**Mesa Calderón Oscar David**

Table of Contents

[ENUCIADO DEL PRIMER PUNTO 2](#_Toc5716137)

[SOLUCION DEL PRIMER PUNTO 2](#_Toc5716138)

[Paso 1 2](#_Toc5716139)

[Paso 2 2](#_Toc5716140)

[Paso 3 2](#_Toc5716141)

[Paso 4 3](#_Toc5716142)

[Paso 5 3](#_Toc5716143)

[Paso 6 4](#_Toc5716144)

[Paso 7 4](#_Toc5716145)

[Paso 8 5](#_Toc5716146)

[Paso 9 5](#_Toc5716147)

[Paso 10 6](#_Toc5716148)

[ENUCIADO DEL SEGUNDO PUNTO 6](#_Toc5716149)

[SOLUCION DEL SEGUNDO PUNTO 6](#_Toc5716150)

[ENUCIADO DEL TERCER PUNTO 6](#_Toc5716151)

[SOLUCION DEL TERCER PUNTO 7](#_Toc5716152)

[ENUCIADO DEL CUARTO PUNTO 8](#_Toc5716153)

[SOLUCION DEL CUARTO PUNTO 8](#_Toc5716154)

[ENUCIADO DEL QUINTO PUNTO 8](#_Toc5716155)

[SOLUCION DEL QUINTO PUNTO 8](#_Toc5716156)

[Bibliografía 9](#_Toc5716157)

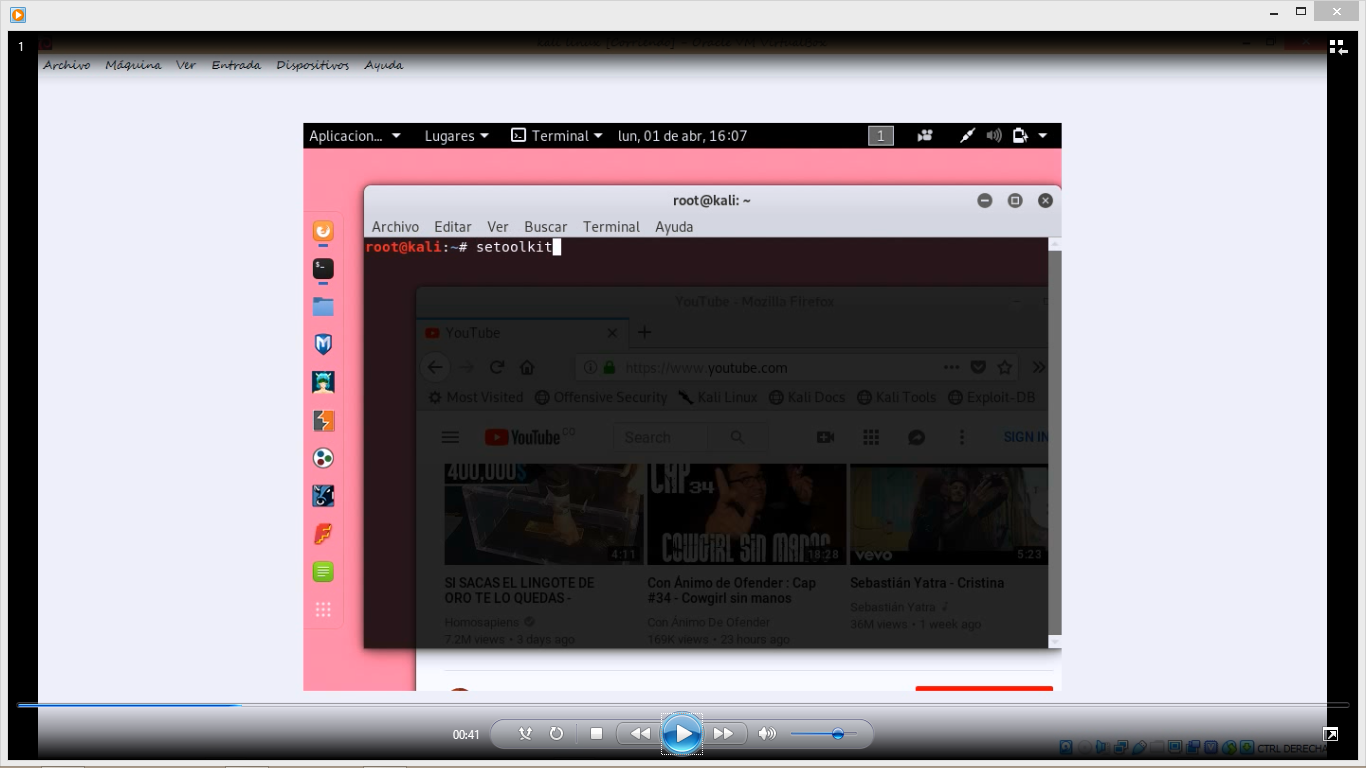
# ENUCIADO DEL PRIMER PUNTO

1.Describa e procedimiento frente a la técnica de ataque set , edifique y explique los pasos

