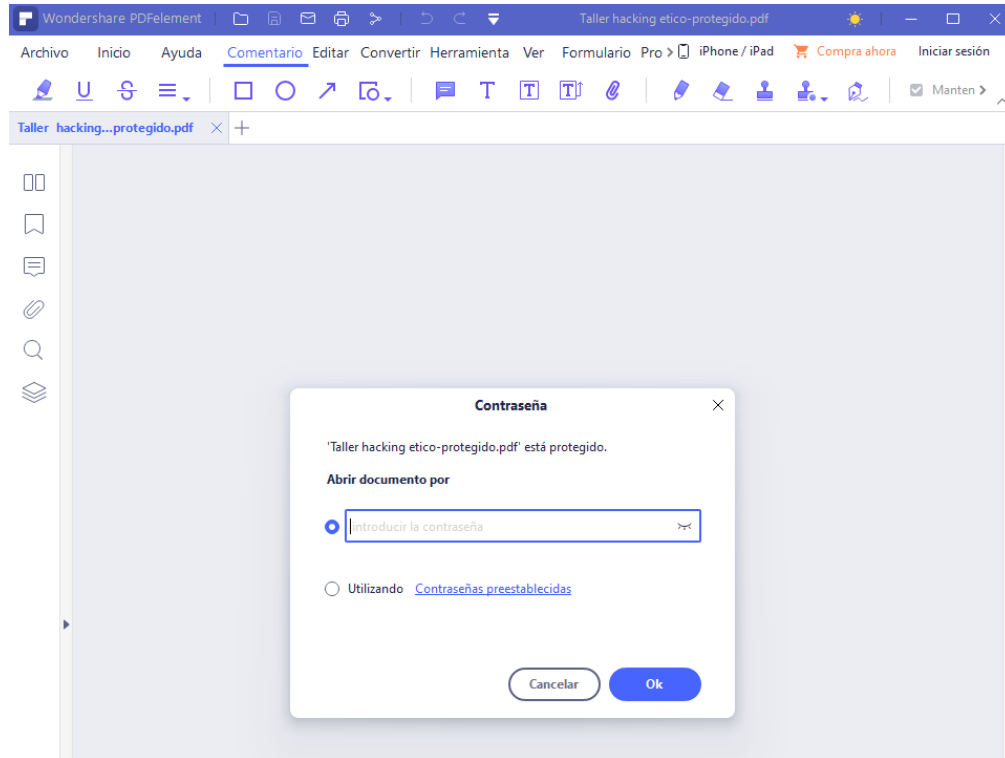


TALLER 1: Hacking Ético

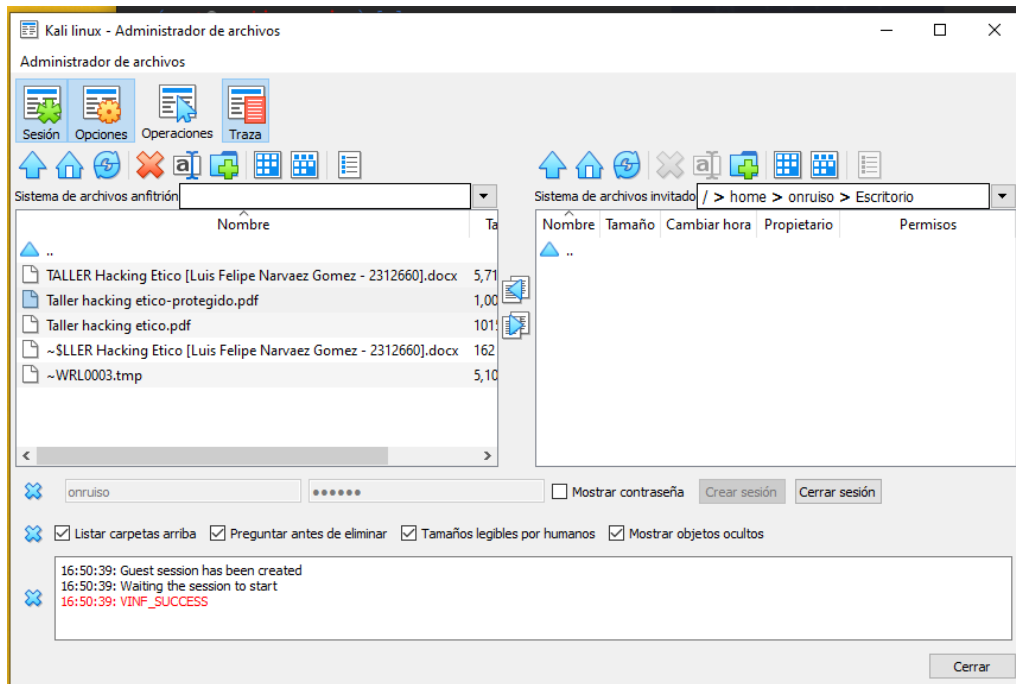
Luis Felipe Narváez Gómez. E-mail: luis.narvaez@usantoto.edu.co. Cod: 2312660. Facultad de Ingeniería de Sistemas.

