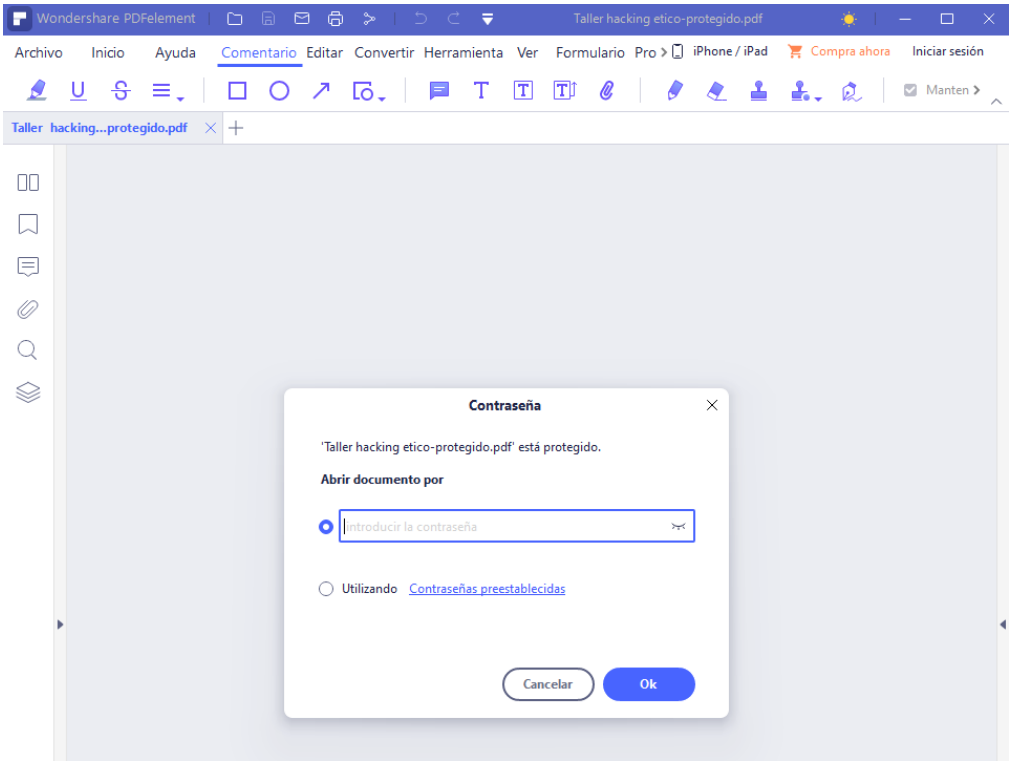
TALLER 1: Hacking Ético

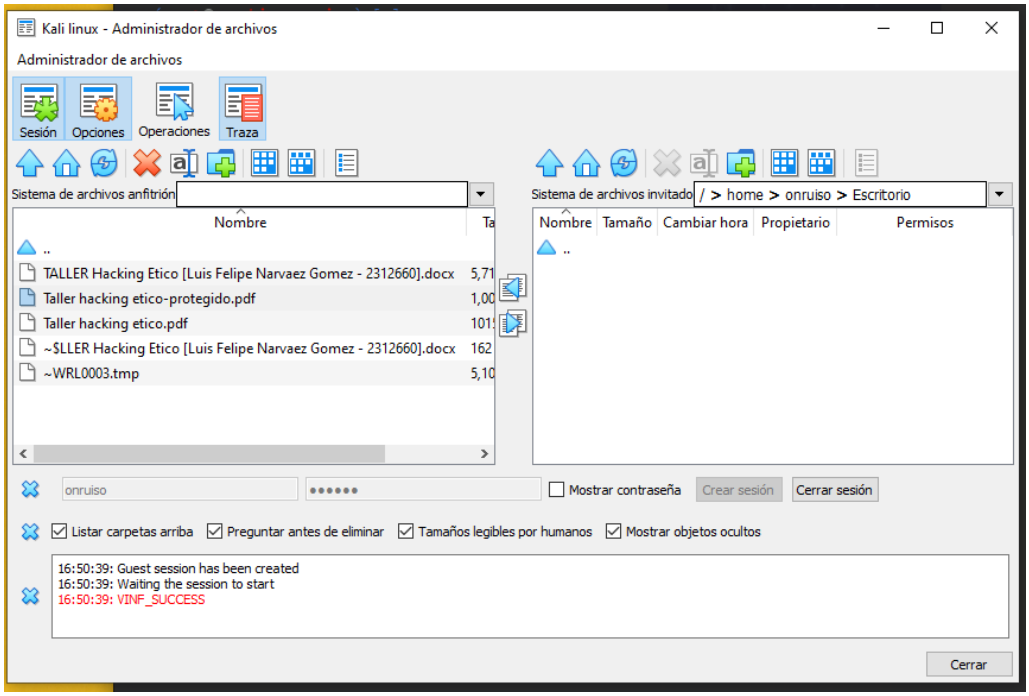
Luis Felipe Narváez Gómez. E-mail: luis.narvaez@usantoto.edu.co. Cod: 2312660. Facultad de Ingeniería de Sistemas.

