Universidad San Buenaventura

Sede Bogotá

Técnicas de ataque

Ing. José Eduardo Patiño Santafé MSc.

Ataque social

Gabriel Peña Rodríguez

Bogotá D.C

Febrero 12 de 2020

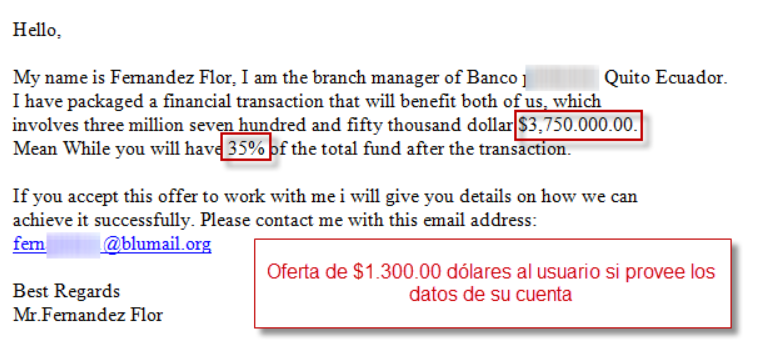
1. La estafa nigeriana

Es el cuento del tío de la era de Internet. ¿Quién no soñó con recibir una inesperada herencia de un pariente lejano?

Los scammers detrás de este tristemente célebre engaño fueron precursores de algo que no solo perduró, sino que se expandió a diversos países e idiomas. Recibió su nombre a raíz del número de artículo del código penal de Nigeria que viola, ya que buena parte de las estafas provienen de ese país y de otros pertenecientes a África.

La estafa nigeriana promete a su víctima una gran fortuna, convenciéndola de que la suma le corresponde por una herencia, por ser ganador de un sorteo, por una generosa donación, porque las autoridades de un país lo necesitan o por otros diversos motivos. Como condición para acceder a ella, se exige el pago de un adelanto nada económico, pero bajo comparado con lo que supuestamente se va a ganar luego.

Naturalmente, existen numerosas variantes de la estafa nigeriana. Eventualmente, hubo casos traducidos al español y dirigidos a usuarios de Latinoamérica, como el que podemos ver en la siguiente captura:



1. Scams relacionados a muertes de celebridades

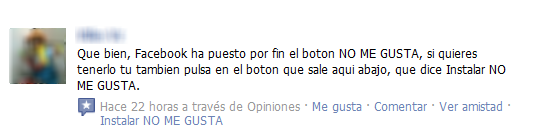
Los casos aquí abundan y no hacen más que demostrar cuánto les rinde a los cibercriminales aprovechar noticias de famosos fallecidos o incluso inventar que murieron, gracias a lo cual consiguen que cientos de usuarios curiosos hagan clic en enlaces engañosos.

Por mencionar algunos ejemplos, tenemos la falsa muerte del cantante Ricardo Arjona y también la del automovilista Michael Schumacher, el suicidio del actor Robin Williams o el rumor de que Michael Jackson estaba vivo.

[](https://www.welivesecurity.com/la-es/2015/05/26/muere-ricardo-arjona-engano-facebook/)

1. Falsas noticias alarmantes de Facebook

Es probable que alguno de tus contactos haya caído en el resonante engaño de que Facebook cambiaría su color a rosa, el cual se propagaba a través de mensajes en las biografías de los usuarios que contenían un enlace. Al hacer clic, se producía una redirección a un sitio infectado. Algo similar sucedía con la supuesta posibilidad de ver quién visitó tu perfil, que a través del clickjacking obtenía al azar los nombres de los contactos de la víctima para publicar automáticamente en su muro y así continuar la propagación de la amenaza.

