Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2020 pp. 12-19 *Correo: editor@istvidanueva.edu.ec*
Volumen 4, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2020 *Fecha de aceptación: abril 2020*

Phishing utilizando SET (Social-Engineer Toolkit) en Kali Linux

Israel Jácome [1]; Galo Diaz[2]

[1] Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, israel_jg10@hotmail.com
[2] Universidad Tecnológica Israel-Departamento de Ciencias de la Ingeniería –Carrera de Sistemas, Quito, Ecuador, gdiaz@uisrael.edu.ec

Resumen: SET (Social-Engineer Toolkit) es una suite completa de herramientas dedicadas a la ingeniería social su equivalente en español seria: kit de herramientas de ingeniería social, está especialmente diseñado para realizar ataques avanzados a la parte más vulnerable; el usuario final.
SET integra muchas de las funciones de Metasploit, por lo tanto, es necesario tenerlo instalado previamente en este caso se lo realizará en SO Kali Linux que es una distribución de Linux basado en Debian destinada a pruebas de penetración y auditoría de seguridad.
SET es multiplataforma y sólo necesitamos tener instalado el intérprete de Python para ejecutarlo e iniciarlo con ./set o Python set en la carpeta donde decidamos guardarlo.

Palabras clave: SET, Kali Linux, Python, Clonación.

Phishing using SET (Social-Engineer Toolkit) on Kali Linux

Abstract: SET (Social-Engineer Toolkit) is a complete suite of tools dedicated to social engineering, its equivalent in serious Spanish: social engineering toolkit, it is specially designed to carry out advanced attacks on the most vulnerable part; the end user.
SET integrates many of the Metasploit functions, therefore, it is necessary to have it installed previously in this case it will be done in SO Kali Linux which is a Debian-based Linux distribution intended for penetration testing and security auditing.
SET is cross-platform and we only need to have the Python interpreter installed to run it and start it with. /set or Python set in the folder where we decide to save it.

Keywords: SET, Kali Linux, Python, Cloning.

1. INTRODUCCIÓN

Decidimos usar una maquina establecida solo para uso de Kali Linux. Lo primero fue descargar Kali Linux 2020.2. Es importante mencionar también que todo el procedimiento se lo ha realizado por interfaz gráfica mediante la instalación de usb portátil para instalación de Kali Linux. Andrew, W. (2009)

Nota

Para la virtualización usamos la configuración de partición de disco al momento de la instalación.

El proceso de instalación no lo describimos pues no es el objetivo primario de este trabajo y además es bastante sencillo e intuitivo. B., G. (2020)

Luego de instalada, siempre es bueno mandar a actualizar (esto toma cierto tiempo):

```
# apt-get update     (actualiza los
repositorios)
# apt-get upgrade    (actualiza
paquetes)
```

1. Estudiante Ing. Sistemas de Información, israel_jg10@hotmail.com
2. Estudiante Ing. Sistemas de Información, gdiaz@uisrael.edu.ec

2. METODOLOGÍA

Una vez instalado, el sistema operativo Kali Linux, procedemos a visualizar la herramienta SET para ingeniería social por ahora no nos conviene que esté ejecutándose pues necesitamos realizar una serie de pruebas de funcionamiento. Dordoigne, J. (2015)

SET ya viene prácticamente listo para usarse, por lo que los pasos a continuación son bastante elementales, pero necesarios:

Primero creamos las credenciales de un usuario para pruebas debemos tener configurado el usuario root o usuario principal con el tendremos acceso a la liena de comandos:

```
#sudo su
#password
```

3. RESULTADOS Y DISCUSIÓN

3.1.Primera prueba de autenticación (local).

Abrimos la consola en el mismo equipo, iniciamos con la prueba ingresando en la línea de comandos y accediendo a SET

```
# sudo python3
/usr/share/set/settoolkit
```

Que nos indica éxito en la autenticación. Si probamos con una clave errónea como poner la "K" mayúscula en la clave no podremos ingresar al sistema ya que la clave definida para sudo es Kali

En caso de tener inconvenientes con este proceso se deberá revisar la configuración de usuario root o administrador de Kali Linux.

