



Laboratorio 3.2

Archivos de Office
con Contraseña

Ing. Alex Araya Rojas, MT
CISSP, CISM

Febrero 2022

Lab 3.2

Archivos de Office con Contraseña

01 Descargar el instalador

02 Procedimiento

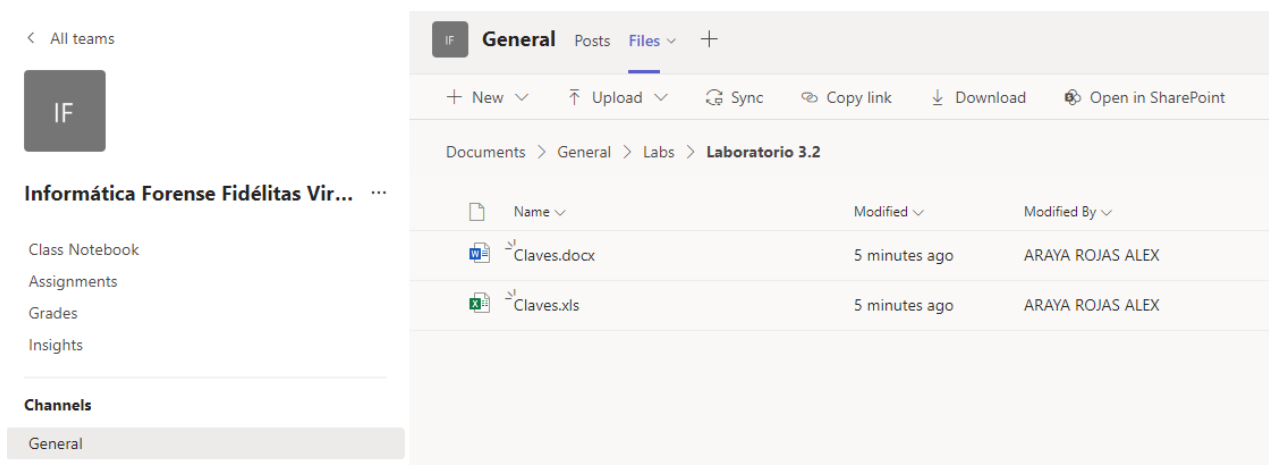
Procedimiento

Descargar el instalador

01. Es recomendable que realice estas pruebas en un equipo virtual para no comprometer la seguridad de su equipo de cómputo.
02. Descargue la última versión de Kali Linux, al momento de la liberación de este laboratorio es la 2021.4a. Este archivo es un archivo que pesa aprox. 2,5 GB (<https://kali.download/virtual-images/kali-2021.4a/kali-linux-2021.4a-vmware-amd64.7z>)
03. Si ya cuenta con el laboratorio 3.1 realizado, puede utilizar ese Kali Linux.
04. Si no cuenta con el software para instalar máquinas virtuales, puede descargar VMware Player en la carpeta de herramientas del Teams del curso Forense.

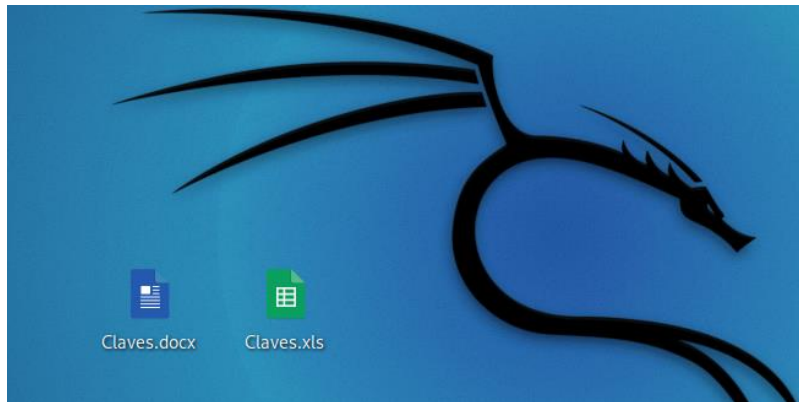
Procedimiento

01. Una vez que cuente con la máquina virtual de Kali corriendo, deberá copiar 2 archivos que se ubican en la carpeta del curso en el escritorio del Kali Linux. Los archivos se llaman Claves.docx y Claves.xls. Puede descargar estos archivos a su equipo host y desde ahí arrastrarlos al escritorio del Kali.