ABRIR UN PDF A FUERZA BRUTA

Lo que primero debemos tener para esta practica es un archivo en formato PDF que este protegido frente a lectura y escritura mediante el uso de contraseña, un ejemplo seria el que se muestra en la imagen.

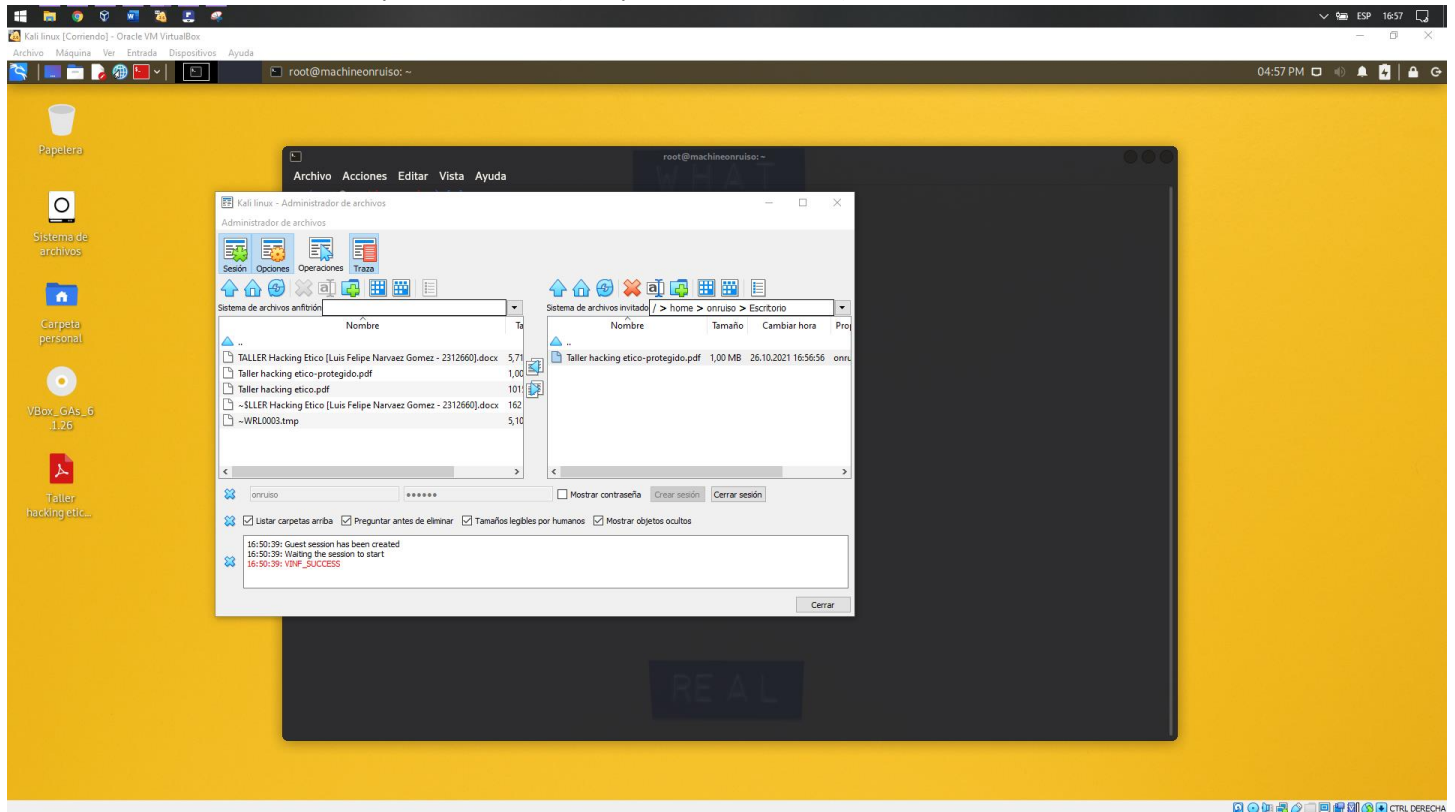


Este archivo se encuentra en la Maquina Anfitrión Windows 10 y debemos pasarlo a nuestra maquina virtual Kali Linux, para eso haremos uso del Administrador de Archivos de Virtual Box con su utilidad de Guest Additions.