# SOLUCION DEL PRIMER PUNTO

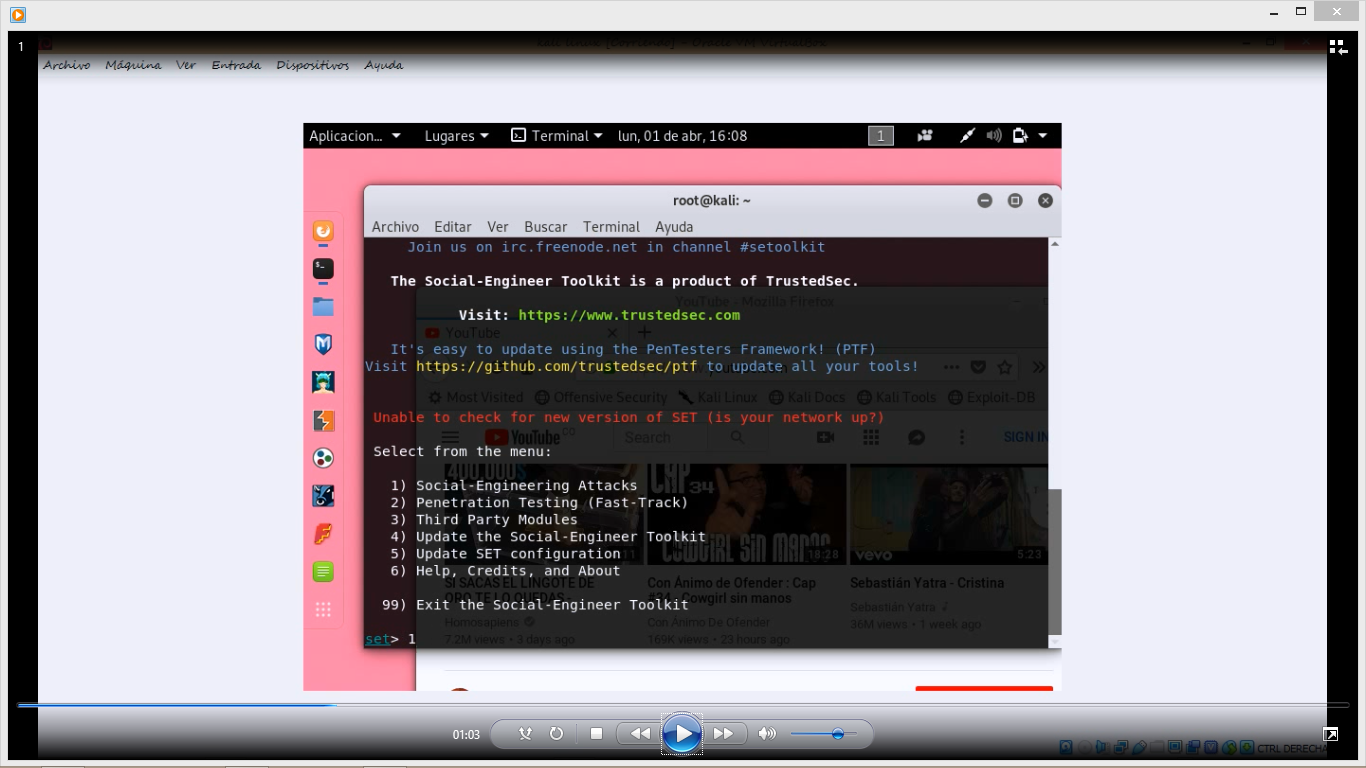
## Paso 1

En un sistema operativo Kali Linux se abre la ventana de comandos y en ella se escribe la siguiente instrucción “setollkit”, la cual invocara la herramienta en la misma ventana.