3.2. Notas sobre Kali Linux:

En Kali Linux, por ser una distro orientada al usuario final, los archivos y complementos no vienen de fábrica por ende toca revisar complementos y herramientas que correspondan a un correcto funcionamiento.

```
# apt-get update
```

3.3. Pruebas con la herramienta de SET

```
# sudo python3
/usr/share/set/settoolkit
```

Procedemos a ingresar contraseña Kali, nos despliega el menú que ofrece la herramienta SET de Kali Linux.

En este caso como vamos a trabajar con Ingeniería Social con ataques y clonación de páginas web ingresamos el literal 1). DragonJAR. (2012)

```
# set> 1
```

Paso siguiente nos despliega el submenú en el cual escogemos la opción 2). Website Attack Vectors

```
# set> 2
```

Nos listara los tipos de ataques que deseamos realizar consiguiente ingresamos la opción 3). Credential Harvester Attack Method.

```
# set> 3
```

Seguido incluiremos el tema tratado de site cloner la opción 2).Site Cloner

```
# set> 2
```

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2020 pp. 12-19 *Correo: editor@istvidanueva.edu.ec*
Volumen 4, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2020 *Fecha de aceptación: abril 2020*

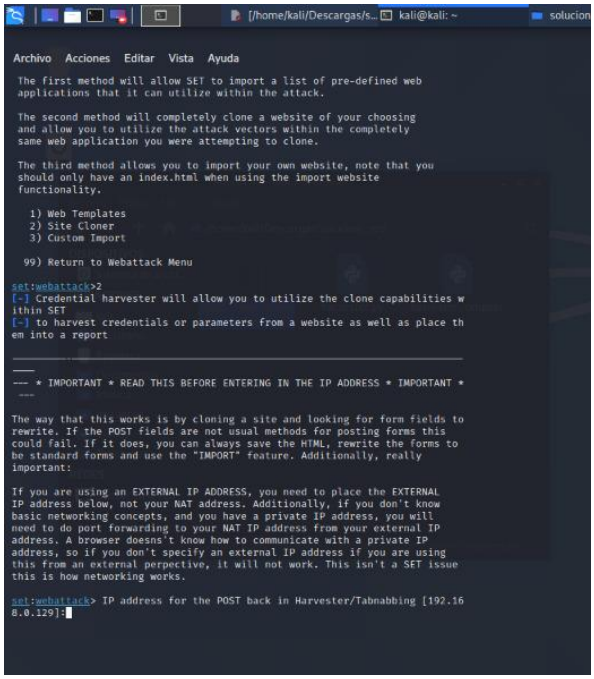

Ilustración 1. Implementación SET.
Fuente: (Linux, 2018)

Luego de ingresar los datos en cada menú se nos desplego la imagen anterior.

La primera prueba la realizamos con una red local, donde seleccionamos conectar la red y obtuvimos la ventana de solicitud de detalles de autenticación para esta conexión:

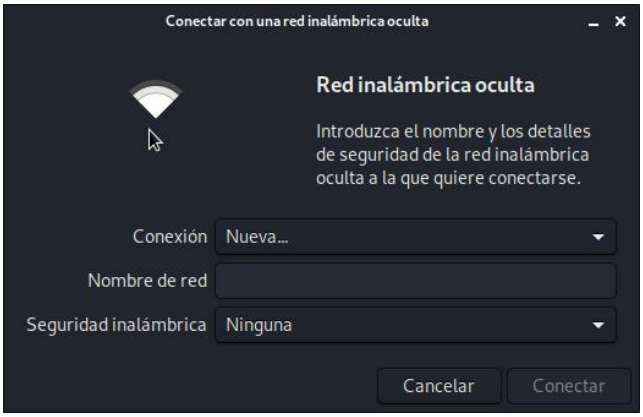

Ilustración 2: Wifi Network
Fuente: (Linux, 2018)

Luego de llenar el usuario, la clave (el cual debe coincidir con un usuario y clave definido, obtenemos la dirección ip donde se clonará la página web.