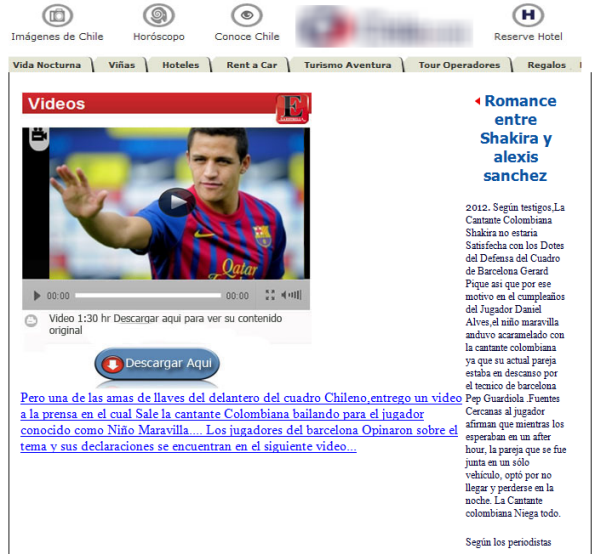
[](https://www.welivesecurity.com/la-es/2011/05/16/engano-facebook/)

Igualmente famoso fue el falso botón “No Me Gusta”, que terminaba ocasionándole a la víctima un gasto extra al quedar suscripta en servicios de SMS Premium. A fin de cuentas, en ese entonces Facebook nunca había anunciado la implementación de esta controversial característica, aunque luego de años de usuarios pidiéndola, Mark Zuckerberg confimó que estaban trabajando en una alternativa al “Me Gusta”. Vendrá en forma de “Reacciones” y ya ha sido implementado en España e Irlanda, con sentimientos como “Me encanta”, “me divierte”, “me alegra”, “me asombra”, “me entristece” o “me enfada” y sus respectivos emojis.

1. Fotos y videos íntimos de famosos, para los más extremos

Muchas fueron las celebridades víctimas de la filtración de fotos íntimas, entre ellas Jennifer Lawrence, Ariana Grande, Rihanna, Kate Upton y Kim Kardashian, en lo que se conoció como Celebgate el año pasado. Como consecuencia, no tardaron en aparecer amenazas disfrazadas de archivos y carpetas conteniendo el material robado, así como scams con enlaces que supuestamente permitían ver videos XXX de las actrices.

Nuestra región no fue la excepción: aquí, Shakira fue objeto de una campaña que propagaba en Facebook un falso video íntimo, en el que la cantante supuestamente había cometido en público un acto poco digno. Al poco tiempo, apareció otro supuesto video que aparentaba mostrar un romance oculto entre ella y el jugador de fútbol Alexis Sánchez, basado en el hecho de que su pareja real, Gerard Piqué, no tenía tantos dotes como ella hubiera querido.

[](https://www.welivesecurity.com/la-es/2012/03/02/video-supuesto-romance-shakira-alexis-sanchez-propaga-malware/)

1. WhatsApp para PC, scam antes de realidad

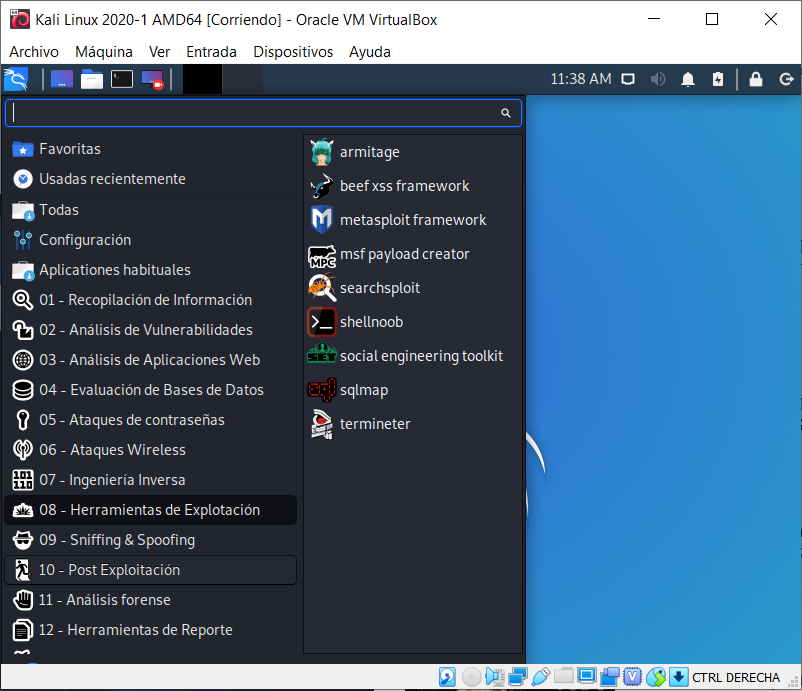
A principios de este año WhatsApp Web ya había sido ampliamente adoptado en la comunidad de usuarios móviles, pero antes, cuando todavía no existía este programa en forma legítima, era un frecuente gancho de scams. Como millones de personas lo esperaban, eran muchos los que hacían clic sin dudarlo cuando se encontraban con una oferta de WhatsApp para PC.