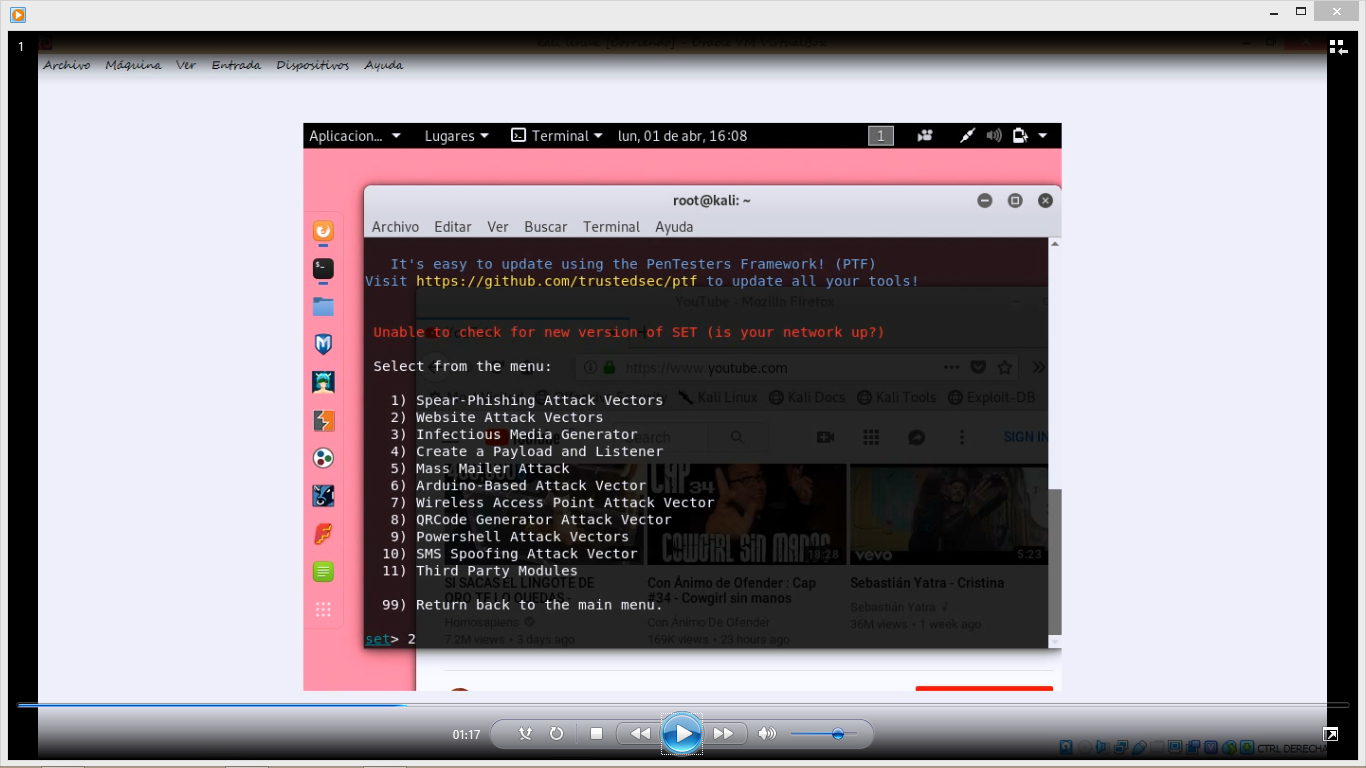
## Paso 2

Al ingresar a la herramienta en la misma ventana se le mostrara el menú donde podrá varias técnicas quelas cuales dispone dicho programa. En este caso se escogerá la opción “1) social engineering Attacks” que traducida al español es ingeniería social.



## Paso 3

Se le mostrara otro menú donde le ofrece 11 técnicas de ataque de ingeniería social, en este caso se seleccionara “2) wedsite Attacks Vectors”.



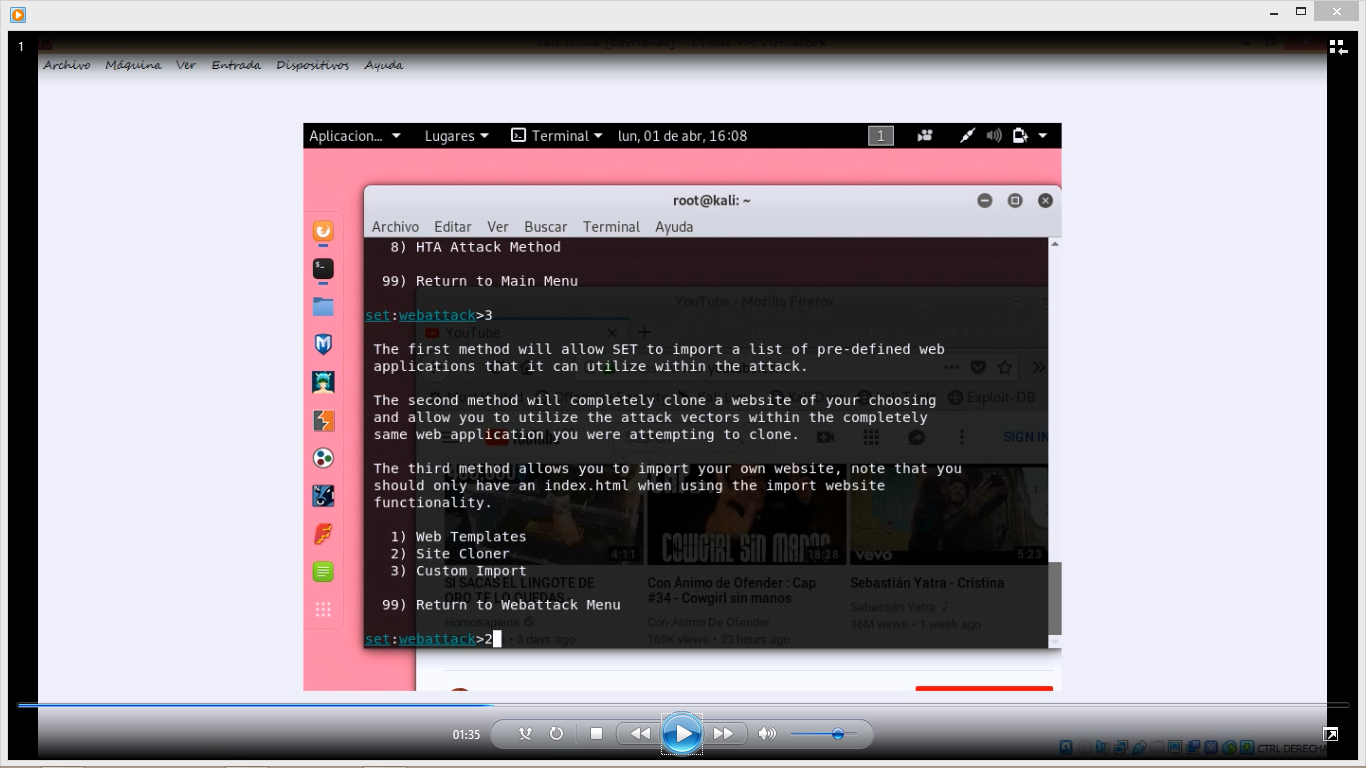
## Paso 4

Se le mostrara un nuevo menú donde se le ofrecen 8 opciones, en este se seccionara la opción “3) Credential Harvester Attack Method”.