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 suso de contraseña, un ejemplo seria el que se muestra en la imagen.

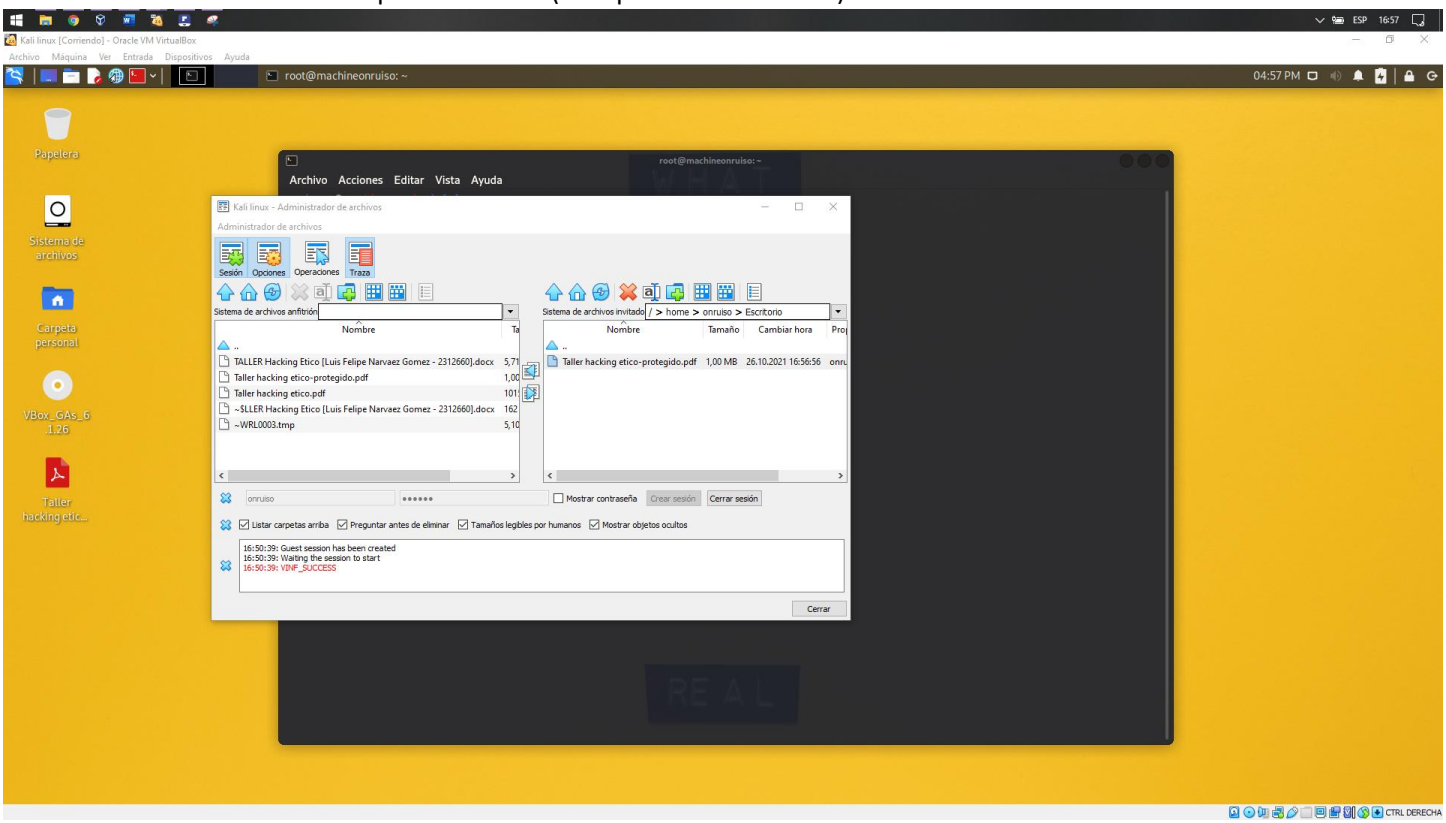


Este archivo se encuentra en la Maquina Anfitrion Windows 10 y debemos pasarlo a nuestra maquina virtual Kali Linux, para eso haremos uso del Administrador de Archivos de Virtual Box con su utilidad de Guest Additions.