The screenshot displays a Microsoft Teams interface. On the left, a sidebar shows the team name 'IF' and the channel 'Informática Forense Fidélitas Vir...'. The main area shows the 'Files' tab for the 'Laboratorio 3.2' channel. A table lists the files in the channel:

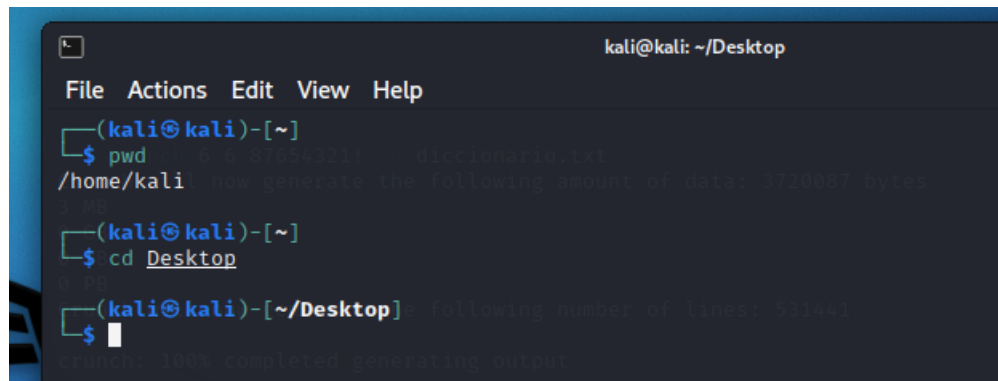
Name	Modified	Modified By
Claves.docx	5 minutes ago	ARAYA ROJAS ALEX
Claves.xls	5 minutes ago	ARAYA ROJAS ALEX



02. Abra una consola de terminal en el Kali Linux.



03. Al abrir la reciente terminal, el directorio de trabajo es /home/Kali, para facilitar el proceso, vamos a definir el escritorio como nuestro directorio de trabajo. El comando pwd les permite visualizar el directorio de trabajo, el comando cd es para cambiar de directorio.



04. Los archivos de Claves que copió en el escritorio del Kali Linux poseen la información de las contraseñas de la persona que estamos investigando. Puede utilizar el comando ls para visualizar los archivos en el escritorio.

```
(kali㉿kali)-[~/Desktop] following number of lines: 531441
$ ls
Claves.docx
Claves.xls
diccionario.txt
```

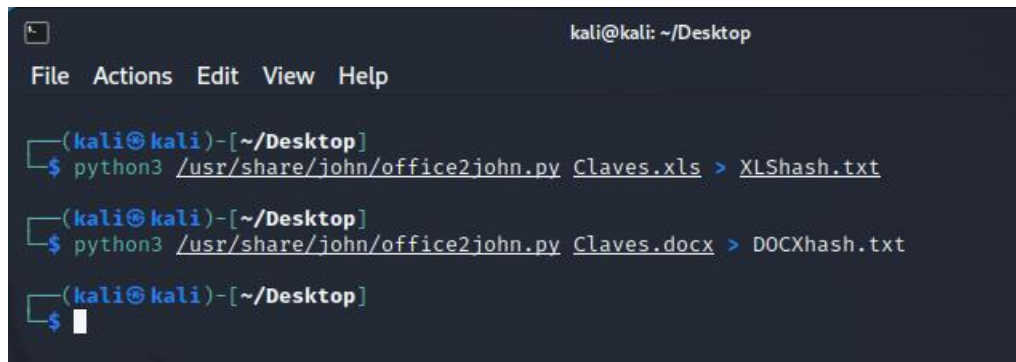
05. La persona investigada, en un esfuerzo de esconder sus actividades, definió una contraseña para estos archivos, de forma que no podemos abrirlos sin contar con dicha contraseña, y es nuestro trabajo “adivinarla” para poder determinar si la información de los archivos es útil para el caso que estamos investigando.
06. Lo primero que vamos a hacer, es retomar el laboratorio 3.1 y generar un archivo de contraseñas para nuestro diccionario, con claves de 6 dígitos de longitud y solo con números y el símbolo “!”
07. Con Crunch, vamos a utilizar la siguiente línea: Crunch 6 6 87654321! -o diccionario.txt, tendremos casi 4 millones de posibles contraseñas para probar.

```
(kali㉿kali)-[~/Desktop]
$ crunch 6 6 87654321! -o diccionario.txt
Crunch will now generate the following amount of data: 3720087 bytes
3 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 531441

crunch: 100% completed generating output

(kali㉿kali)-[~/Desktop]
$
```