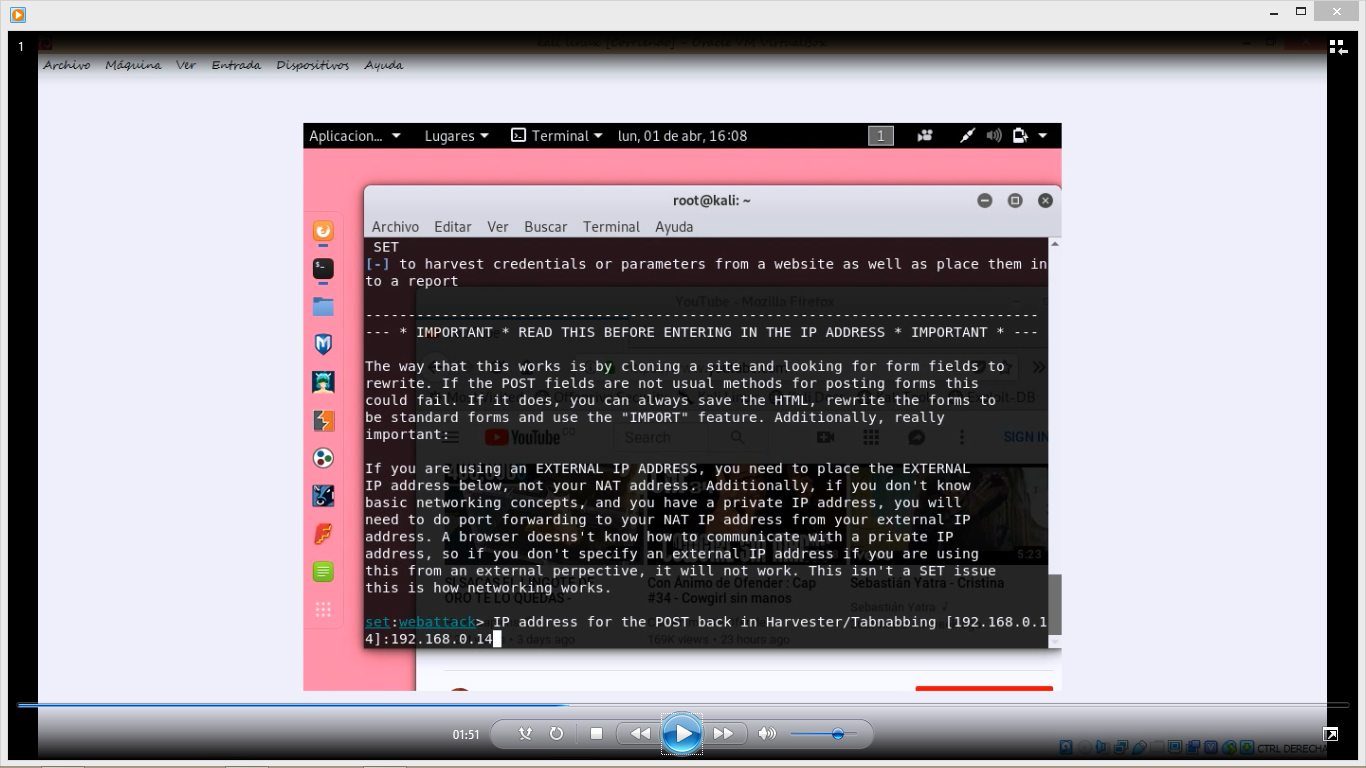
## Paso 5

En el nuevo menú se escogerá la opción de clonación de página web, la cual corresponde a la opción “2) Site Cloner”.