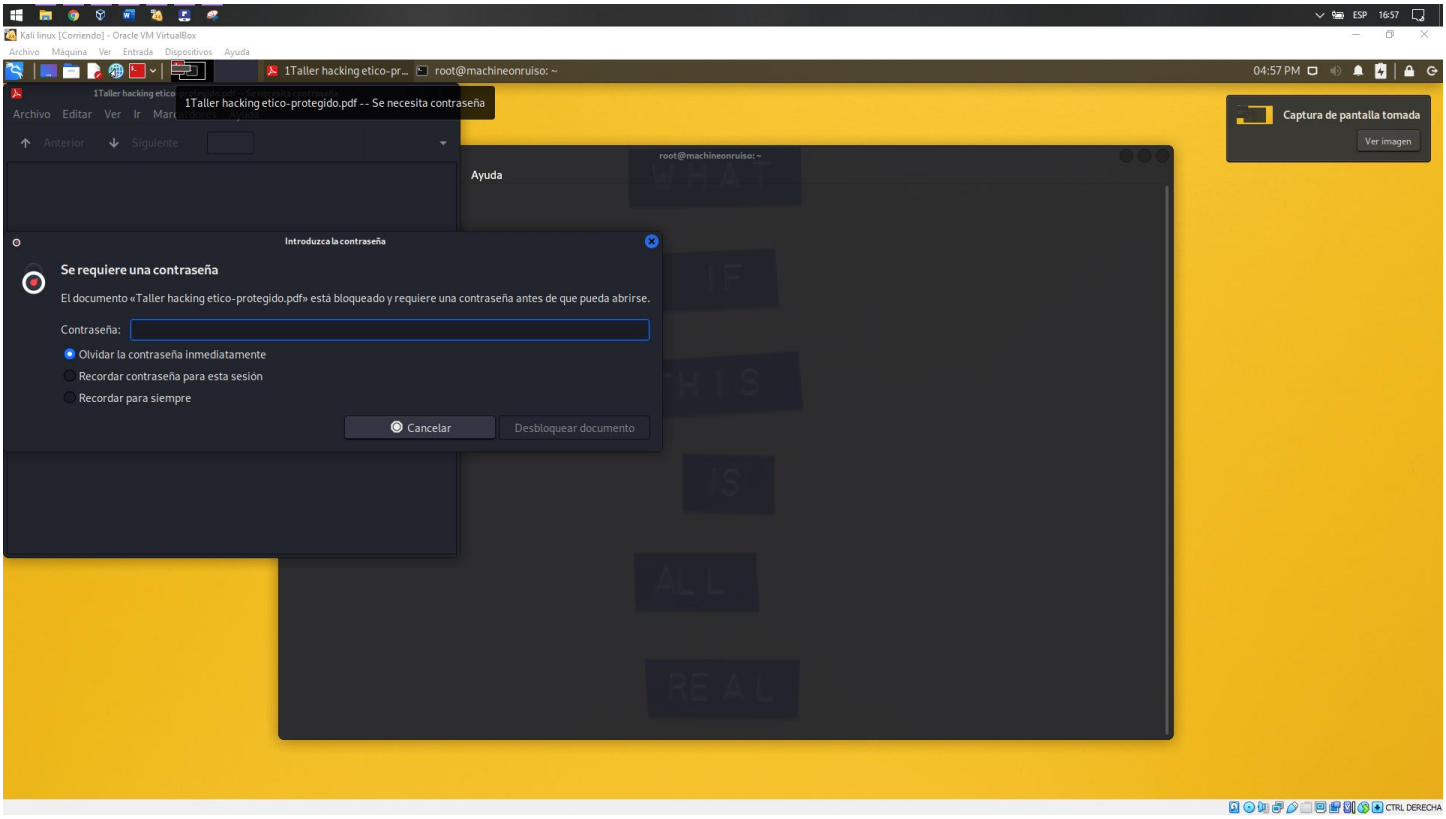


Para que funcione nuestra transacción entre maquinas debemos tener en cuenta que hay que crear la sección en el Administrador de archivos de nuestra maquina virtualizada. Para ello ingresaremos las credenciales normales de ingreso