Ingresamos la ip definida y nos solicita ingresar un enlace a una pagina web en este caso la que deseamos clonar.

Ilustración 3: Enlace Página web.
Fuente: (Linux, 2018)

Surgieron ciertos errores al momento de obtener las credenciales y la clonación por ende culminamos la segunda prueba con la herramienta SET y pasamos a configuración de archivos de SET.

3.4. Configuración Ficheros.

Vimos que entre los paquetes que se actualizarán, falto configurar el archivo harvester.py para utilizar por SET de ingeniería social así que procedimos a configurarlo ingresando los comandos para agregar el complemento.

```
#usr/share/set/src/webattack/harvester
/harvester.py
```

el siguiente paso debemos modificar este archivo ingresando con cualquier editor de texto, es importante destacar que debemos ingresar como usuario administrador o usuario root.

Pues bien, comenzamos en KaliLinux con la modificación del archivo Python.

Lo principal de modificar en este archivo son dos acciones importantes la primera es importar librería html, la segunda es cambiar en la línea 75 de código en lugar de cgi incluir html con esto el archivo estará listo.

Ilustración 4: Configuración
Fuente: (Linux, 2018)

Cuando este configurado el archivo ya podremos ingresar a la herramienta SET, sin embargo, es recomendable reiniciar el servicio de Kali Linux porque estamos modificando a nivel de root.

Si la configuración resulto complicado existe el código del archivo en internet accediendo a el de manera fácil lo recomendable seria borrar el archivo existente y reemplazarlo con el archivo descargado modificado, a nuestra forma de reemplazar es mucho más fácil por CLI, entonces se mostrará los comandos utilizados. Romero, J. G. (2019)

Tomar en cuenta que el archivo solo podrá ser modificado con el usuario root o administrador.

```
Sudo rm
usr/share/set/src/webattack/harvester
/harvester.py (elimina)

Sudo cp
usr/share/set/src/webattack/harvester
/  (copia archivo)
```

Con esta configuración ya realizada podremos continuar con el reinicio del sistema Kali Linux

Finalizamos la configuración de ficheros para ya realizar la prueba definitiva del proceso de SET.

3.5. SET ENGINEERING TOOLKIT:

Como lo habíamos propuesto antes, una de las ventajas de usar SET es que nos permite automatizar tareas que van desde el de envío de SMS (mensajes de texto) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, a clonar cualquier página web y poner en marcha un servidor para hacer phishing en cuestión de segundos. (Vaca, 2012) El kit de herramientas SET está especialmente diseñado para realizar ataques avanzados contra el elemento humano.

Una vez instalado todo y agregado todos los ficheros de configuración de set, entramos a la parte de desarrollo de verificación de vulnerabilidades de clonación de páginas web con SET:

Primer paso para realizar la configuración es ingresar a la herramienta SET de Kali Linux, podemos ingresar de dos maneras ya sea por línea de comandos (CLI) o por entorno gráfico.

Se mostrará las dos formas de ingresar a SET.

Primera forma (CLI)

```
# sudo python3/usr/share/set/settoolkit
```

Esta forma nos permita acceder por una terminal de Kali Linux de manera rápida accediendo por los directorios, es importante destacar que es complicado conocer las rutas si no se conoce acerca de directorios.