08. Ahora es necesario extraer los hash de las contraseñas de ambos archivos, ya que con ese hash es que vamos a trabajar posteriormente. Existe una utilidad que nos permite hacer eso, copie los siguientes comandos y genere los hash en los archivos XLSHash y DOCXhash, siempre en el escritorio del Kali Linux.



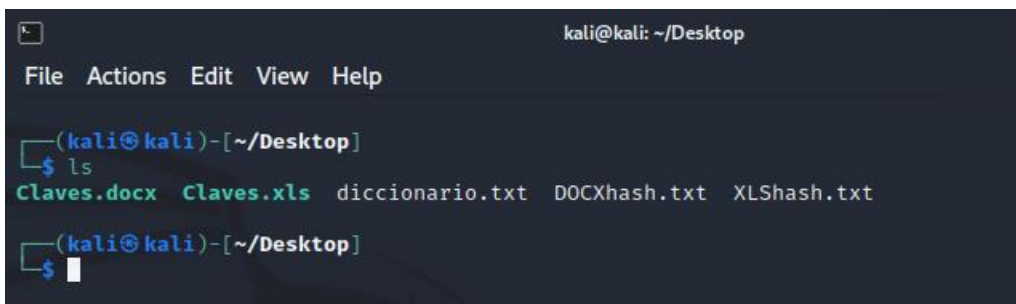
```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ python3 /usr/share/john/office2john.py Claves.xls > XLShash.txt

(kali@kali)-[~/Desktop]
$ python3 /usr/share/john/office2john.py Claves.docx > DOCXhash.txt

(kali@kali)-[~/Desktop]
$
```

09. En este punto del laboratorio, deberá tener 5 archivos en su escritorio, tal y como se muestra en la siguiente imagen.

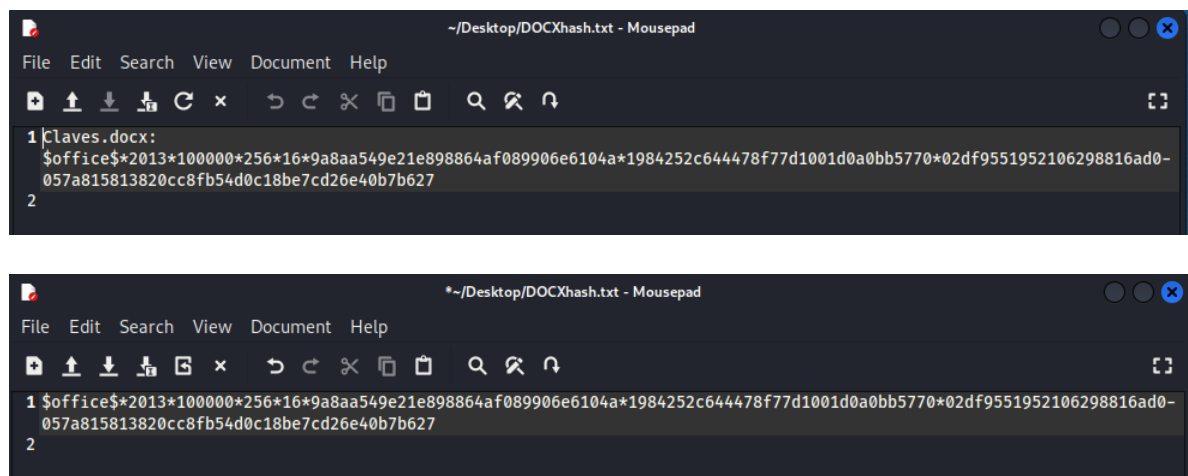


```
kali@kali: ~/Desktop
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ ls
Claves.docx Claves.xls diccionario.txt DOCXhash.txt XLShash.txt

(kali@kali)-[~/Desktop]
$
```