[](https://www.welivesecurity.com/la-es/2014/01/09/whatsapp-para-pc-cibercriminales-buscan-enganar-usuarios-brasil/)

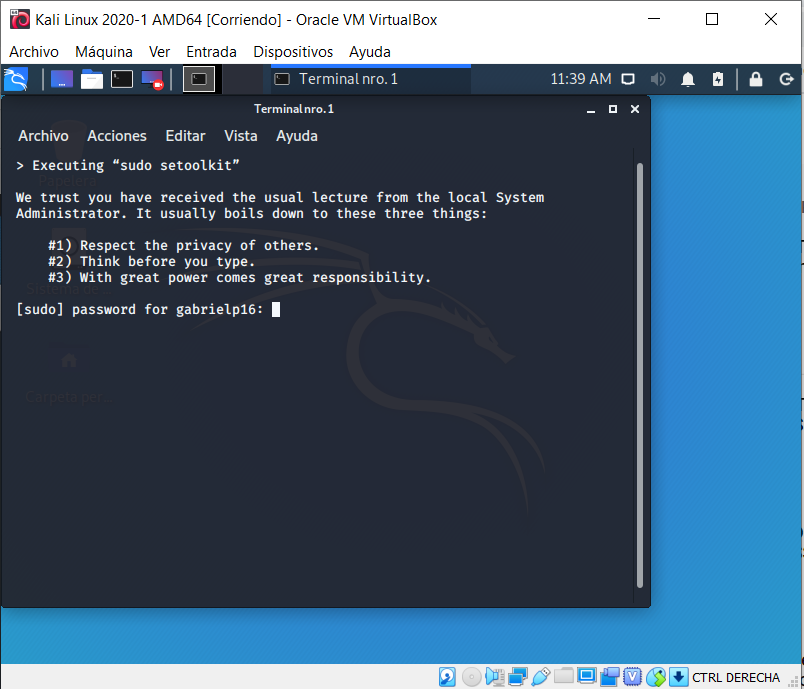
Ese es precisamente el título que llevaba un engaño descubierto por ESET en Brasil, que contenía un malware enfocado en la extracción de información personal bancaria.

**Utilización de la herramienta SET de Kali Linux**

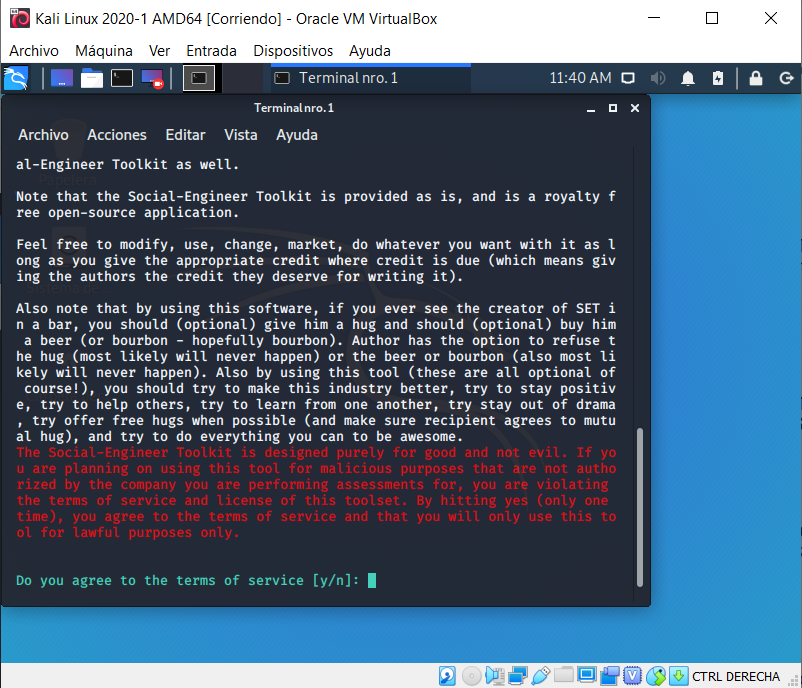
Se escoge la herramienta de explotación “Social Engineering toolkit”