Segunda forma (Interfaz Gráfica)

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2020 pp. 12-19 *Correo: editor@istvidanueva.edu.ec*
Volumen 4, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2020 *Fecha de aceptación: abril 2020*

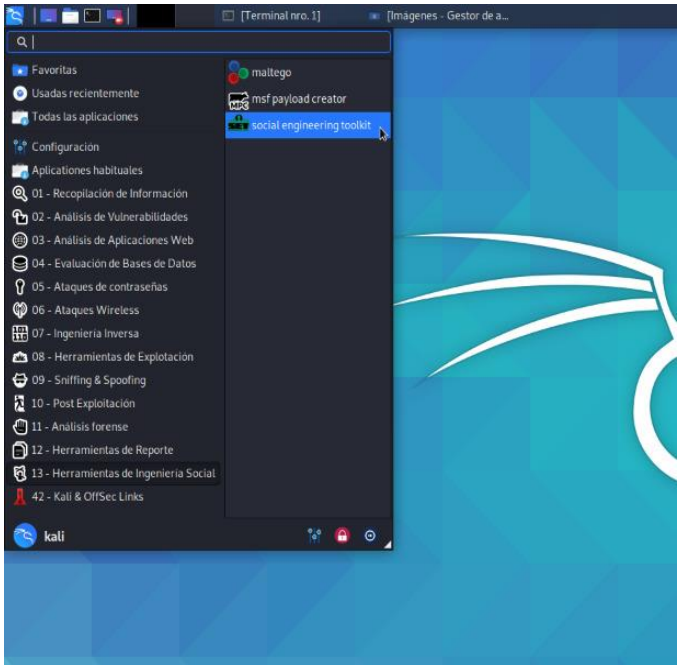

Ilustración 5: Interfaz
Fuente: (Linux, 2018)

Ya ingresando a la herramienta SET nos mostrara una ventana en la cual ingresamos con las credenciales de nuestro usuario root o administrador.

Procedemos con los datos de login. Pws:kali

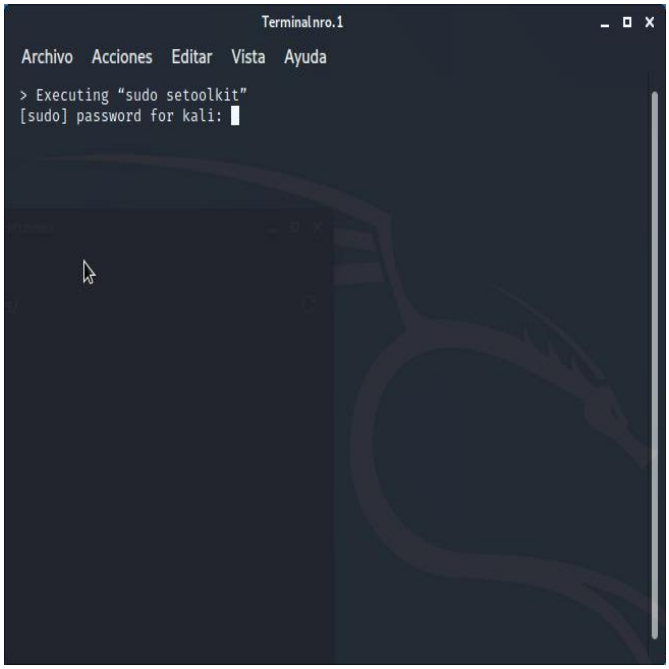

Ilustración 6: Credenciales
Fuente: (Linux, 2018)

Entramos a la interfaz de la herramienta de SET, una vez dentro escogemos la opción de ingeniería social en ingles Social-Engineering Attaks

