OSCAR DAVID MESA CALDERON

TAREA CLASE 1

# PUNTO A.1

Mencione y explique mínimo 10 tipos de ataques de ingeniería social.

## Phishing

Este consiste en ataques por medio de envió de correos electrónicos masivo con links o contenido adjunto infectados por un programa maligno. Con el objetivo de tomar el control de la maquina o robar información. Otro caso es ganarse la confianza de la víctima para comprometer más información.

## Vishing/Phreakers:

Este consiste en ataques por medio de llamada telefónica con el objetivo de suplantando la identidad de una persona o compañía para conseguir información de la víctima.

## Redes Sociales

Este consiste en ataques por medio de publicaciones, mensajes, observar en las redes sociales. Con el objetivo de recolectar información en e principal caso para extorsionar o para conocer mas a la victima. También de da el caso de publicaciones o enlace que redirigen a páginas con programas maliciosos.

## Baiting

Este consiste en ataques por medio USB infectadas con un programa maligno, colocadas en el camino de un trabajos o estudiante a una institución o oficinas. Con el objetivo de que la encuentre y la use en computadoras del edificio o en su computadora personal.

## Smishing

Este consiste en ataques por medio de mensajes de texto, donde suplantan una compañía para que accedan a un link , llamen a un numero o respondan al mensaje. Con el objetivo de infectar el dispositivo móvil o solicitar información.

## Pretexting/Impersonate

Son dos ataques los cuales se usan en conjunto por medio de suplantar un servicio técnico de la empresa a la que pertenezca la victima con el objetivo de convencerlo de algún error en su equipo o cuenta, posteriormente intervenir en el equipo o cuenta con ayuda de la victima para robar información o instalar programas.

## Tailgaiting

Este consiste en ataques por medio de abusar de la amabilidad del empleado que esta ingresando en las instalaciones de trabajo. Intentando entrar con la entrada del empleado real escusándose de no traer tarjeta de ingreso. Otro caso es cuando no comprueban el documento físico de una visita.

## Dumpster Diving

Este consiste en ataques por medio de revisar el cubo de basura de la victima en busca de documento con información del mismo o datos de su ambiente.

## Shoulder Surfing

Este consiste en ataques por medio de la observación a la victima en momento que ingresa una credencial o información en su celular o información.

## Farming

Este consiste en ataques por medio comunicación prologada con la victima con el objetivo de conseguir datos personales. Utilizando chantajes con videos privados o la misma información.

# PUNTO A.2

Relacione un caso real para cada uno de los tipos de ataques.

## Suplantación Telefónica

Relacionado con el ítem 2 del punto A.1. Kebin Mitnick, accedió al número del policía que lo custodiaba en el arresto domiciliario. El número había sido suspendido sin embargo este no había sido dado de baja en la oficina, dando como resultado que Kevin se hiciera pasar por el oficial con el numero aun registrado para obtener información del oficial.

## Suplantación BBVA

Relacionado con el ítem 1 del punto A.1. Correos masivos los cuales suplantan una cuenta de servicio de BBVA con el asusto confirmación de datos, la cual redireccionaba a una página web falsa donde le solicitaba ingresar sus credenciales de ingreso a dicha entidad.

## Estafa Nigeriana

Relacionado con el ítem 1 y 6 del punto A.1. Estafa que promete por medio de un correo electrónico que expresa una significativa herencia o rifa ganada. A razón de lo anterior se solicita un abono por anticipado para recibir la recompensa.

## Muerte de celebridades Ricardo Arjona

Relacionado con el ítem 3 del punto A.1.Acidenete aéreo donde falsamente murió el cantante fue publicada como noticia en Facebook, donde ciberdelincuentes aprovecharon para colocar link a la noticia que redirigían a lugar engañosos.

## Botón “no me gusta”

Relacionado con el ítem 3 y 5 del punto A.1. Funcionalidad de Facebook de incluir un botón de “no me gusta” la cual se ofr4ecia por publicaciones que decían necesitar una instalación mediante un botón en la misma publicación. Botón el cual solo suscribía a la victima a un servicio de sms premium.

## Facebook Rosa

Relacionado con el ítem 3 y 1 del punto A.1. Presentaba como mensajes con un enlace en la biografía del usuario. Al acceder en enlace le dabas acceso a tu lista de contactos y algunos a azar para publicar automáticamente en su muro el mismo mensaje.

## Suplantación Correos

Relacionado con el ítem 3 y 5 del punto A.1. la cual expresaba un paquete entrante el cual debía reclamar, la gestión para reclamarlo era por medio de una aplicación que sugiere el correo que instalara. En caso de no instalarla el correo expresaba un cargo extra por día que no se recoge el paquete. Dicha aplicación encripta el contenido de los archivos de la victima para luego pedir un recate.

## Virus Stuxnet

Relacionado con el ítem 4 del punto A.1. En el 2010 se introdujo una USB en el centro nuclear de Natanz. El cual propago el virus por la red de las instalaciones y termino utilizando las centrifugadoras usadas para enriquecer el uranio.

## WhatsApp PC

Relacionado con el ítem 1 y 3 del punto A.1. En Brasil cuando aún no existía la versión oficial para pc de este programa comenzó a circular correos ofrecían dicho programa el cual le ofrecía un programa falso que contenía un programa maligno que recolectaba información bancaria.