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.

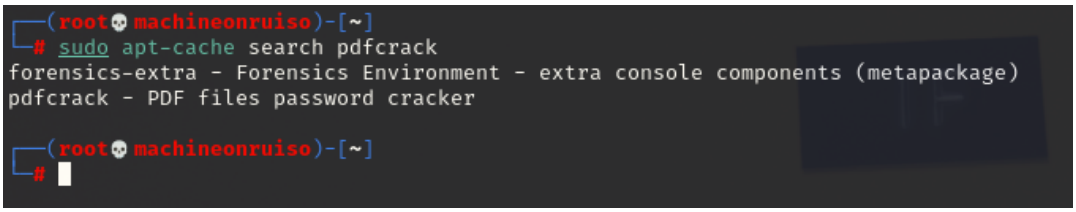


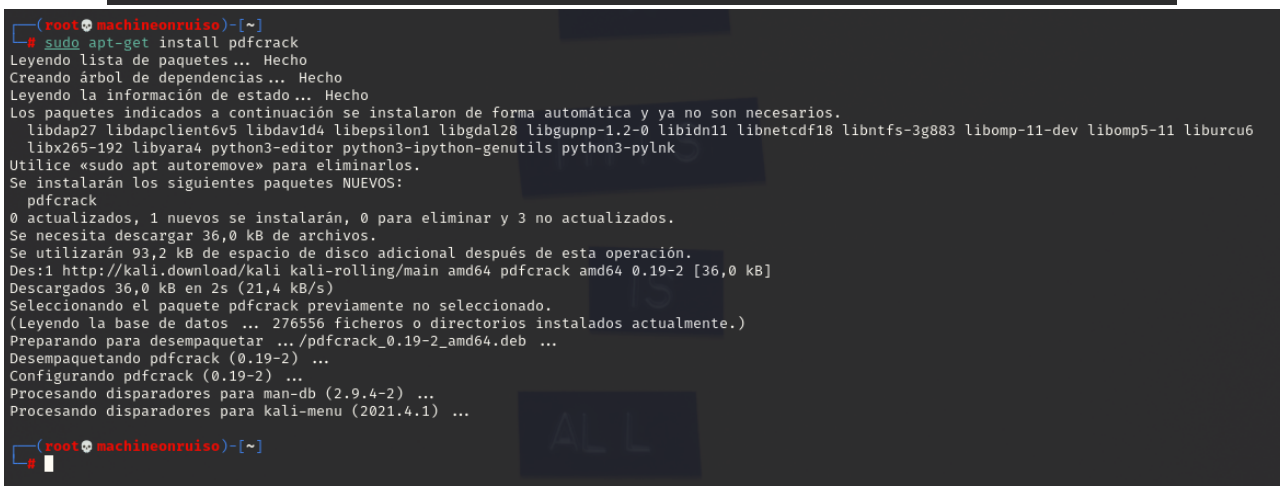
Si intentamos abrirlo sin la contraseña aun en Kali Linux, no podremos, como aprece en la siguiente imagen.



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.