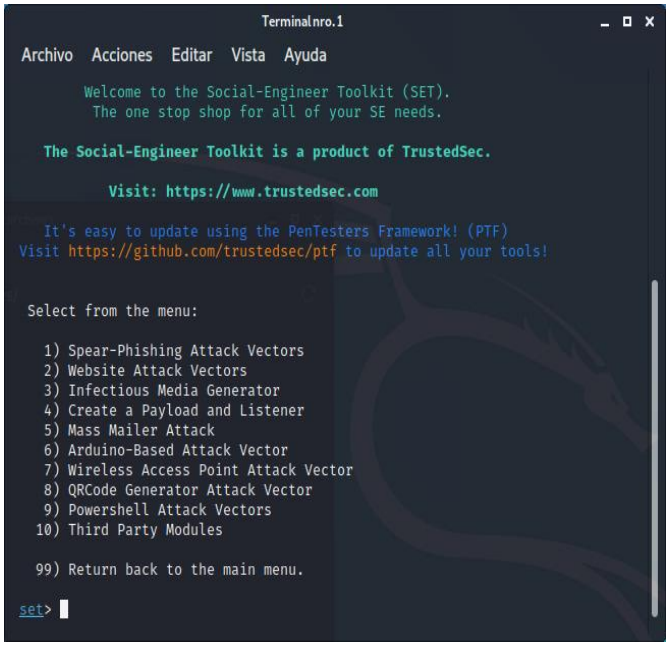

Ilustración 7: Ingeniería Social
Fuente: (Linux, 2018)

En este submenú escogemos la opción metodo de ataque de credenciales en ingles Credential Harvester Attack Method.

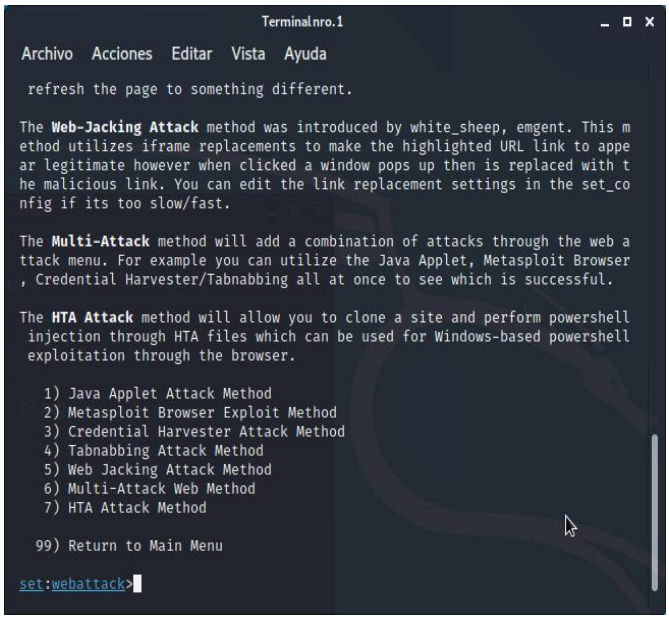

Ilustración 8: Menú 1
Fuente: (Linux, 2018)

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2020 pp. 12-19 *Correo: editor@istvidanueva.edu.ec*
Volumen 4, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2020 *Fecha de aceptación: abril 2020*

Nos despliega los métodos que tiene este ataque escogemos la opción tratada en el tema que es la clonación de sitios web ingresamos el numeral 2) Site Cloner:

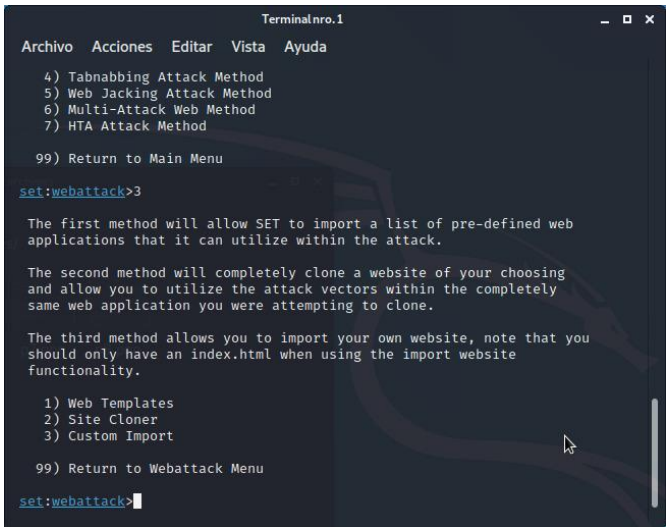

Ilustración 9: Menú 2
Fuente: (Linux, 2018)