## Facturas Falsas

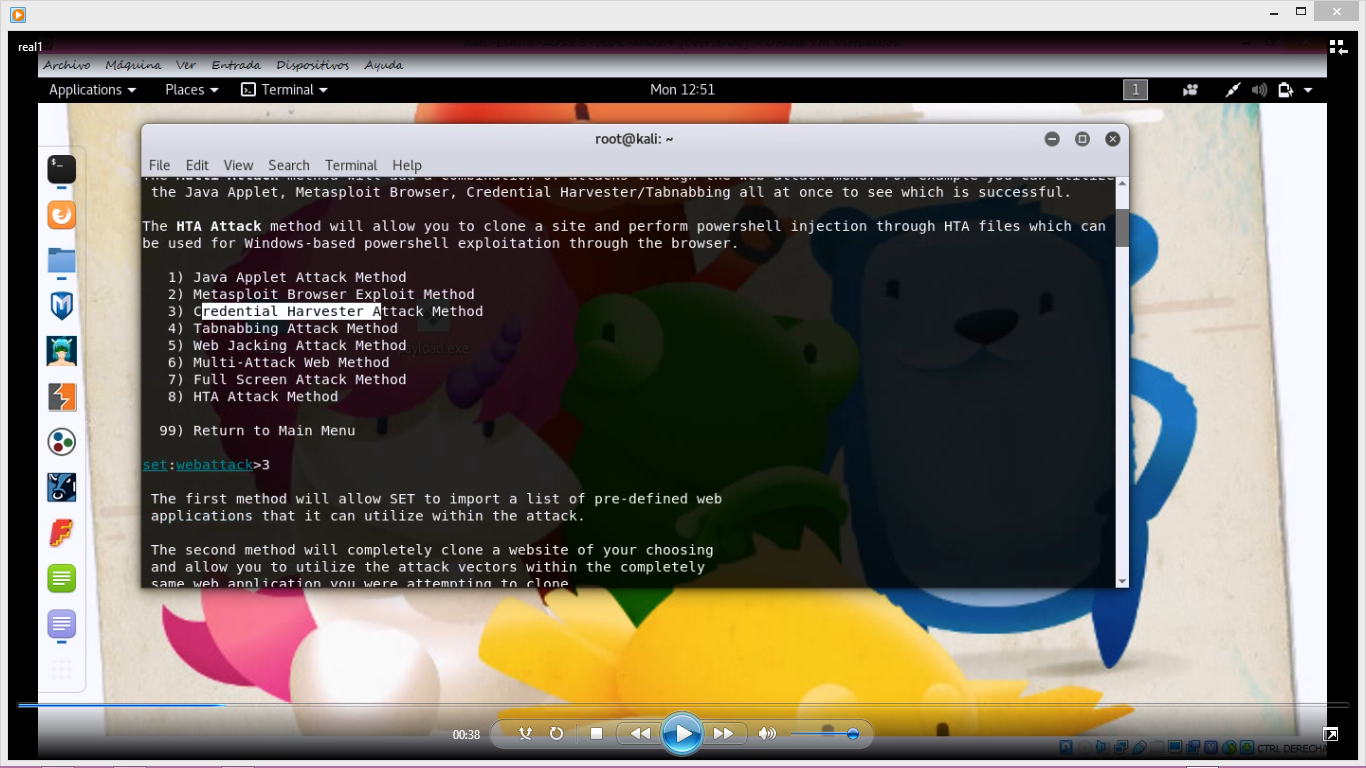
Relacionado con el ítem 1 del punto A.1. Oleada de correos con facturas en formato Excel las cuales estaban realizadas como un macro el cual puede realizar instrucciones si habilitamos la edición del documento una vez descargado. O causaba la instalación de un programa maligno la computadora de la víctima.

# PUNTO B

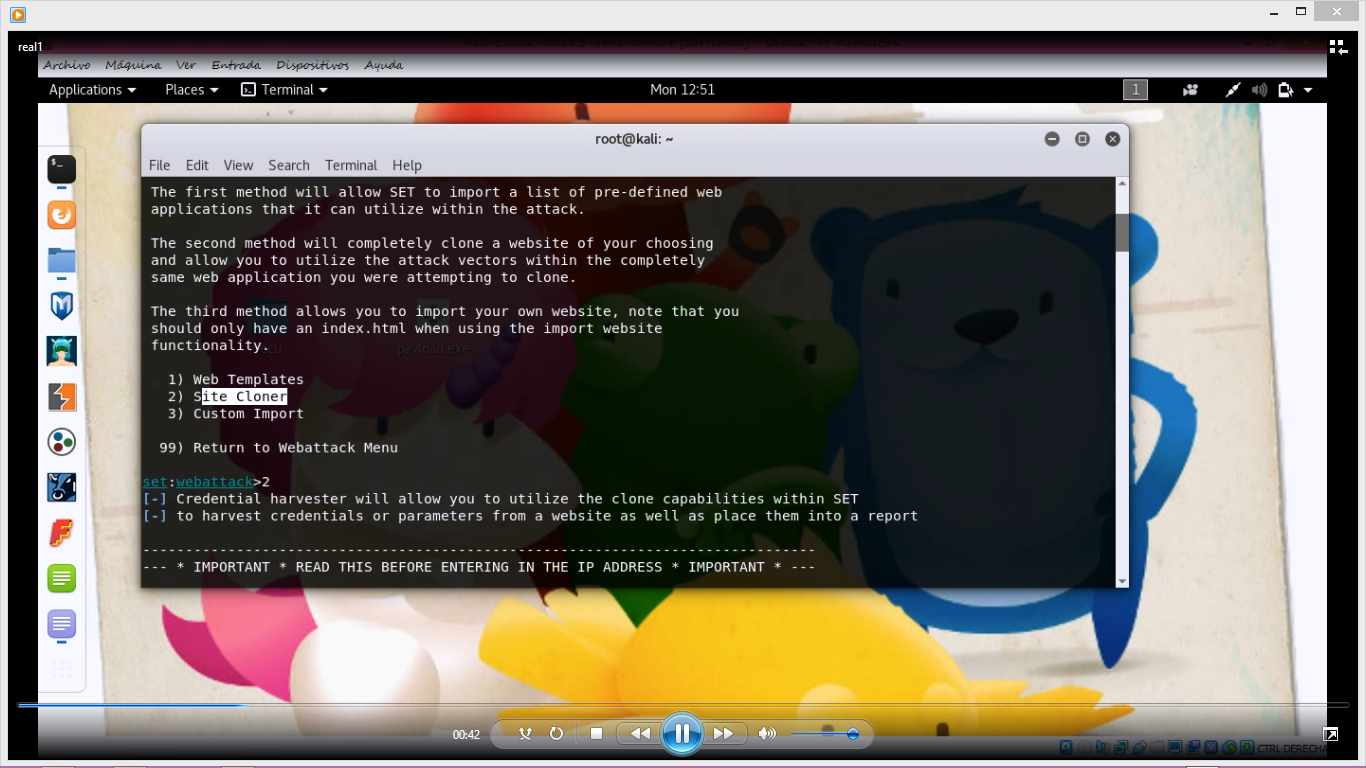
Aplique 2 de las técnicas de ataque por medio de la herramienta SET de Kali Linux.