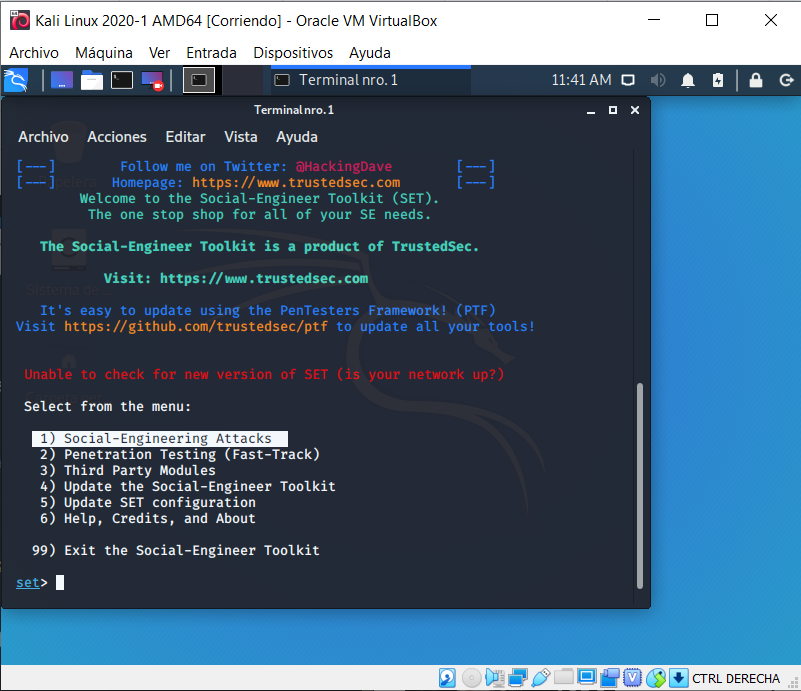
Se ingresa la contraseña del usuario para poder ingresar



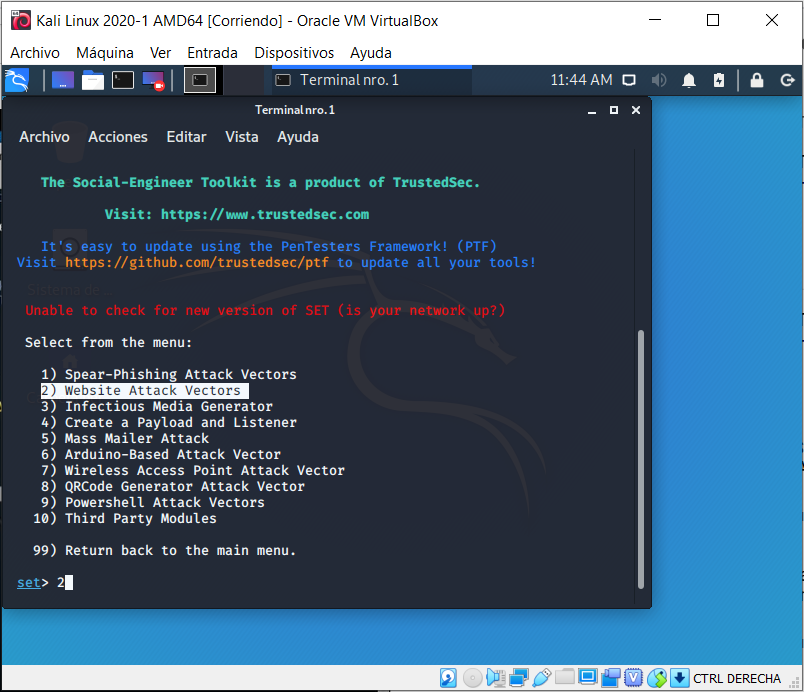
Se aceptan los términos y condiciones para la utilización de la herramienta