Seguido de estos pasos ya nos encontramos en la interfaz de requerimientos nos solicita ingresar la dirección IP en la que nos encontramos esto es ya que es una página web necesitamos un dominio para mostrar la clonación web

Aclaremos lo que es una red IP. La dirección IP es un conjunto de números que identifica, de manera lógica y jerárquica, a una Interfaz en la red de un dispositivo que utilice el protocolo TCP/IP. (Dordoigne, 2015)

Para saber cuál es nuestra dirección de red en el sistema Kali Linux es de la siguiente forma ingresamos a una terminal de comando (CLI) y ejecutamos el siguiente comando.

```
# ifconfig
```

En este comando nos permite configurar o desplegar numerosos parámetros de las interfaces de red residentes en el núcleo, como la dirección IP (Linux, 2002).

Nota: la dirección IP es la que se encuentra con el nombre de Wlan0.

Seguido de este comando y conociendo nuestra dirección IP pasamos a la herramienta SET para ingresar la red.

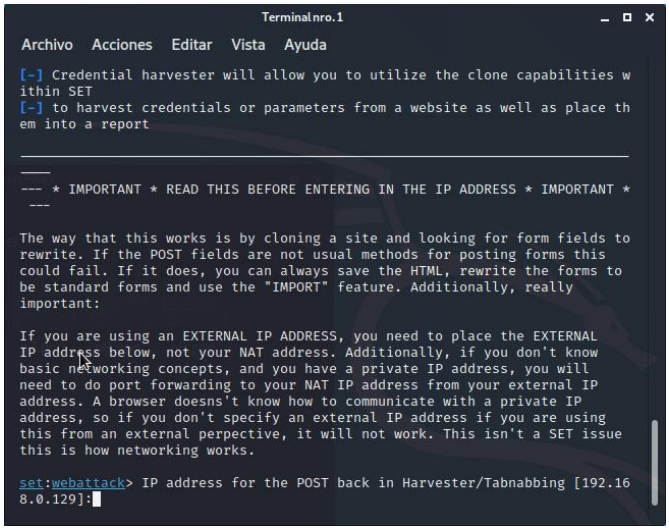

Ilustración 10: Configuración Red
Fuente: (Linux, 2018)

Después de ingresar la red nos solita el ingreso de un enlace web del sitio que deseamos clonar. En este aspecto hay que tener las debidas precauciones en cuanto al sitio que se escoge para clonar ya que poseen sus permisos y actividades legales.

Es necesario solicitar el permiso al entidad o persona necesaria para esta actividad ya que es algo que puede vulnerar la entrada a su dominio.

Acerca de que es un dominio, es un nombre único que identifica a una subárea de Internet. es traducir las direcciones IP de cada activo en la red, a términos memorizables y fáciles de encontrar. (B., 2020)

Es este caso utilizamos el dominio de la plataforma de la Universidad Tecnológica Israel con sus debidos permisos otorgado por el administrador de Red de la Universidad con el fin de solo y estrictamente fines educativos. Lucia, P. G. (2018)

Ingresado el dominio de www. Solicitado
La herramienta SET se encarga de clonar la pagina web en su red IP.