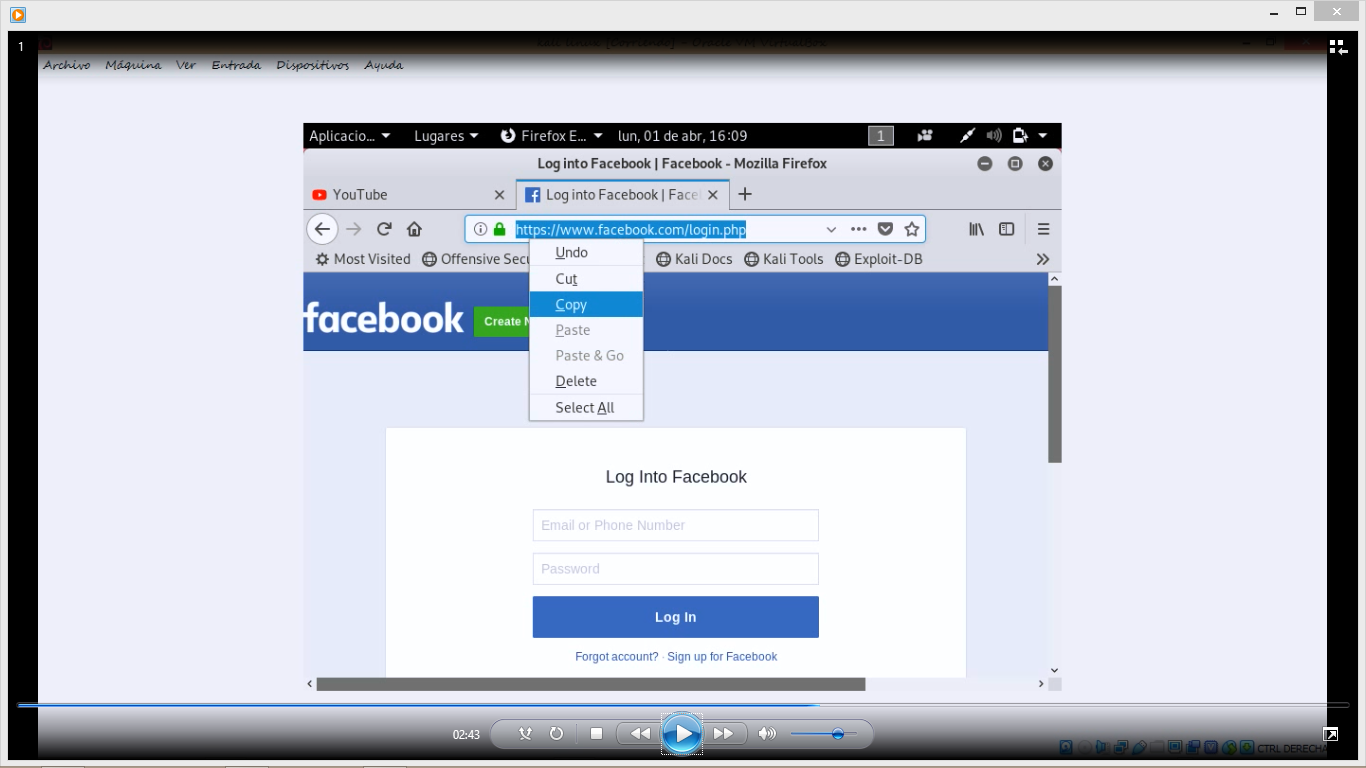
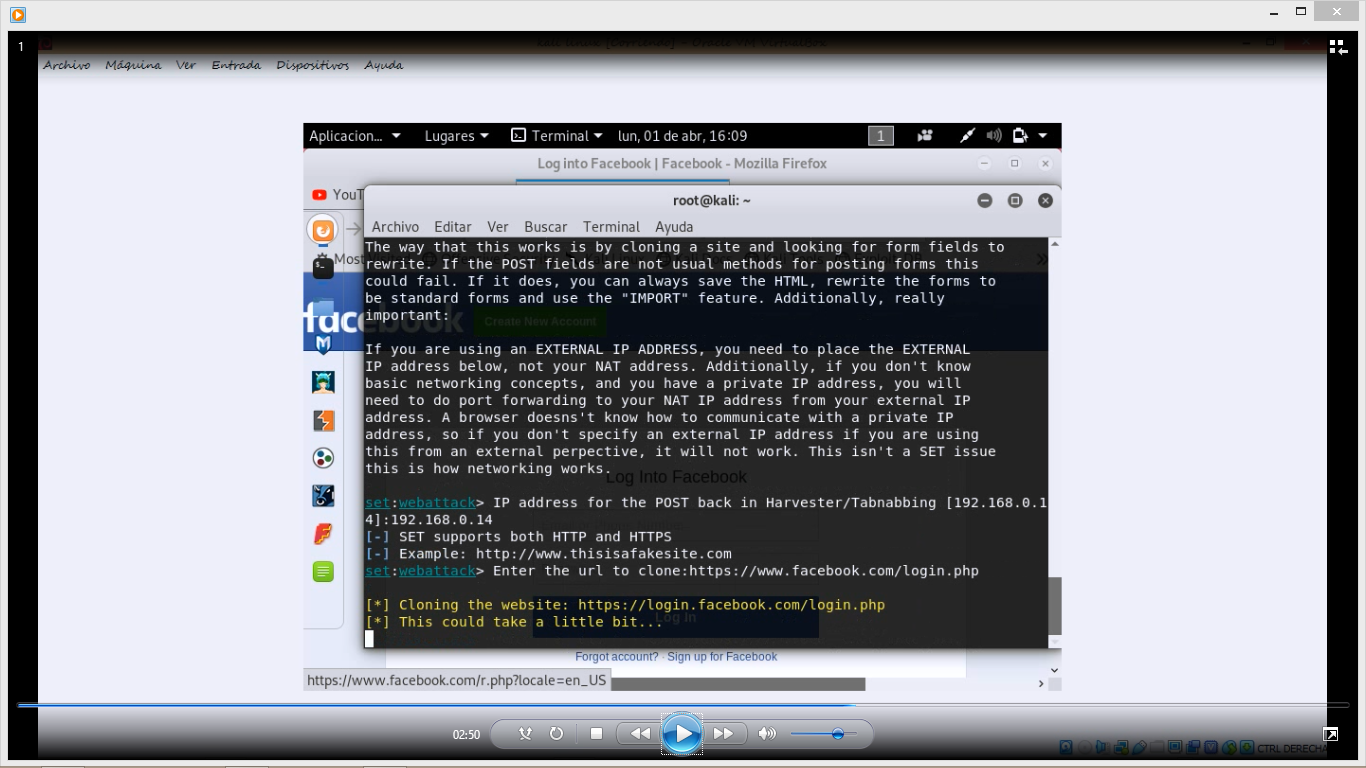
## Paso 6

Este le mostrara un mensaje, pidiéndole la dirección ip de su computadora Kali Linux. Solo tendrá que escribirla como se muestra e la imagen.