## Website Attack Vectors

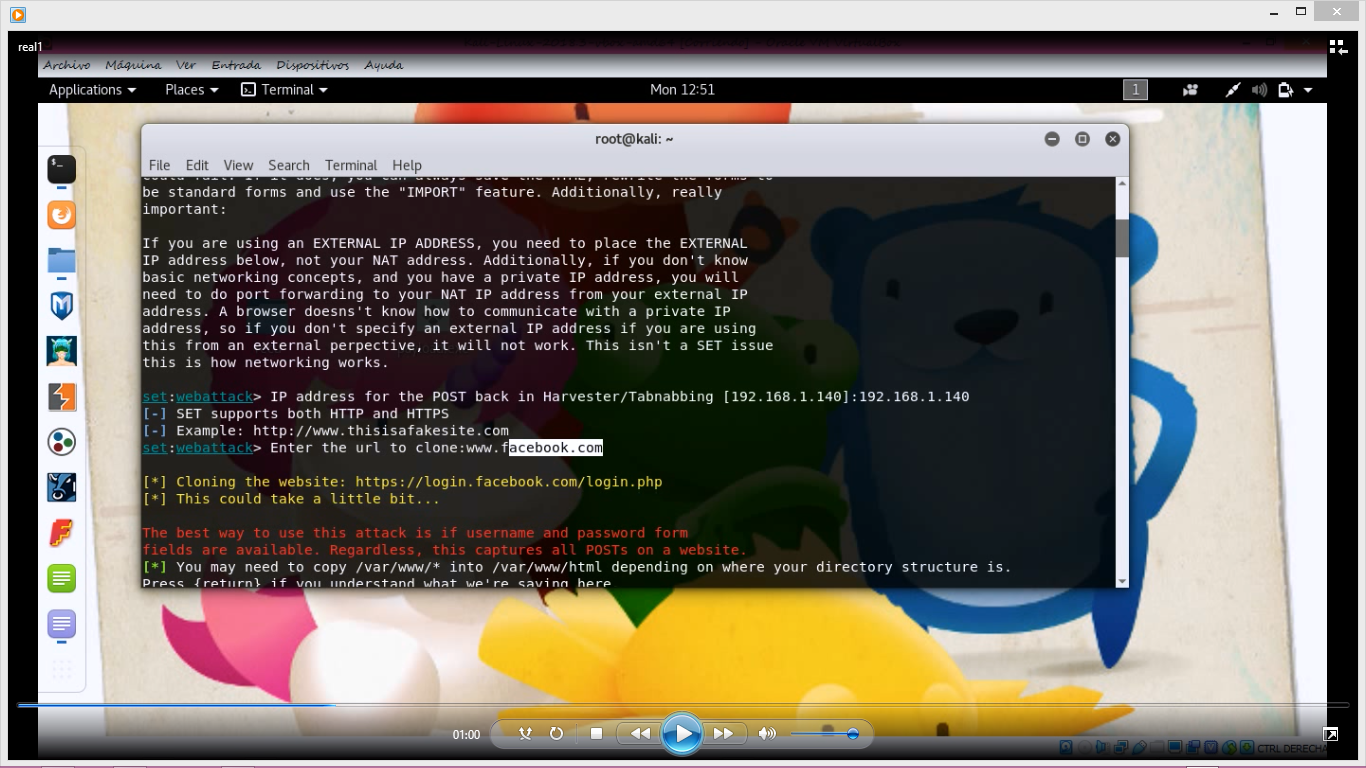
El tipo de ataque se denomina Credential Harvester Attack Method el cual consiste en obtener credenciales.