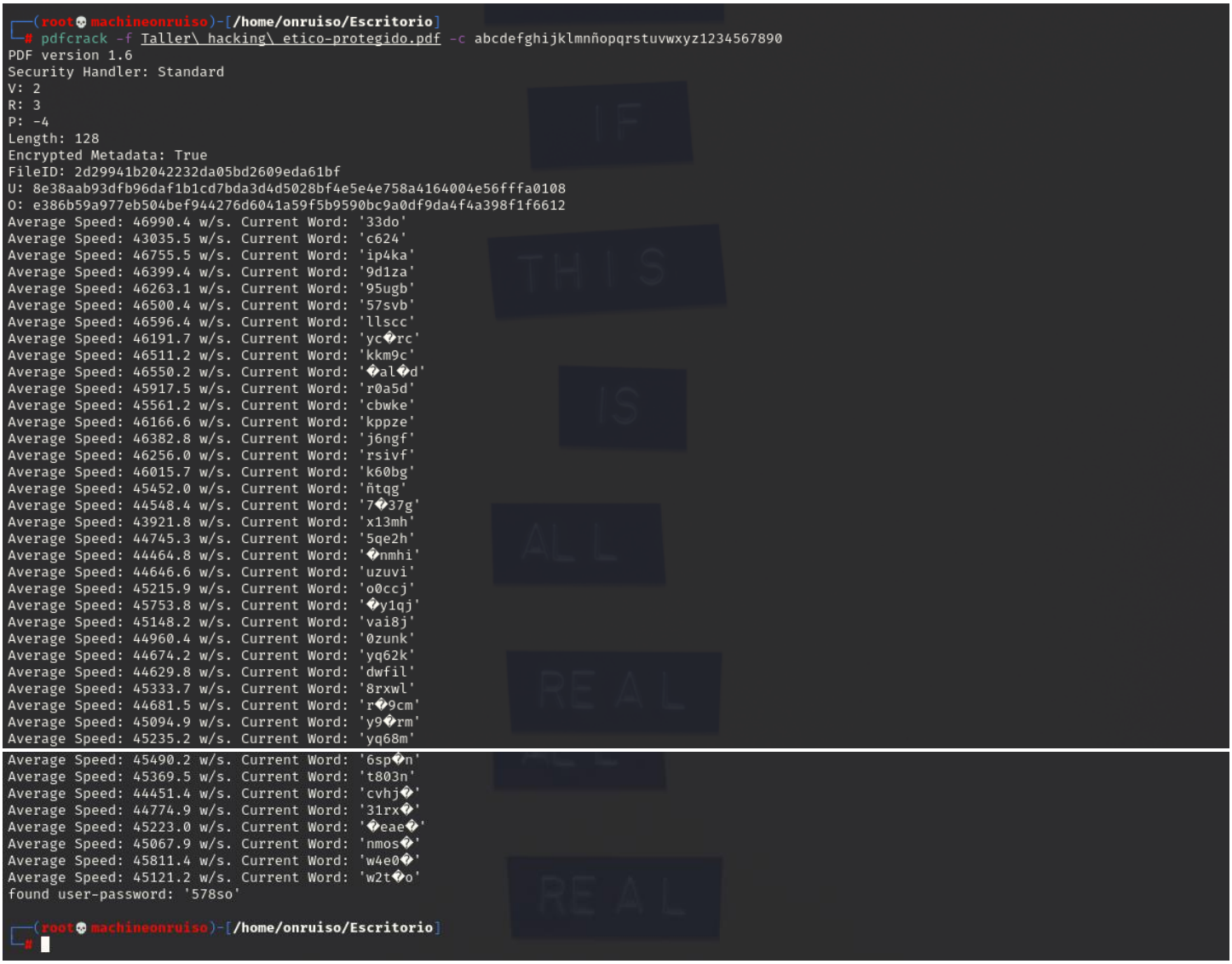
Lo primero será instalar la herramienta PDFCRACK con el comando “sudo apt-cache search pdfcrack” seguido del comando “sudo apt-get install pdfcrack”.