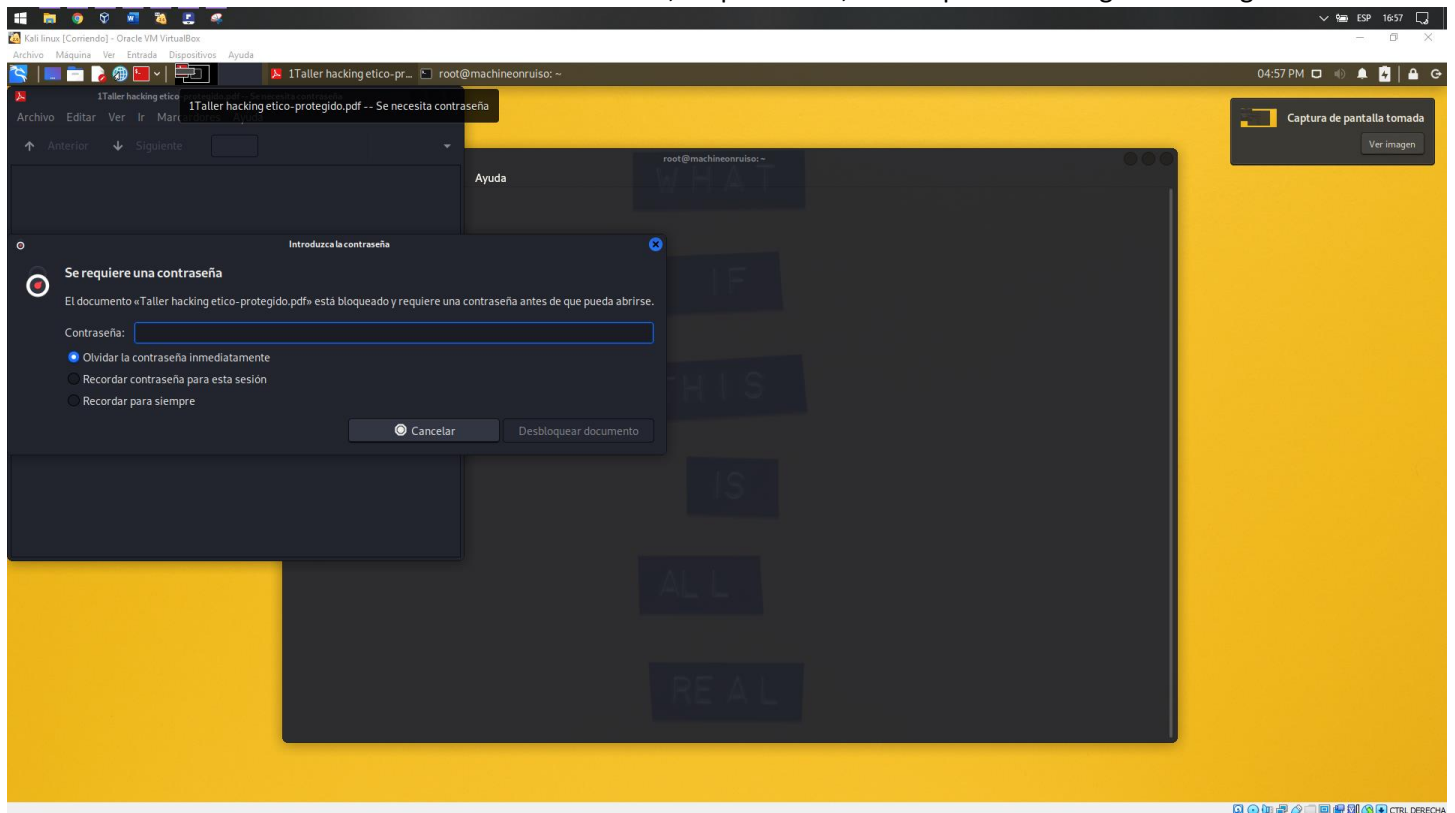


Para que funcione nuestra transacción entre maquinas debemos tener en cuenta que hay que crear la sección en el Administrador de archivos de nuestra maquina virtualizada. Para ello ingresaremos las credenciales normales de ingreso

en la parte inferior de la ventana, seguido de esto ubicaremos en ambos espacios tanto el archivo que queremos pasar como la ruta a donde que queremos pasarlo. Para pasarlo solo debemos seleccionar el archivo de origen e indicar con las flechas centrales el sentido en que se moverá (lo copiará en el destino) a su nuevo destino.



Si intentamos abrirlo sin la contraseña aun en Kali Linux, no podremos, como aparece en la siguiente imagen.



Ahora bien, hay varios métodos para poder obtener las credenciales o abrir sin ellas un PDF protegido por contraseña, la herramienta que utilizaremos es PDFCRACK, la cual, mediante el uso de fuerza bruta, probar una lista de caracteres u contraseñas cíclicamente hasta abrir el documento, lograr abrir el archivo que queremos.

Lo primero será instalar la herramienta PDFCRACK con el comando “sudo apt-cache search pdfcrack” seguido del comando “sudo apt-get install pdfcrack”.

```
(root@machineonruiso)-[~]
# sudo apt-cache search pdfcrack
forensics-extra - Forensics Environment - extra console components (metapackage)