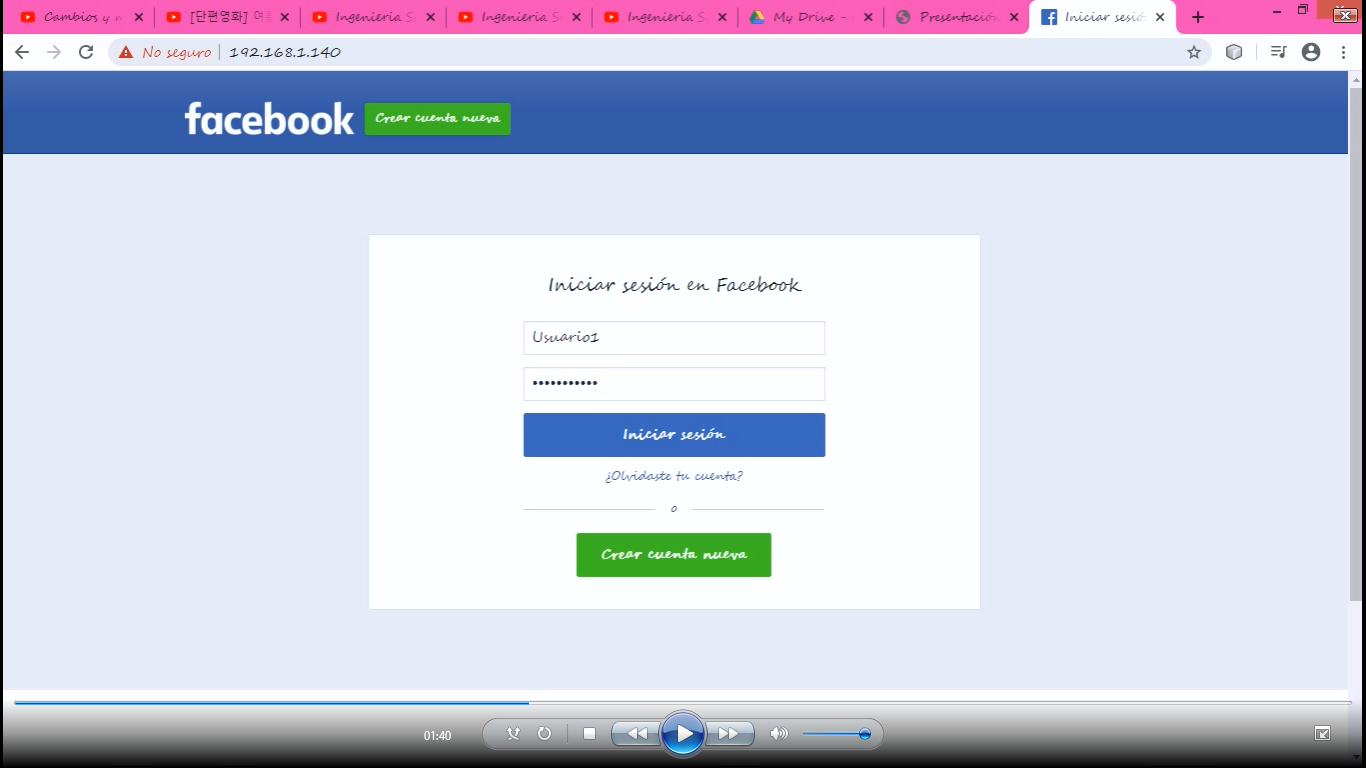
El método a utilizar será clonando un sisio web donde la victima inicie sesión.



La página para clonar será el login de Facebook el cual será clonada en el localhost de la dirección ip de la maquina atacante.



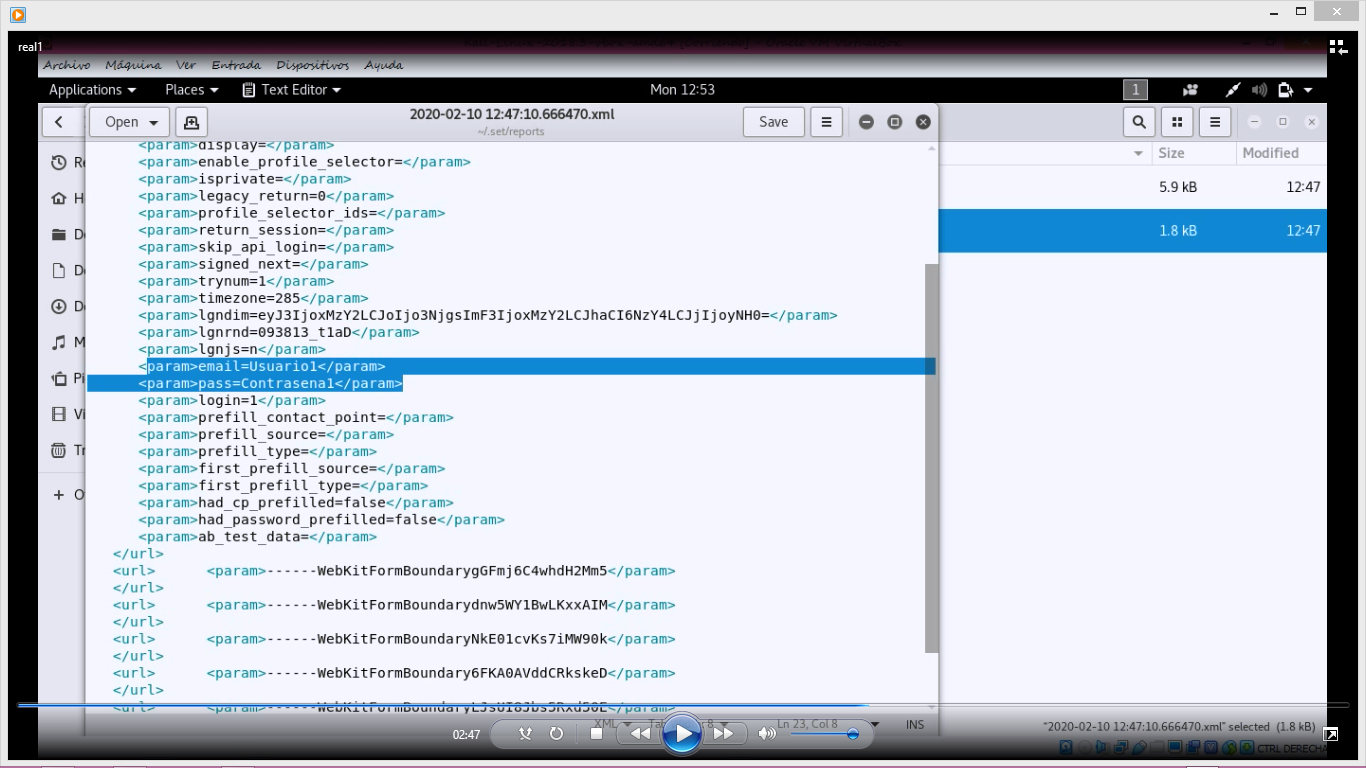
Ya con el servidor de la pagina clonada encendida, desde cualquier computador de la red donde se encuentre el atacante. Podrán acceder al sitio e iniciar sesión.