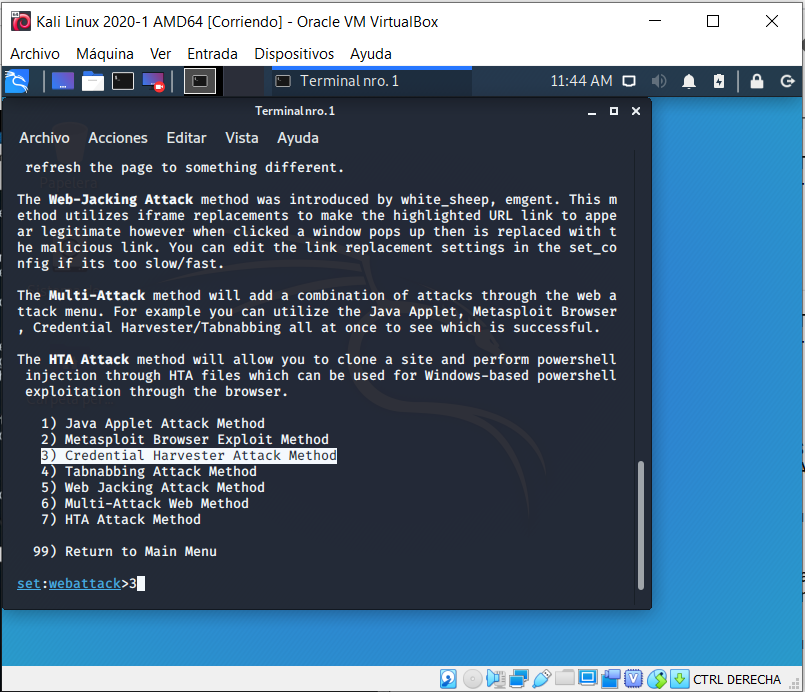
Nos aparece un menú y escogemos la opción “Ingeniería de ataque social“



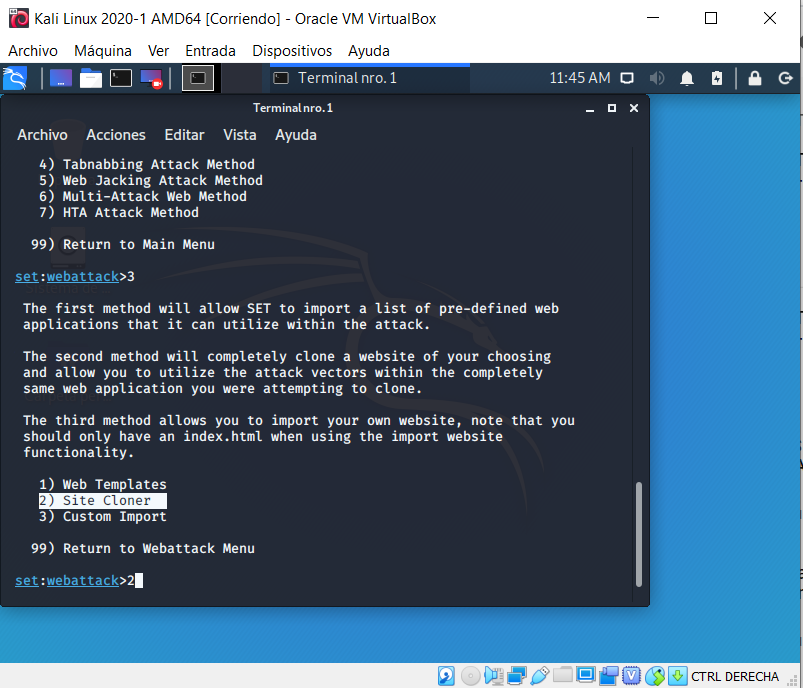
Luego escogemos “Ataque a un website”