pdfcrack - PDF files password cracker

(root@machineonruiso)-[~]
# sudo apt-get install pdfcrack
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  libdap27 libdapclient6v5 libdav1d4 libepsilon1 libgdal28 libgupnp-1.2-0 libidn11 libnetcdf18 libntfs-3g883 libomp-11-dev libomp5-11 liborc6
  libx265-192 libyara4 python3-editor python3-ipynb python3-genutils python3-pylnk
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes NUEVOS:
  pdfcrack
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 36,0 kB de archivos.
Se utilizarán 93,2 kB de espacio de disco adicional después de esta operación.
Des:1 http://kali.download/kali kali-rolling/main amd64 pdfcrack amd64 0.19-2 [36,0 kB]
Descargados 36,0 kB en 2s (21,4 kB/s)
Seleccionando el paquete pdfcrack previamente no seleccionado.
(Leyendo la base de datos ... 276556 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../pdfcrack_0.19-2_amd64.deb ...
Desempaquetando pdfcrack (0.19-2) ...
Configurando pdfcrack (0.19-2) ...
Procesando disparadores para man-db (2.9.4-2) ...
Procesando disparadores para kali-menu (2021.4.1) ...

(root@machineonruiso)-[~]
#
```

Ahora podemos hacer uso de la herramienta, hay varias formas de hacerlo, incluso poder acelerar la búsqueda, orientarla a trabajar con solo con números, limitar el numero de caracteres a probar, trabajar con un diccionario de claves, etc.