Revista Nexos Científicos *ISSN: 2773-7489*
Enero –Junio 2020 pp. 12-19 *Correo: editor@istvidanueva.edu.ec*
Volumen 4, Número 1 *URL: http://nexoscientificos.vidanueva.edu.ec/index.php/ojs/index*
Fecha de recepción: febrero 2020 *Fecha de aceptación: abril 2020*

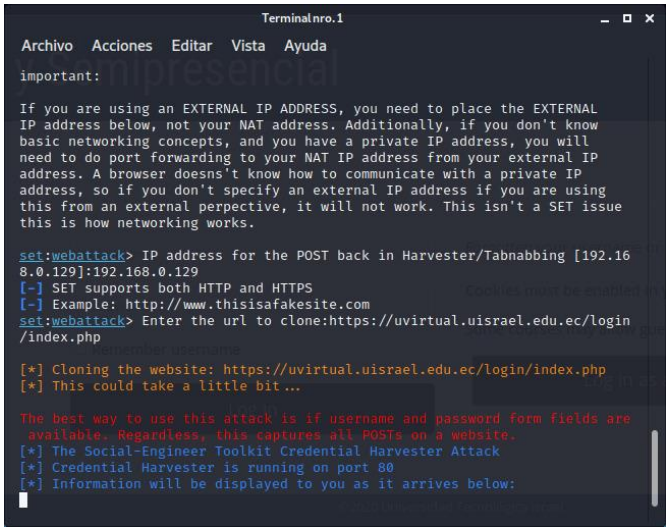

Ilustración 11: Clonación
Fuente: *(Linux, 2018)*

Esta en la ventana abierto desde un navegador con la dirección de red de nuestro dominio. Como se observa en la imagen la interfaz gráfica es similar por ende para un usuario es muy complicado identificar a vista rápida cual es y cual no.

Es importante conocer que al entrar en un dominio visualizar si es un sitio seguro no entraremos a más detalles de cómo saber un sitio seguro ya que este no es el objetivo del tema. W, X., & H, J. (2014)

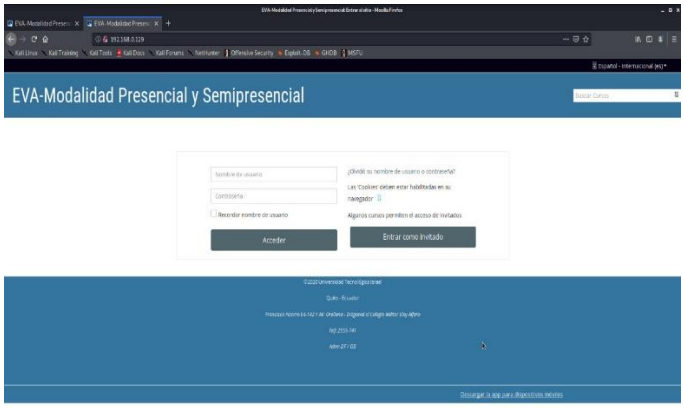

Ilustración 12: Interfaz Clonada
Fuente: *(Linux, 2018)*

Ya con el sitio clonado, SET solo espera a las acciones ingresadas por la victima de esta clonación al ingresar su usuario y contraseña la información estará ingresando a nuestro dominio mas no al propio de la Universidad Tecnológica Israel en el cual SET nos muestra el usuario y contraseña que ingreso con esto ya tenemos las credenciales de una persona.

Nota: Tomar en cuenta que esta es una acción ilícita y que tiene como consecuencias una penalización económica y legal sobre la persona que lo realiza. Es importante conocer que esto se realiza con el fin de una auditoria o con el fin estrictamente educativo. Vaca, M. (2012)

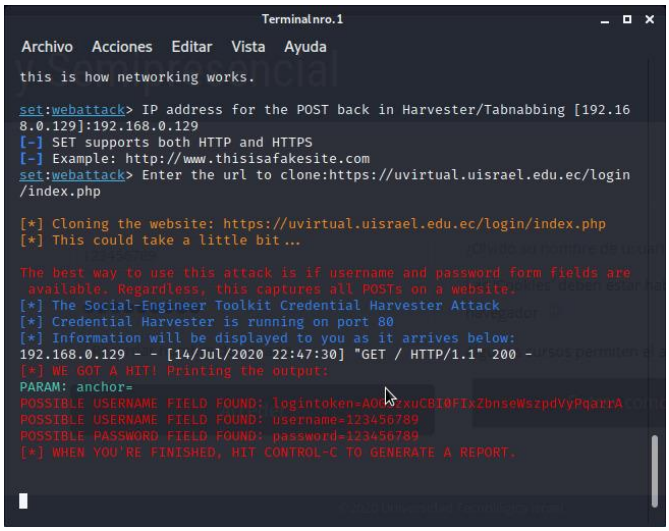

Ilustración 13: Resultado Credenciales
Fuente: *(Linux, 2018)*

Al ingresar el comando exit saldremos de SET y el sitio clonado ya desaparece.

