```
┌──(kali㉿kali)-[~/Desktop/ripper]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt 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 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:01:10 0.04% (ETA: 2023-09-27 09:59) 0g/s 91.00p/s 91.00c/s 91.00C/s f
atty..yamyam
0g 0:00:01:48 0.06% (ETA: 2023-09-27 09:24) 0g/s 90.84p/s 90.84c/s 90.84C/s l
ucky12..jonas1
0g 0:00:03:12 0.09% (ETA: 2023-09-27 15:16) 0g/s 81.84p/s 81.84c/s 81.84C/s c
amels..blair
0g 0:00:03:13 0.09% (ETA: 2023-09-27 15:02) 0g/s 81.89p/s 81.89c/s 81.89C/s h
eriberto..fuckthis1
mindgame         (?)
1g 0:00:17:44 DONE (2023-09-25 04:57) 0.000939g/s 56.34p/s 56.34c/s 56.34C/s
mindgame..midnight3
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Comprueba con el programa Keepass que puedes abrir el archivo cifrado de passwords con el que ha encontrado John.

Segundo paso: “Cómo extraer el almacén de contraseñas del equipo sospechoso”

Tratamos de obtener el archivo de passwords. Añade la imagen del disco sospechosa a la máquina virtual de Kali Linux. Tienes que añadirlo a la controladora SATA en los parámetros de la máquina virtual



• Ahora copiaremos los archivos de passwords (/etc/passwd y /etc/shadow) en un directorio diferente para no dañar el disco original de la víctima (por ejemplo en /home/kali/trabajo). Es necesario trabajar en un directorio temporal fuera del disco de la víctima.

• Convierte el archivo shadow en un archivo estándar de contraseñas con el comando unshadow.

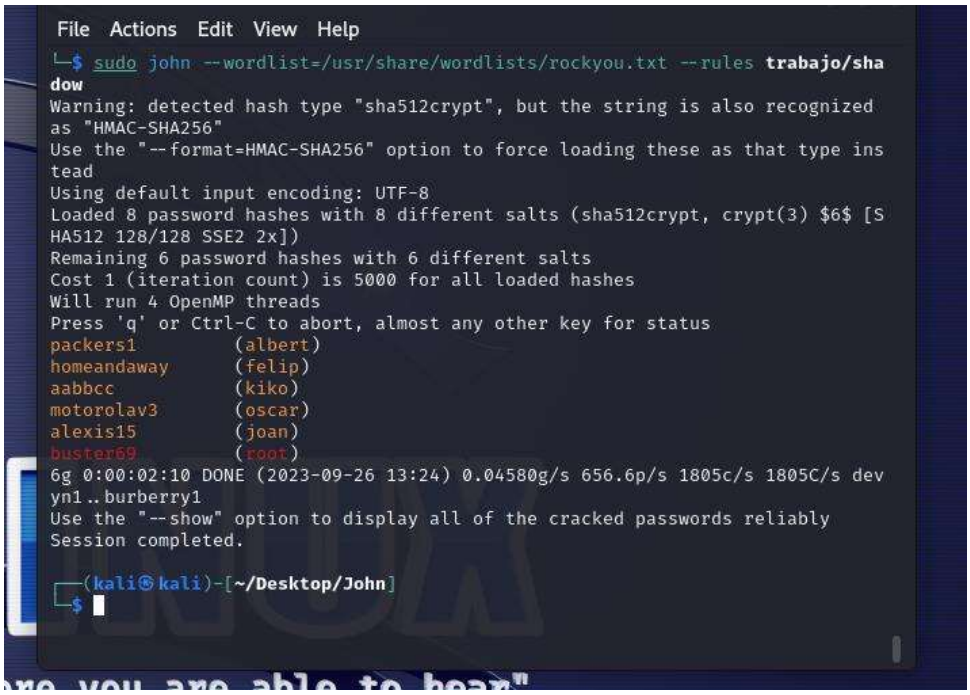
```
┌──(kali㉿kali)-[~/Desktop/John/trabajo]
└─$ sudo unshadow /etc/passwd /etc/shadow > combinadas.txt

[sudo] password for kali:

┌──(kali㉿kali)-[~/Desktop/John/trabajo]
└─$ ls
combinadas.txt  passwd  shadow

┌──(kali㉿kali)-[~/Desktop/John/trabajo]
└─$ cat combinadas.txt
root:*:0:0:root:/root:/usr/bin/zsh
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
```

Ejecuta John the Ripper con el archivo obtenido. En una primera aproximación que tarda poco tiempo, hacemos "John" en modo Single. Se aplican reglas básicas como poner el nombre de usuario y datos personales que aparecen en el archivo de passwords como si fueran el password.

```
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 128/128 SSE2 2x])
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
maria            (maria)
jordi123         (jordi)
Almost done: Processing the remaining buffered candidate passwords, if any.
2g 0:00:00:09 DONE (2023-09-26 13:06) 0.2024g/s 1832p/s 1835c/s 1835C/s felip
999991900..999991900
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Crack de passwords con reglas

Ahora ejecutamos a John con una lista mucho más completa (más lento). Atacaremos con la wordlist "rockyou.txt":



4. Al final de la tarea debemos haber obtenido TODAS las contraseñas. Escribe en una tabla los nombres de los usuarios seguidos de su contraseña

Deberia ser del archivo combinadas pero como me confundi en el proceso el unshadow fue solo a shadow y tuve que seguir ejecutando el proceso sobre shadow.