Cuando la víctima inicie sesión, los datos consignados terminaran e la maquina del atacante en la siguiente dirección. El archivo .xml contendrá la información de las victimas dentro de la cual se incluye el usuario y contraseña.

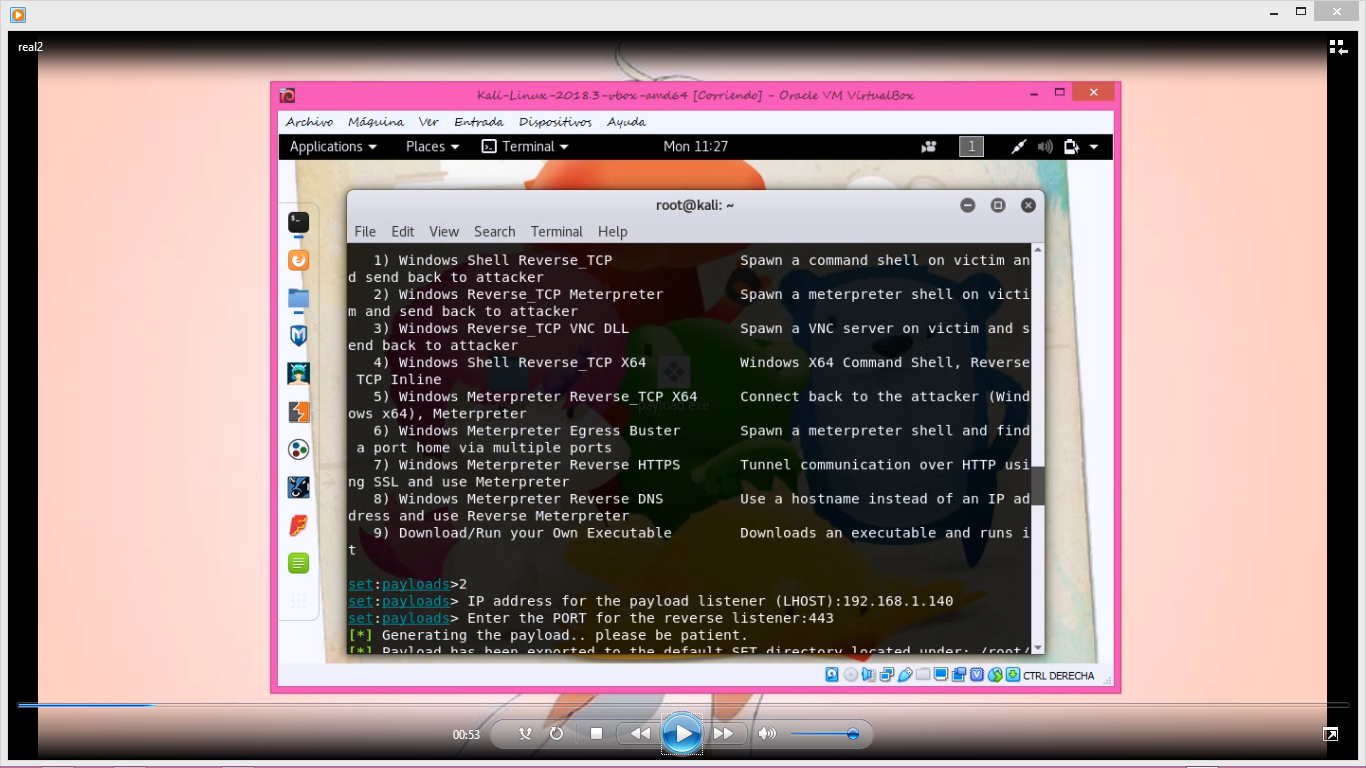


El contenido del archivo contiene la información que el usuario ingreso en el sitio web clonado.