Escogemos la opción de “Método de recolección de credenciales”



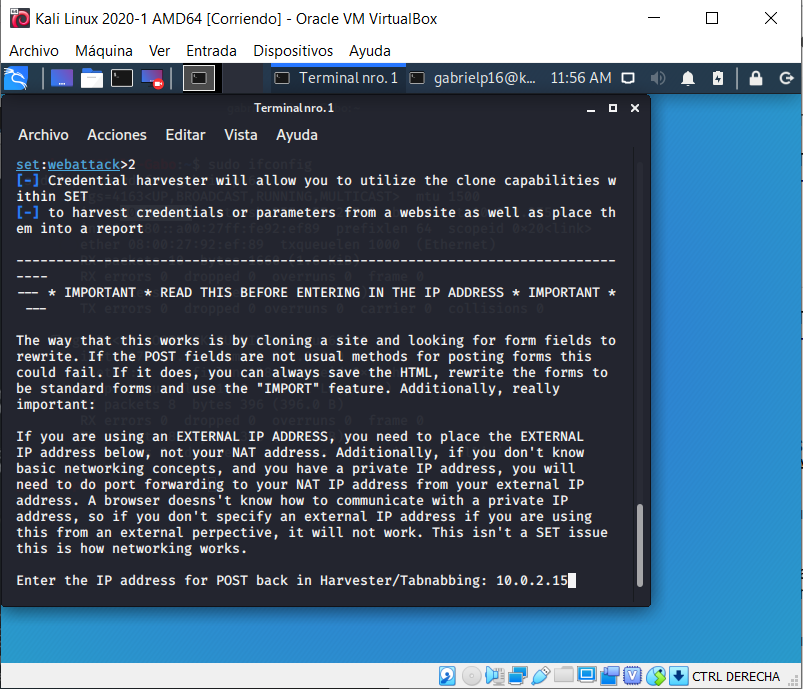
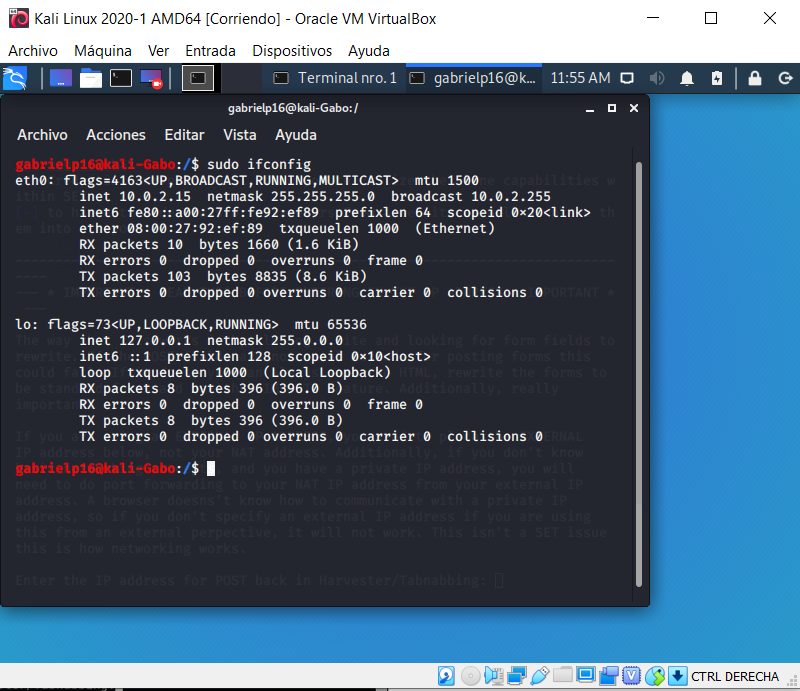
Luego escogemos la opción “Clonar sitio web”