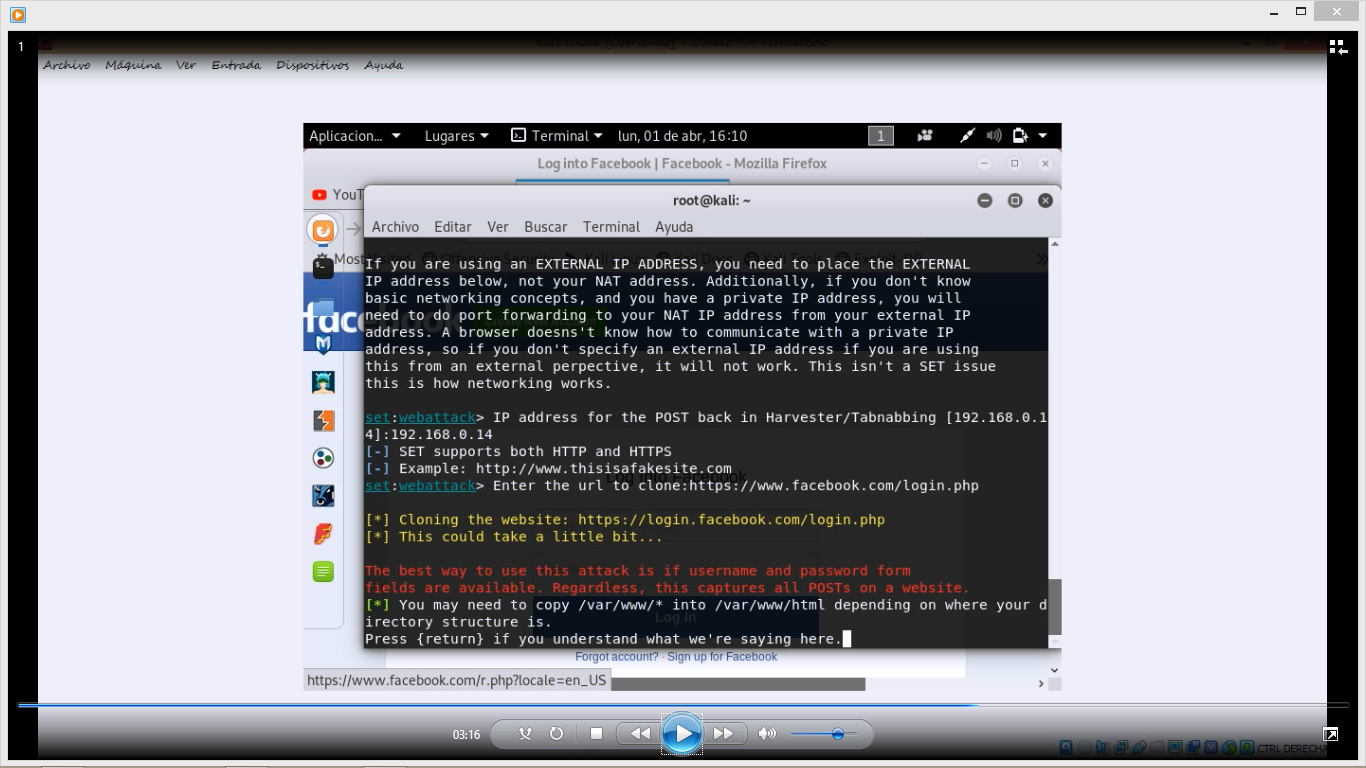
## Paso 7

En el siguiente mensaje, se le solicita una dirección url de la página que desea clonar en este caso copiaremos la de Facebook directamente del navegador y le daremos “enter” una vez copiada correctamente.