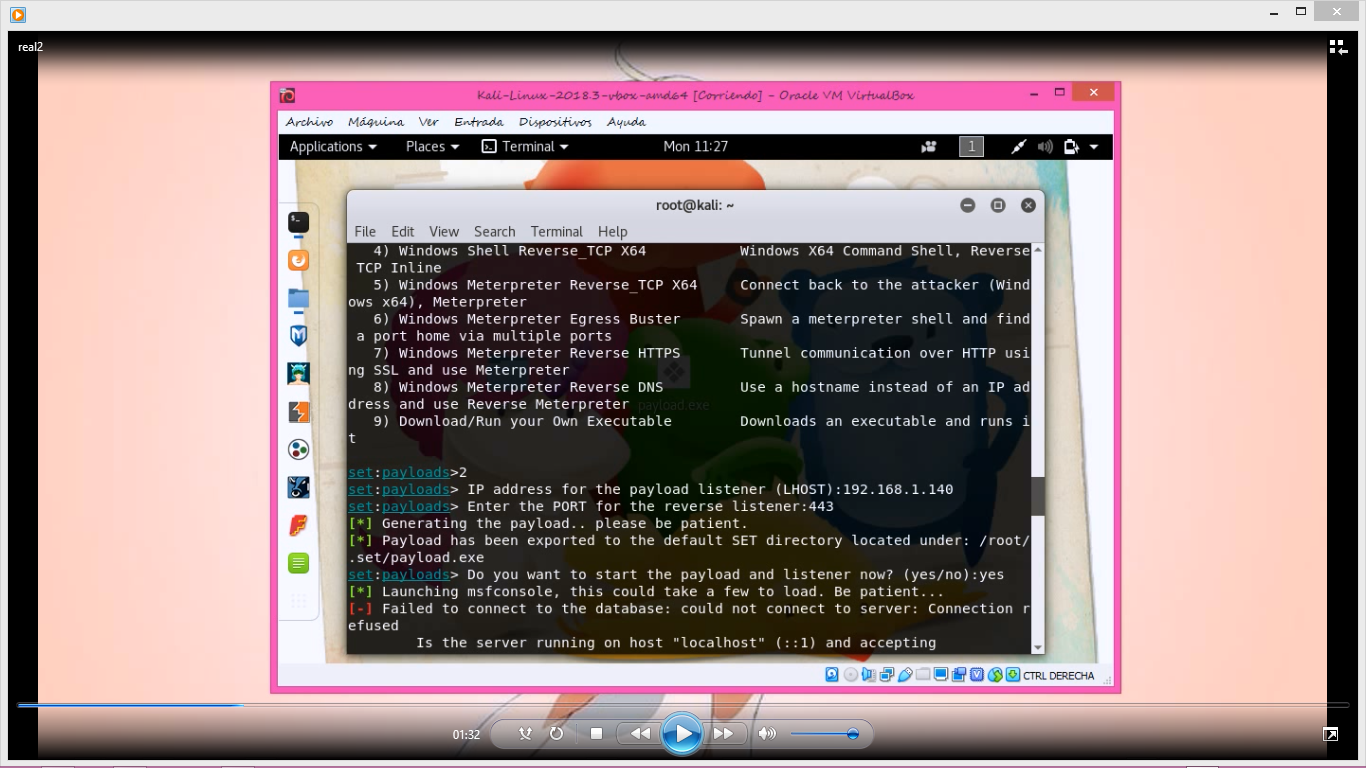


## Create a Payload and Listener

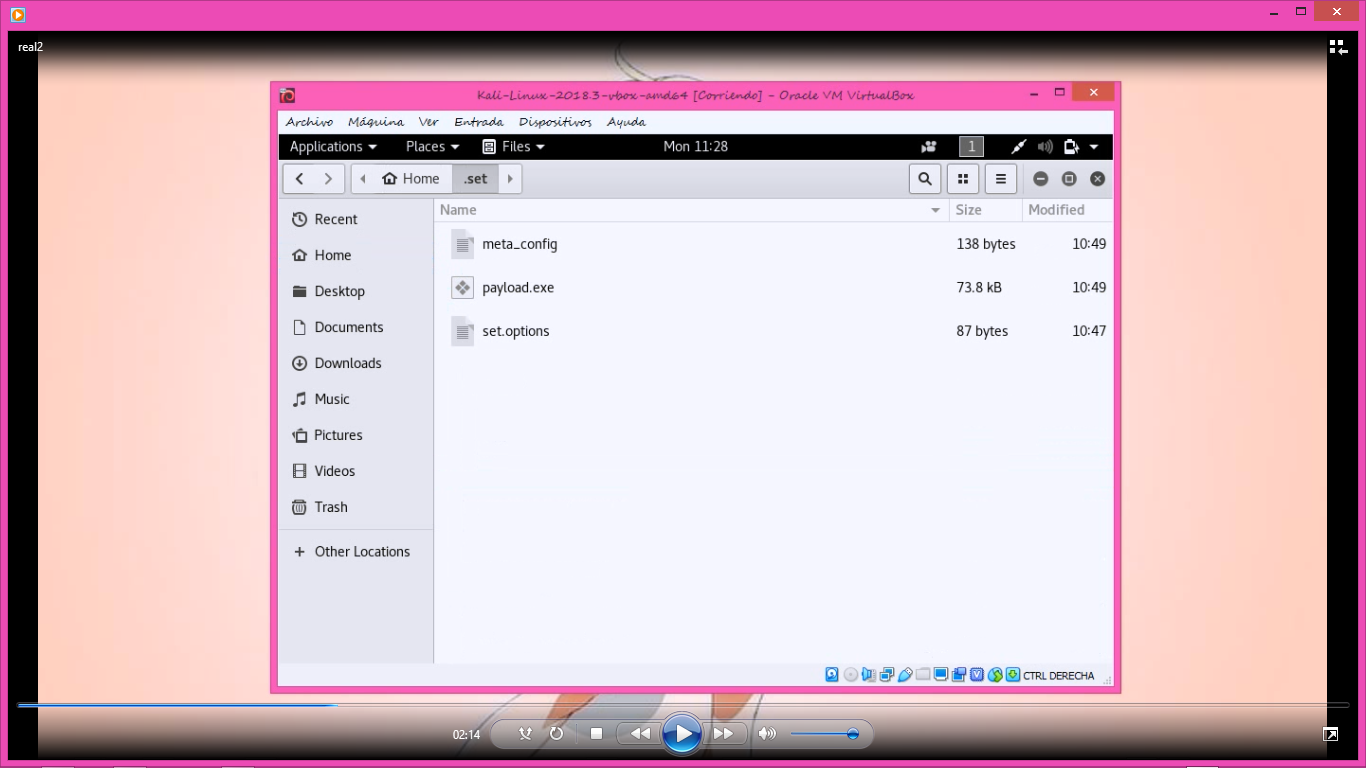
El método a ejecutar fue Windows Reserve\_TCP Meterpreter, se puede interpretar como un ejecutable que tomara información de tu maq8uina y la enviara por el protocolo TCP al atacante.