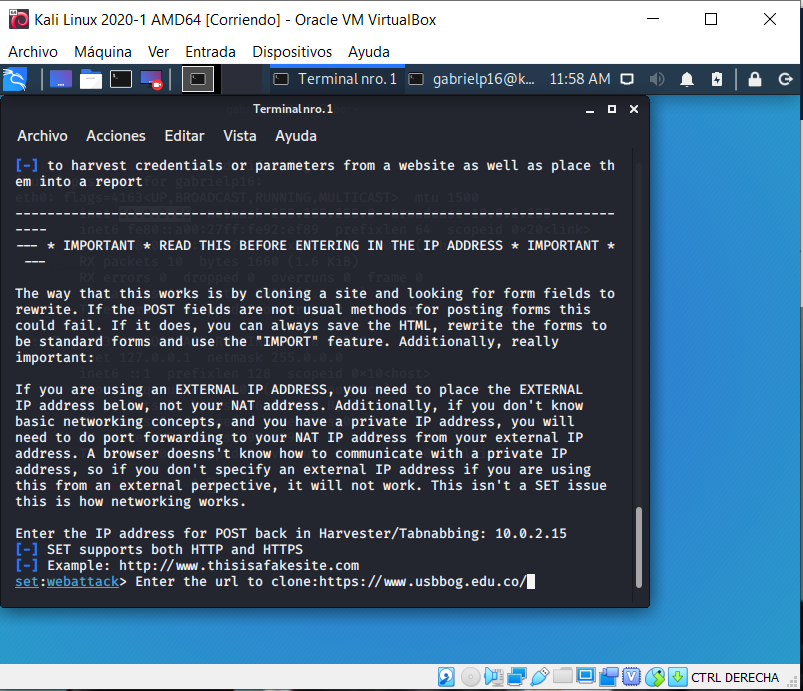
La herramienta nos solicita una dirección IP donde se alojará la información.



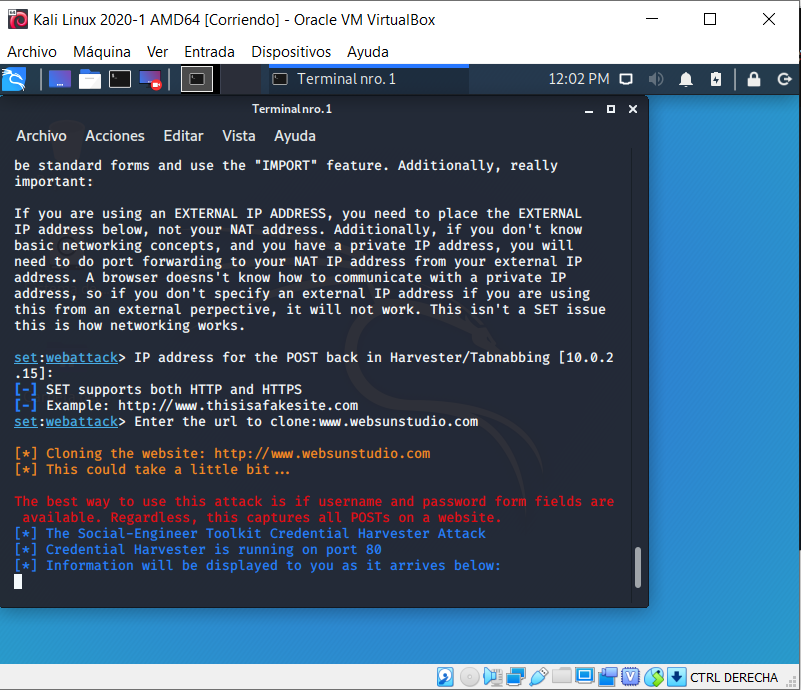
Gracias a la terminal obtenemos la dirección IP de la máquina. Luego la ingresamos la IP cuando la herramienta SET la solicita