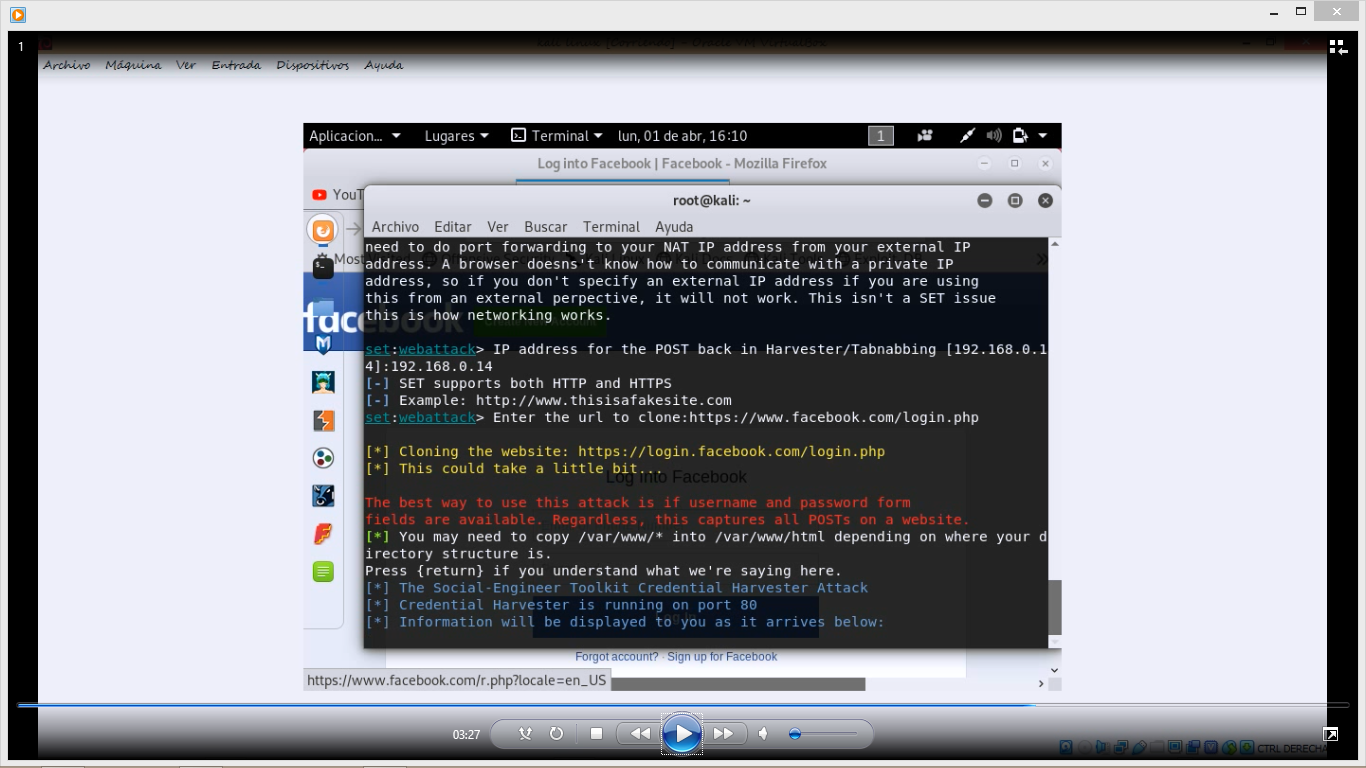
## Paso 8

Este comenzara a clonarla y en unos instantes le saldrá un nuevo mensaje el cual le solicita confirmación de la clonación, solo presionar enter.



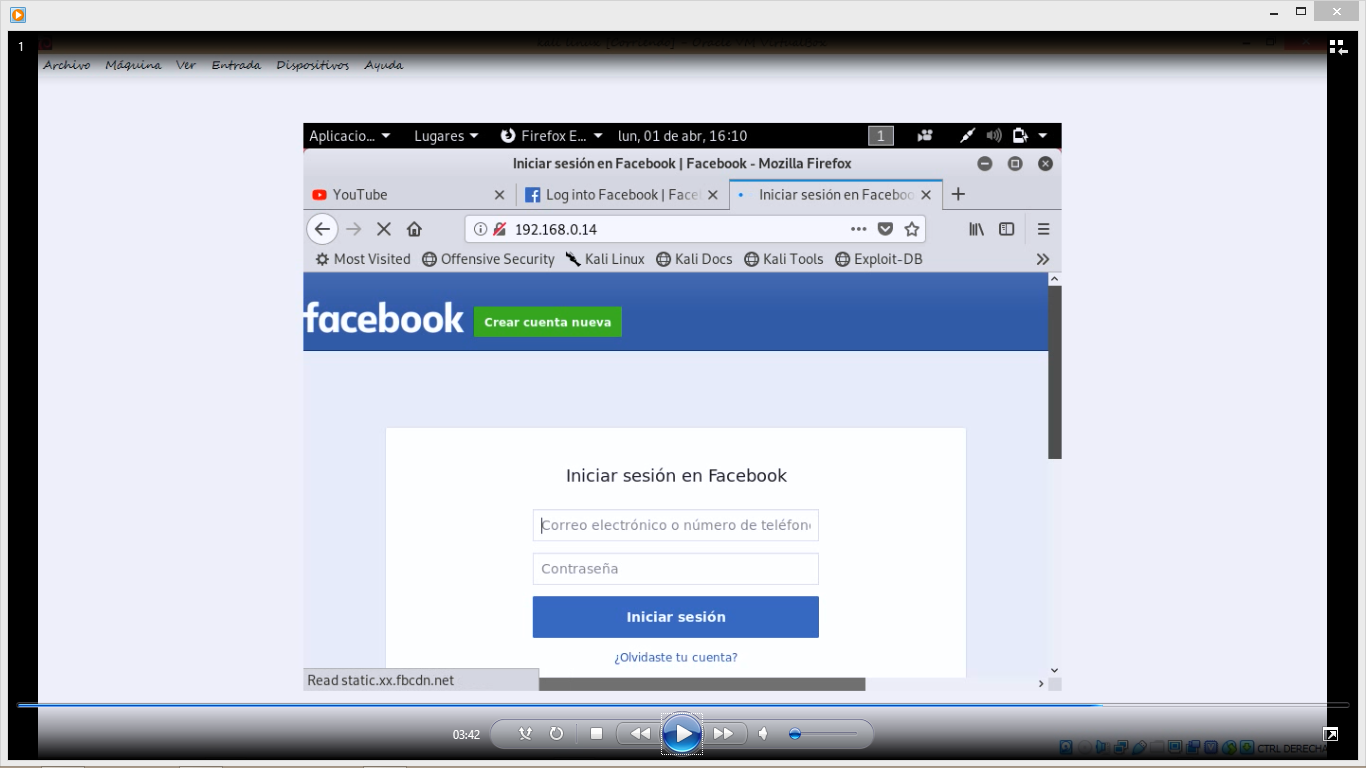
## Paso 9

Luego de unos minutos le saldrá tres líneas en color azul las cuales le indican que la clonación se ha realizado y puede ingresar a comprobarlo.



## Paso 10

Ingrese por su navegador a su dirección ip, como se indica en la siguiente imagen. Donde se puede comprobar que el sitio web sea clonado.



# ENUCIADO DEL SEGUNDO PUNTO

2.Particionar la memoria usb y formatear una partición Fat 16 y la segunda en ext4. Almacene\* información sobre cada partición, borre y recupere.

# SOLUCION DEL SEGUNDO PUNTO

SE Formateo de manera rápida en formato fat 16 luego se creó un archivo de texto y posteriormente se eliminó. Finalmente se intento recuperar por Recuva en Windows.