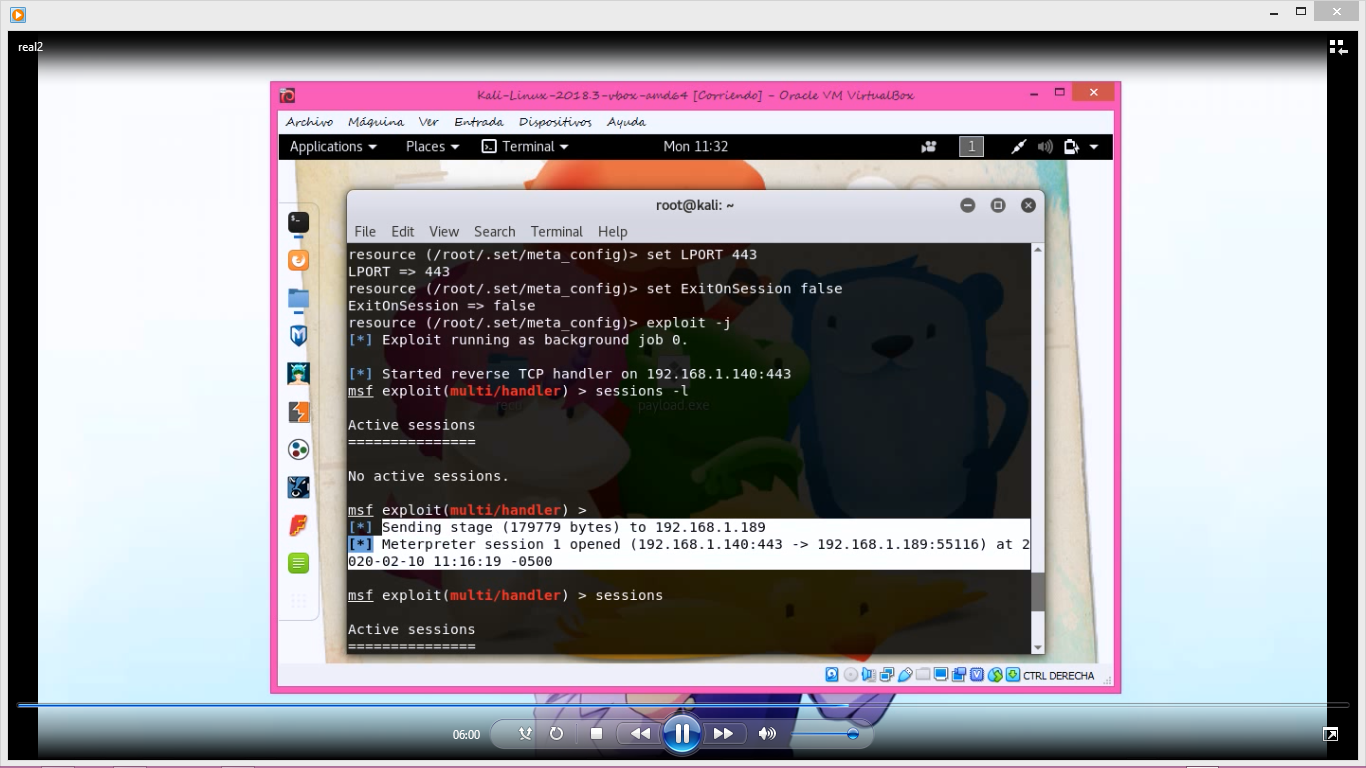
Posteriormente, les pedirán el host local donde llegará la información y el puerto por el cual se conectará desde la maquina víctima. Se recomienda poner el puerto 443.



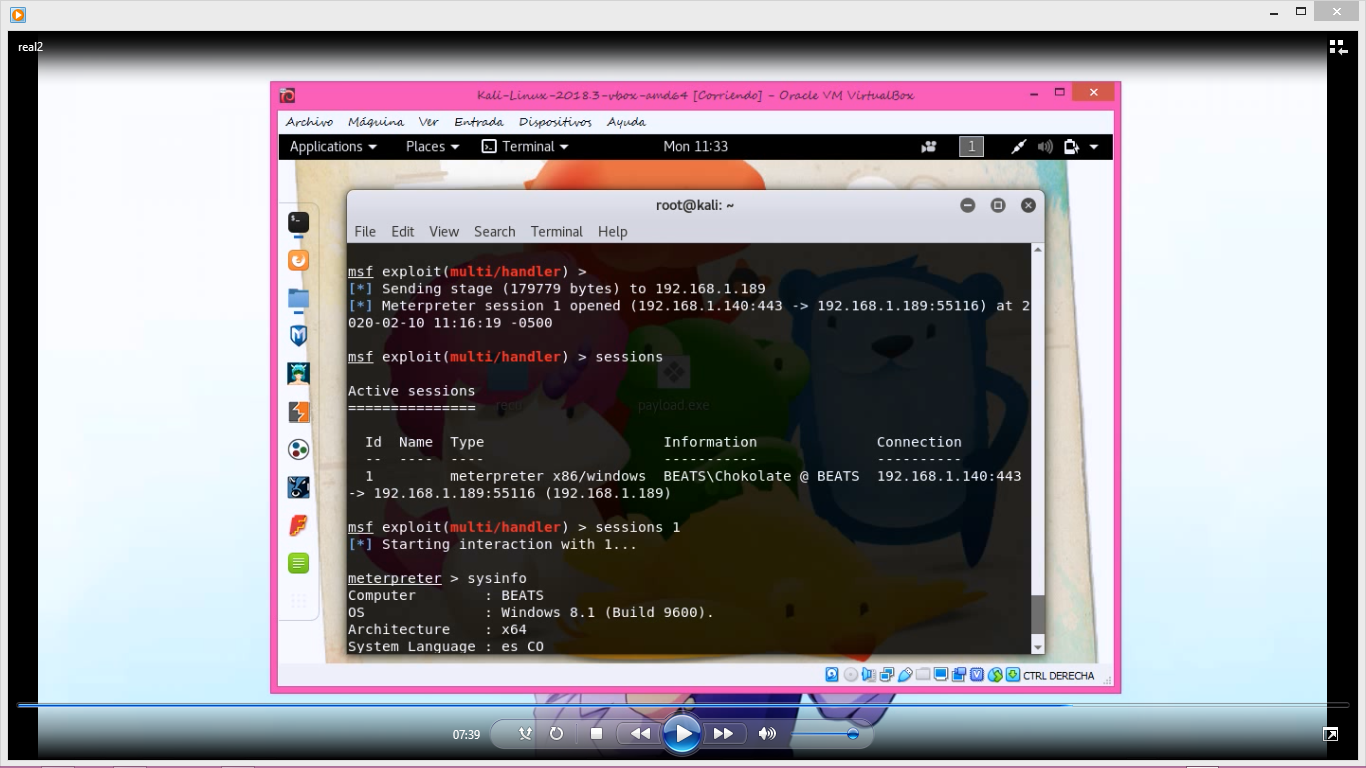
Luego se generará el payload con extensión .exe en la carpeta que se muestra en la imagen. Este ejecutable es el “programa” que al ejecutarse infectara la maquina de la víctima. Esconderlo dentro de otro formato puede funcionar para la victima lo ejecute o subiéndolo a algún servidor donde se prometa descargar algo y lo que se esté haciendo este instalar el payload.