10. Elimine la primera línea de los archivos hash, para que queden en el formato adecuado para la siguiente herramienta, se muestra a continuación el cambio que debe realizarse en el archivo de Word



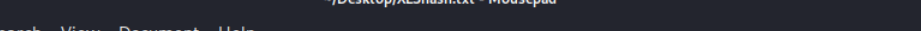
The first screenshot shows the initial content of the file `DOCXhash.txt` in Mousepad:

```
1 Claves.docx:
  $office$*2013*100000*256*16*9a8aa549e21e898864af089906e6104a*1984252c644478f77d1001d0a0bb5770*02df9551952106298816ad0-
  057a815813820cc8fb54d0c18be7cd26e40b7b627
2
```

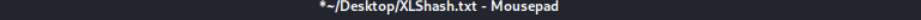
The second screenshot shows the file after the first line has been removed, leaving only the hash value:

```
1 $office$*2013*100000*256*16*9a8aa549e21e898864af089906e6104a*1984252c644478f77d1001d0a0bb5770*02df9551952106298816ad0-
  057a815813820cc8fb54d0c18be7cd26e40b7b627
2
```

11. Ahora modifique el archivo hash del Excel.



The screenshot shows a Windows File Explorer window. The address bar displays the path `~\Desktop\XLShash.txt - Mousepad`. The menu bar includes `File`, `Edit`, `Search`, `View`, `Document`, and `Help`. The toolbar contains icons for file operations. The main pane shows a folder named `1` which contains a file named `claves.xls`. The file's details are shown below the file name: `Soldoffice$4*f90ecc3ff4168a2310b86e119c8b8666*f4c780927d729bb3576358d69b050fbc*06552ff24d19c8228fc1460475ee9970081245-a1`.



The screenshot shows a terminal window with a dark background. The title bar at the top reads "*/~/Desktop/XLSHash.txt - Mousepad". The menu bar includes "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with icons for file operations. The terminal content shows a file path on line 1: `1 |boldoffice$4*f90ecc3ff4168a2310b86e119cb8b666*f4c780927d729bb3576358d69b050fbc*06552ff24d19c8228fc1460475ee9970081245-` and a command on line 2: `2 a1`.

12. En la herramienta hashcat, debemos especificar el tipo de hash que estamos procesando, esta herramienta tratará de realizar un descubrimiento automático, pero no siempre será efectivo. Para el archivo de Word, al tratarse de un archivo DOCX, estableceremos el comando de la siguiente forma:

```
(kali㉿kali)-[~/Desktop]
$ hashcat -m 9600 -o /home/kali/Desktop/DOCXcracked.txt DOCXhash.txt diccionario.txt
```

13. Ahora solo debemos esperar hasta que el proceso finalice, el password del archivo estará al final del hash en el archivo DOCXcracked.txt

[illegible]

14. Ahora toca el turno del archivo Excel, el comando es muy similar:

```
(kali㉿kali)-[~/Desktop]
$ hashcat -m 9800 -o XLScrapped.txt XLShash.txt diccionario.txt
```

15. Realice sus propias pruebas con archivos en los cuales ud asigne la contraseña.
16. Recuerde que el esfuerzo del equipo para dar con la contraseña dependerá del archivo diccionario y su exactitud, si ud agregar caracteres adicionales fácilmente este esfuerzo puede requerir días o semanas de procesamiento.