# ENUCIADO DEL TERCER PUNTO

3.Explique y mencione 5 ejemplos asociados al convenio de Budapest (en qué caso se dan)

# SOLUCION DEL TERCER PUNTO

En la “sección 1- Derecho penal sustantivo” definida por el “Titulo 1- Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos”. Tomado de [2]

Se pueden encontrar varios artículos(ejemplos) como:

* Articulo 3 – Interceptación ilícita

El cual dice que en el caso de presentarse “la intercepción deliberada e ilegitima por medios técnicos de datos de información en transmisiones no publicas dirigidas a un sistema informático o efectuadas dentro del mismo”. Tomado de [2] las partes involucradas lo pueden considerar como delito ya que podría haber intención delictivas. Ver [2]. Lo que quiere decir que si intercepta información a la cual no tiene un permiso de acceder con anterioridad será considerado Intercepción Ilícita.

* Articulo 5- Ataques a la integridad del sistema

El cual dice que cada parte involucrada tendrá que adoptar medidas legislativas para tipificar como delito “la obstaculización grave, deliberada y ilegitima del funcionamiento de un sistema de información mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.” Tomado de [2]. Lo que quiere decir que si intenta afectar a un sistema de cualquiera de las formas mencionadas será considerado como ataque a la integridad del sistema.

* Artículo 7-Falsificacion de información

El cual dice que cada parte involucrada tendrá que adoptar medidas legislativas para tipificar como delito “la introducción, alteración, borrado o supresión deliberada e ilegítimos de datos informáticos que generen datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia que los datos sean legibles e inteligibles directamente. Tomado de [2]. Lo que quiere decir que cualquier modificación de los tipos que se mencionó anteriormente que no sea autorizada por el sistema es considerada como falsificación de información.

* Articulo 4 – ataques a la integridad de los datos

El cual dice que cada parte involucrada tendrá que adoptar medidas legislativas para tipificar como delito todo acto deliberado e ilegitimo que dañe, borre, deteriore, altere o suprima datos informáticos. Tomado de [2]. Lo que indica que cualquier modificación no autorizada a los datos es considerada Ataque a la integridad de los datos.

* Artículo 2- Acceso Ilícito

El cual dice que cada parte involucrada tendrá que adoptar medidas legislativas para tipificar como delito el acceso deliberado e ilegitimo a todo o parte de un sistema informático. Tomado de [2]. Lo que quieres decir que si accede a un sistema sin previa autorización será considerado como Acceso ilícito.

# ENUCIADO DEL CUARTO PUNTO

4.Relacione las estafas que se dan en la banca electrónica.

# SOLUCION DEL CUARTO PUNTO

Las estafas relacionadas son:

* Phishing: Esta consiste en aplicar ingeniería social para obtener información de la víctima. Según [3].
* Skimming: Esta consiste en el copiado de la banda magnética de una tarjeta. Según [].
* Vishing: Esta consiste en la recreación de voz para suplantar funcionarios de entidades. Según [3].
* Smishing: Este consiste en enviar mensajes de texto que lo redireccionen a página fraudulenta. Según [3].
* Nigerianos: Esta consiste en ilusionar a la víctima con dinero y solicitarle un dinero por adelantado. Según [3].
* Loterías: Esta consiste en recolectar información por medio de loterías falsas. Según [].
* Falso Antivirus: Esta consiste en permitir el acceso de virus y recolección de información, ofreciendo un antivirus falso. Según [3].

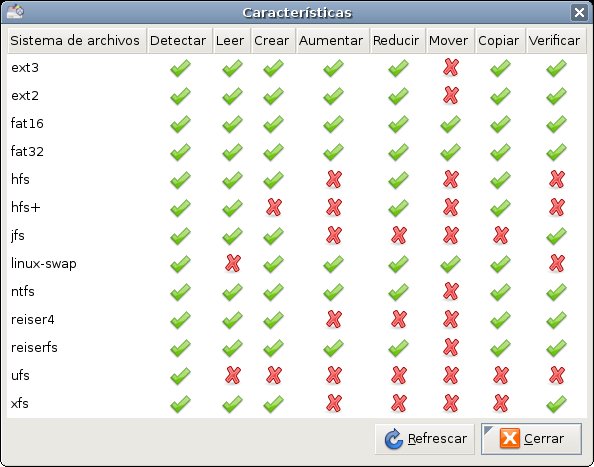
# ENUCIADO DEL QUINTO PUNTO

5.Mediante una tabla comparativa, relacione los diferencias, ventajas y desventajas, frente los archivos en Windows y Linux.

# SOLUCION DEL QUINTO PUNTO

Los sistemas de ficheros son estructuras lógicas del sistema operativo. Los cuales permiten estructurar la información para poder mostrarla, tanto de forma gráfica como de forma textual. Según [4].

Para sistema Linux podemos encontrar sistemas de ficheros: minix, xiq, ext2, ext3, ext4, reiserFS, xfs, jfs, nfs, cifs, ufs, sysfs, swap. Según [4].



comparativa de sistemas de fichero. Ver [4]

Para sistemas Windows podemos encontrar sistemas de ficheros: FAT 16, FAT 32, NTFS, Resf. Según [4].

# Bibliografía

[1]

[2] COUNCIL OF EUROPA, 2001, CONVENIO SOBRE LA CIBERDELICUENCIA, Budapest, pp 2.

[3]Patiño E. ,2019, Delito Informáticos Sesión No.5, Bogotá, Universidad San Buenaventura, pp 9.

[4] Raúl Juncos, 2008, Sistema de ficheros GNU/Linux, observatorio cnice.