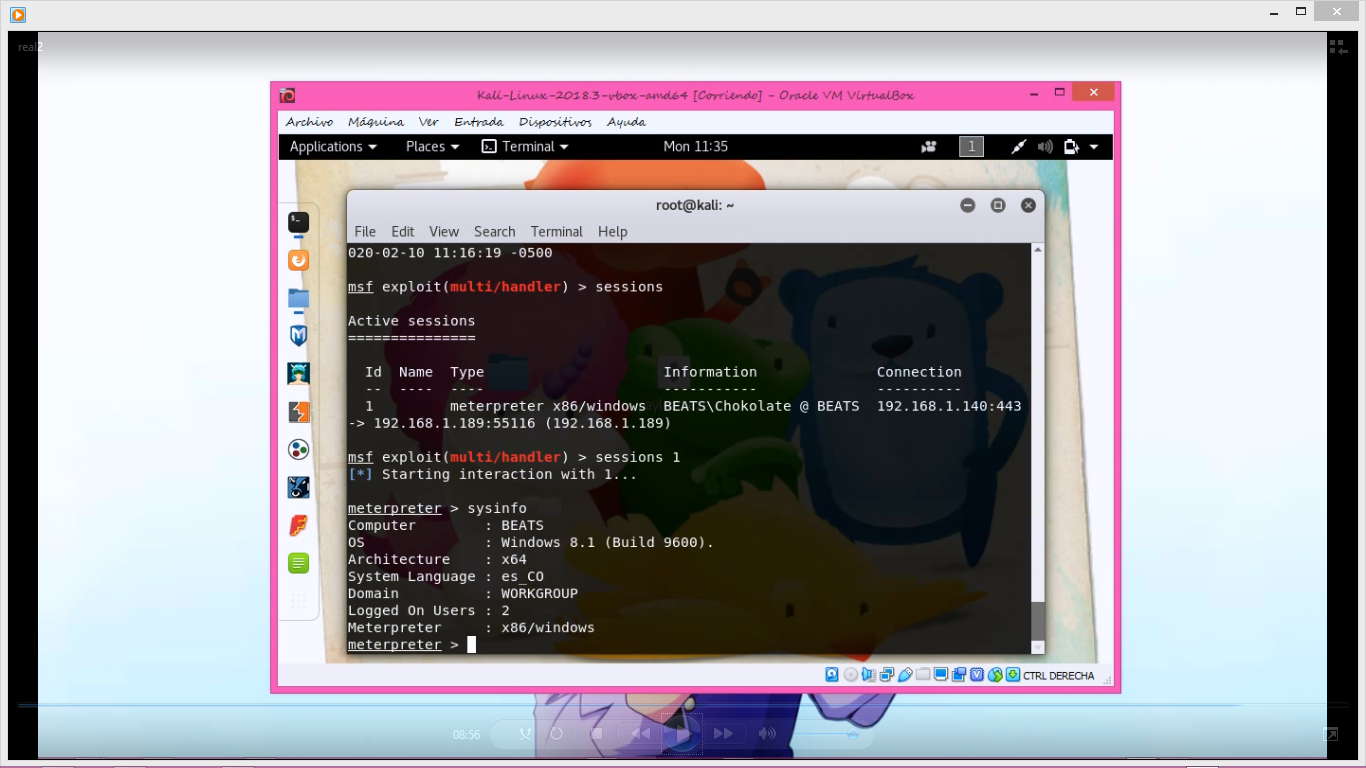
Cuando la victima lo ejecute, en el ordenador del atacante aparecera lo siguiente. Indicanddole que una ma1uina con ip 192.168.1.189 a instalado el programa y que la conexion esta hecha.



Posterior a esto se ejecuta el comando sessions para comprobar y sessions 1 para escoher la victima y conectar a su equipo.



Una vez dentro puede ejecutr el comando sysinfo por ejemplo, el cual le mostrara inforacion del equipo de la victima.



# Bibliografía

1. https://ayudaleyprotecciondatos.es/2019/01/09/ataques-ingenieria-social-evitarlos/
2. http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/
3. https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse
4. https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-correos-extorsionan-supuestos-videos-privados
5. https://www.incibe.es/protege-tu-empresa/avisos-seguridad/detectada-oleada-correos-facturas-infectaran-tu-equipo
6. https://www.incibe.es/protege-tu-empresa/avisos-seguridad/campana-phishing-suplantando-entidad-bancaria-bbva
7. https://ciberseguridad.blog/anatomia-del-ataque-de-ingenieria-social-y-como-prevenirlo/
8. https://aprendederedes.com/seguridad-informatica/ingenieria-social/
9. <https://www.welivesecurity.com/la-es/2015/12/01/historias-de-ingenieria-social-ridiculas/>

## Videos

funciono real 1

<https://www.youtube.com/watch?v=bH9cgiI55g4>

funciono real 2

<https://www.youtube.com/watch?v=PnuynLy0NvU>