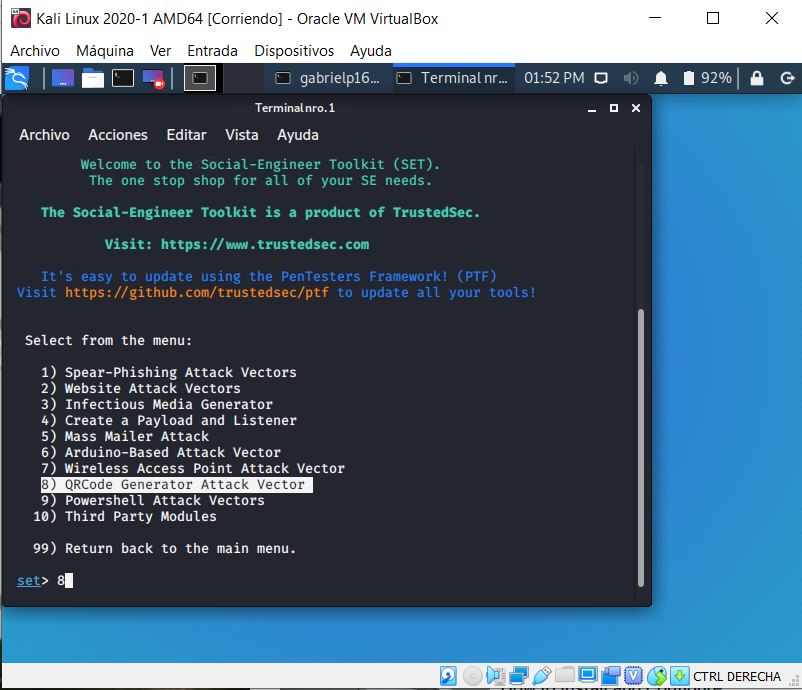
La herramienta solicita la URL del sitio a clonar, lo ingresamos y esperamos a que sea clonado el sitio



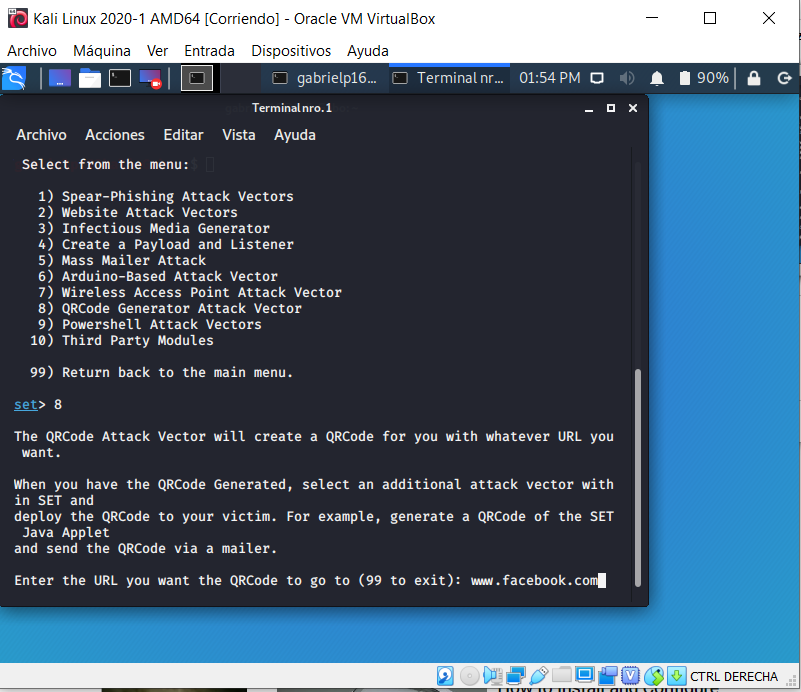
Ya tenemos el sitio clonado y el archivo .php el que nos ayudará a obtener los datos de los usuarios que ingresan.



Luego escogemos el ataque “Generar un código QR”



La herramienta nos solicita un sitio el cual se va a atacar para generar el código QR



Le herramienta nos confirma que ya se encuentra creado el archivo QR en la dirección “/root/.set/reports/qrcode\_attack.png”