4. CONCLUSIONES

- La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos del sistema, con el único objetivo de obtener información, acceso al sistema e incluso privilegios elevados en dicho sistema.

- La ingeniería social convierte al usuario de una tecnología en el objetivo, en la potencial víctima. Es así como el usuario pasa a ser el eslabón más débil de la ciberseguridad en cualquier situación.

- La ingeniería social en muchos casos está relacionada con ciberdelincuentes, pero estas

técnicas también son utilizadas por investigadores de seguridad para comprobar la seguridad de una determinada empresa

- Set es una herramienta poderosa que junto a Metasploit logra hacer ataques de ingeniería social, para ejecutarla no se necesita el mayor conocimiento sobre seguridad.

- El elemento que permite ataques de Ingeniería Social y una serie de problemáticas que se encierran dentro del conocimiento y desconocimiento sobre el tema es sin duda alguna, el factor humano, ya que es parte esencial y primordial de la seguridad.

- No existe ningún sistema informático que no dependa de algún dato ingresado por un usuario. Por esta razón se convierte en una debilidad de seguridad universal, independientemente de plataformas, software, red, equipo y la edad de la persona que sea afectada.

- La falta de conocimiento y capacitación sobre las distintas técnicas y maneras de ser atacados con el uso de la Ingeniería Social es lo que hace vulnerable a cualquier usuario.

- La disrupción de los avances tecnológicos también ha facilitado diferentes técnicas y ha creado de nuevas, los dispositivos móviles con cámaras más potentes, buenas grabadoras o los dispositivos GPS son algunos ejemplos de ello.

- SET permite realizar ataques automáticos a un usuario que ingrese (por medio de ingeniería social) a una dirección que se le especifique.

- La ingeniería social es una de las puertas de acceso más utilizadas por los delincuentes, para robar la información personal o infiltrarse en una empresa.

REFERENCIAS

Andrew, W. (11 de 06 de 2009). *informit.com.* Obtenido de https://www.informit.com/articles/article.aspx?p=1350956&seqNum=11

B., G. (28 de 04 de 2020). *Hostinger*. Obtenido de Hostinger: https://www.hostinger.es/tutoriales/que-es-un-dominio-web

Dordoigne, J. (2015). *Redes informáticas-Nociones fundamentales.* Ediciones Eni.

DragonJAR. (05 de 2012). *dragonjar.org.* Obtenido de https://www.dragonjar.org/the-social-engineer-toolkit.xhtml

Linux. (2002). *Trasparencias del Curso de IPv6.* GDU.

Linux, K. (2018). *Penetration testing and ethical hacking linux distribution.*

Lucia, P. G. (08 de 2018). *repository.uniminuto.edu.* Obtenido de https://repository.uniminuto.edu/bitstream/handle/10656/1091/TR_PedrazaGarzonCarmenLucia_2011.pdf?sequence=1&isAllowed=y

Romero, J. G. (01 de 2019). *openaccess.uoc.edu.* Obtenido de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89045/6/joanenricgarciaromeroTFM0119memoria.pdf

Vaca, M. (12 de 10 de 2012). *SET*. Obtenido de SET: https://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html

W, X., & H, J. (2014). Traffic Simulation Modeling and Analysis of BRT Based on Vissim. *Intelligent Computation Technology and Automation (ICICTA), 2014 7th International Conference* (págs. 879-882). IEEE.