- Algunos ejemplos serian:
- Con diccionario de claves: “pdfcrack -f "Old is g0ld.pdf" -w /usr/share/wordlists/rockyou.txt”
- Aceleracion dando opciones de caracteres que puede llegar a tener: “pdfcrack -f file.pdf -c abcdef123”
- Especificar que trabaje con números y con un limite de 11 digitos: “sudo pdfcrack -f Extracto_Protección_S.A._202003_518113930.pdf -c 1234567890 -n 11”

```

(root@machineonruiso)-[/home/onruiso/Escritorio]
pdfcrack -f Taller\ hacking\ etico-prottegido.pdf -c abcdefghijklmñopqrstuvwxyz1234567890
PDF version 1.6
Security Handler: Standard
V: 2
R: 3
P: -4
Length: 128
Encrypted Metadata: True
FileID: 2d29941b2042232da05bd2609eda61bf
U: 8e38aab93dfb96daf1b1cd7bda3d4d5028bf4e5e4e758a4164004e56fffa0108
O: e386b59a977eb504bef944276d6041a59f5b9590bc9a0df9da4f4a398f1f6612
Average Speed: 46990.4 w/s. Current Word: '33do'
Average Speed: 43035.5 w/s. Current Word: 'c624'
Average Speed: 46755.5 w/s. Current Word: 'ip4ka'
Average Speed: 46399.4 w/s. Current Word: '9d1za'
Average Speed: 46263.1 w/s. Current Word: '9sugb'
Average Speed: 46500.4 w/s. Current Word: '57svb'
Average Speed: 46596.4 w/s. Current Word: 'llscc'
Average Speed: 46191.7 w/s. Current Word: 'ycrc'
Average Speed: 46511.2 w/s. Current Word: 'kkm9c'
Average Speed: 46550.2 w/s. Current Word: 'alld'
Average Speed: 45917.5 w/s. Current Word: 'r0a5d'
Average Speed: 45561.2 w/s. Current Word: 'cbwke'
Average Speed: 46166.6 w/s. Current Word: 'kppze'
Average Speed: 46382.8 w/s. Current Word: 'j6ngf'
Average Speed: 46256.0 w/s. Current Word: 'rsivf'
Average Speed: 46015.7 w/s. Current Word: 'k60bg'
Average Speed: 45452.0 w/s. Current Word: 'ntqg'
Average Speed: 44548.4 w/s. Current Word: '737g'
Average Speed: 43921.8 w/s. Current Word: 'x13mh'
Average Speed: 44745.3 w/s. Current Word: '5qe2h'
Average Speed: 44464.8 w/s. Current Word: 'nmhi'
Average Speed: 44646.6 w/s. Current Word: 'uzuvi'
Average Speed: 45215.9 w/s. Current Word: 'o0ccj'
Average Speed: 45753.8 w/s. Current Word: 'y1qj'
Average Speed: 45148.2 w/s. Current Word: 'vai8j'
Average Speed: 44960.4 w/s. Current Word: '0zunk'
Average Speed: 44674.2 w/s. Current Word: 'yq62k'
Average Speed: 44629.8 w/s. Current Word: 'dwfil'
Average Speed: 45333.7 w/s. Current Word: '8rxwl'
Average Speed: 44681.5 w/s. Current Word: 'r9cm'
Average Speed: 45094.9 w/s. Current Word: 'y9orm'
Average Speed: 45235.2 w/s. Current Word: 'yq68m'
Average Speed: 45490.2 w/s. Current Word: '6spn'
Average Speed: 45369.5 w/s. Current Word: 't803n'
Average Speed: 44451.4 w/s. Current Word: 'cvhj'
Average Speed: 44774.9 w/s. Current Word: '31rx'
Average Speed: 45223.0 w/s. Current Word: 'eae'
Average Speed: 45067.9 w/s. Current Word: 'nmos'
Average Speed: 45811.4 w/s. Current Word: 'w4e0'
Average Speed: 45121.2 w/s. Current Word: 'w2to'
found user-password: '578so'

```

Listo, hemos averiguado la contraseña, ahora a utilizarla y ver lo que contiene el archivo.