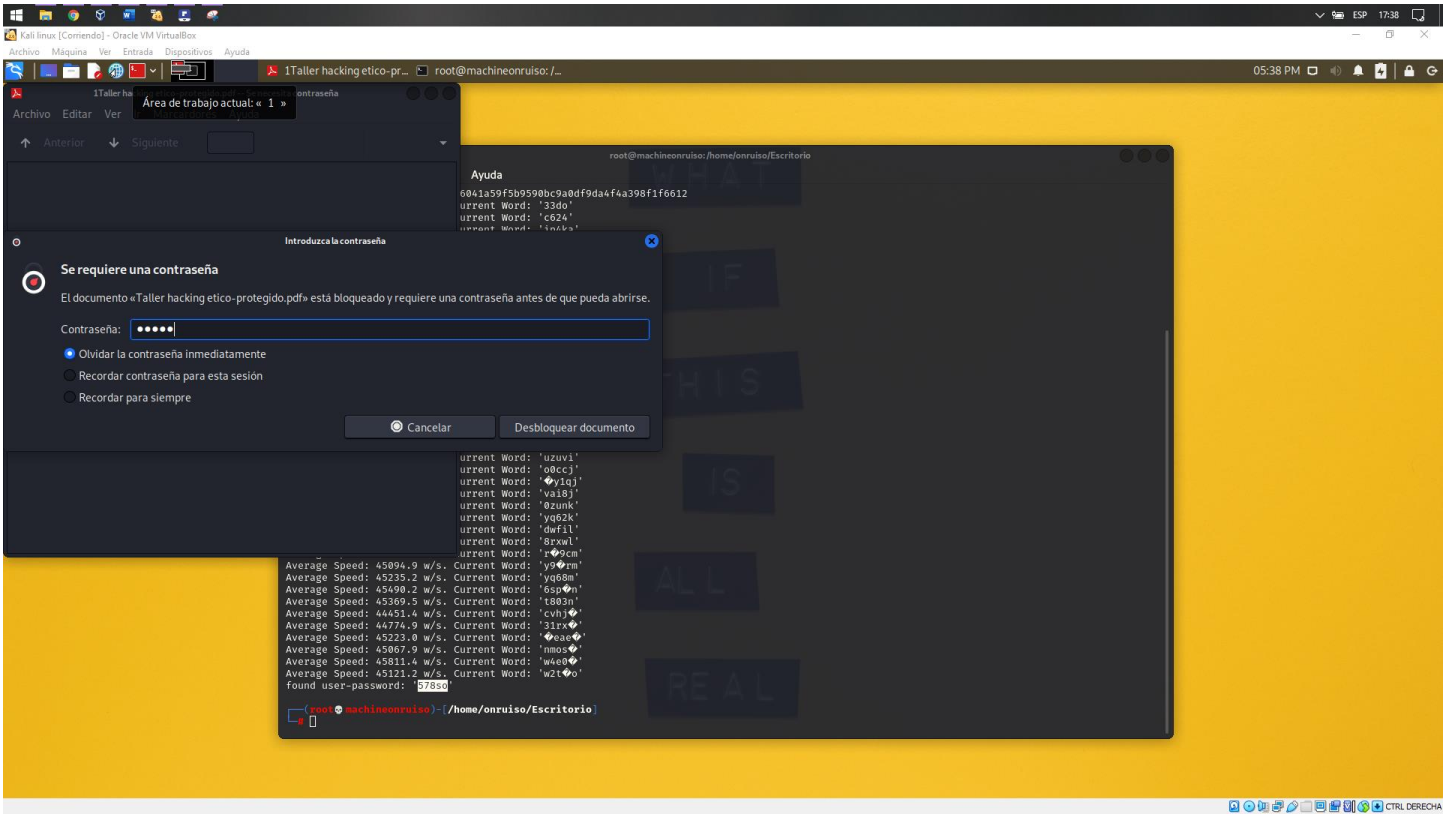


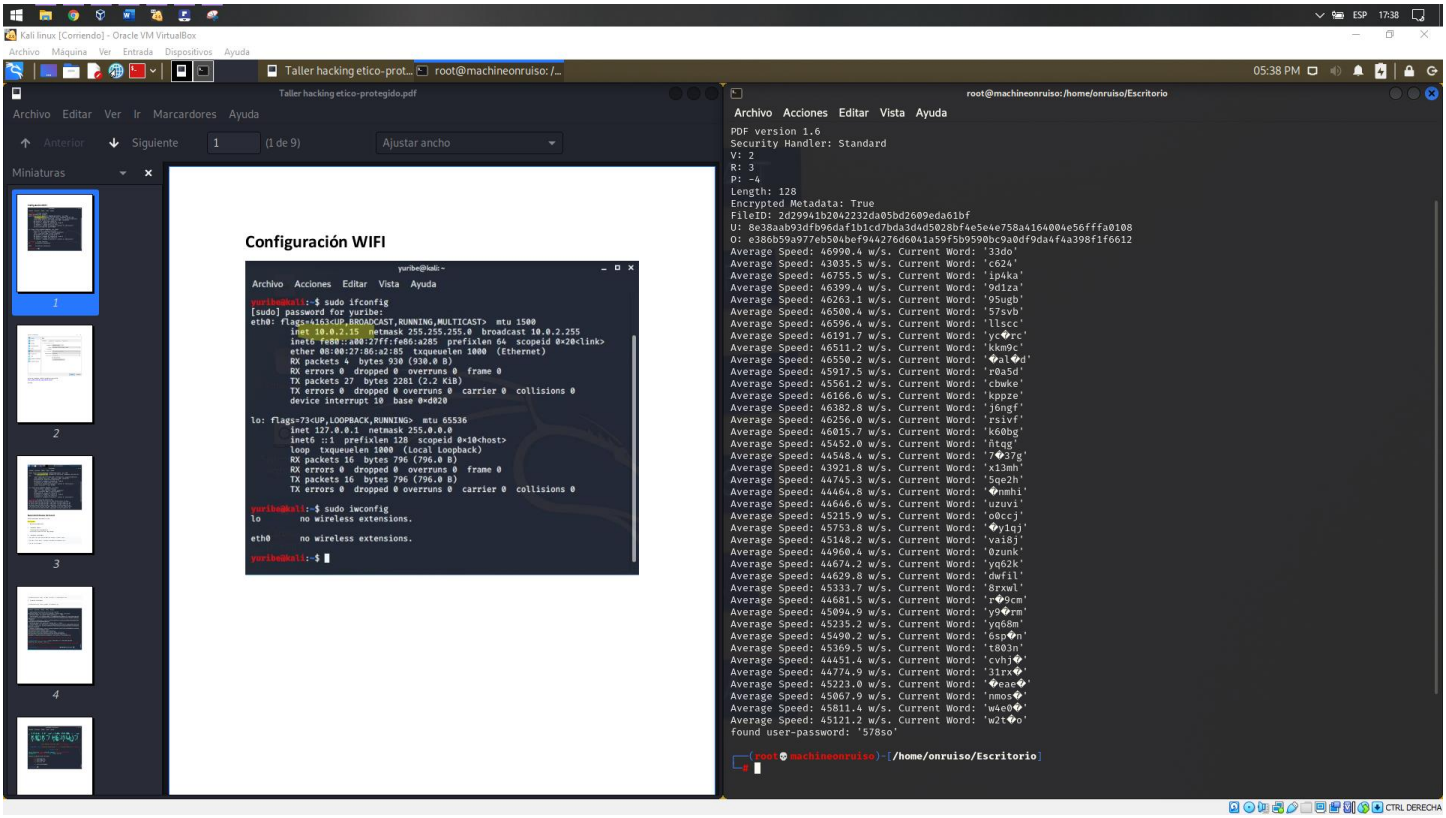
Ahora podemos hacer uso de la herramienta, hay varias formas de hacerlo, incluso poder acelerar la búsqueda, orientarla a trabajar con solo con números, limitar el numero de caracteres a probar, trabajar con un diccionario de claves, etc.

- Algunos ejemplos serian:
- Con diccionario de claves: “pdfcrack -f "0ld 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”



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


Área de trabajo actual: « 1 »
Introduzca la contraseña
Se requiere una contraseña
El documento «Taller hacking etico-protegido.pdf» está bloqueado y requiere una contraseña antes de que pueda abrirse.
Contraseña:
Olvidar la contraseña inmediatamente
Recordar contraseña para esta sesión
Recordar para siempre
Cancelar
Desbloquear documento
root@machineonruiso:/home/onruiso/Escritorio
Ayuda
found user-password: '578so'
(root machineonruiso)-[/home/onruiso/Escritorio]


Taller hacking etico-protegido.pdf
Configuración WIFI
root@machineonruiso:/home/onruiso/Escritorio
found user-password: '578so'
(root machineonruiso)-[/home/onruiso/Escritorio]