The Social-Engineer Toolkit (SET)

Created by: David Kennedy (ReL1K)

 Versión: 8.0.1

 Bueno en esta ocasión vamos a realizar un ataque de ingeniería social, a sitios que contengan como inicio de sección un login, por ejemplo un nombre y una contraseña, o un correo y una contraseña.

 Para este ataque vamos a utilizar la herramienta setoolkit, la cual trae un arsenal de herramientas destinadas para la ingeniería social.

 En el primer ataque vamos a usar una de las máquinas virtuales que descargamos anteriormente, como víctima la cual será la OWASPBROKEN.

 Para este ataque vamos a iniciar la herramienta llamándola desde el menú de aplicaciones, o como a mí me gusta desde la consola. Con el comando SETOOLKIT

 Una vez abierta la herramienta, vemos un par de opciones la cuales vamos a ver en detalle alguna de ellas.

La primera que vamos a usar va a ser la numero 4 para que todos trabajemos con la misma versión.

 4) Update the Social-Engineer Toolkit

Esta opción lo que nos hace es actualizar a la última versión lanzada por los creadores de la misma.

La segunda opción que vamos a usar es la numero uno.

 1) Social-Engineering Attacks

Esta opción nos abre un apartado con más opciones, la cual se realizan ATAQUES DE INGENIERIA SOCIAL.

La segunda opción que vamos a usar es la numero dos

 2) Website Attack Vectors

Esta opción es la que realiza lo ataques web.

La cuarta opción que vamos a utilizar es la 3.

 3) Credential Harvester Attack Method

Esta opción va a cosechar o recolectar las credenciales del ataque que realizaremos.

Y la quinta opción es la numero 2.

 2) Site Cloner

Esta opción tiene la finalidad de clonar sitios ustedes en lo posible tienen que clonar sitios que contengan login, o en su defecto que usen credenciales de acceso.

Nosotros vamos a utilizar como víctima la máquina virtual que les brinde en clases anteriores. Owaspbroken.

Una vez seleccionada la última opción nos va a pedir que ingresemos la ip nuestra. En mi caso la ip es la 192.168.52.128

Importante este ataque se realiza dentro del rango de nuestra red ósea que es un ataque local.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.52.128]:192.168.52.128

Al darle enter nos pide que ingresemos la dirección que vamos a clonar. En nuestro caso a a ser la dirección de login de la web de la owasp.

Acá nos muestra que el sitio está siendo clonado con satisfacción.

[\*] Cloning the website: http://192.168.52.188/bWAPP/login.php

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

Esto otro nos indica que la mejor forma de usar este ataque es que el enlace contenga un formulario de login de usuario y contraseña. De todos modos, esto captura todos los POST en un sitio web.

The best way to use this attack is if username and password form

fields are available. Regardless, this captures all POSTs on a website.

Es posible que deba copiar / var / www / \* en / var / www / html dependiendo de dónde se encuentre la estructura de su directorio.

Presione {return} si entiende lo que estamos diciendo aquí.

You may need to copy /var/www/\* into /var/www/html depending on where your directory structure is.

Press {return} if you understand what we're saying here.

El ataque del creador de credenciales del kit de herramientas del ingeniero social

[\*] Credential Harvester se está ejecutando en el puerto 80

[\*] La información se te mostrará cuando llegue a continuación

[\*] The Social-Engineer Toolkit Credential Harvester Attack

[\*] Credential Harvester is running on port 80

[\*] Information will be displayed to you as it arrives below:

A continuación vamos a nuestra víctima y le enviamos la ip para que pueda ejecutar las credenciales para acceder.

yyyy guala ya tenemos las credenciales......

192.168.52.128 - - [03/Nov/2019 03:38:27] "GET / HTTP/1.1" 200 -

[\*] WE GOT A HIT! Printing te output:

POSSIBLE USERNAME FIELD FOUND: login=bee

POSSIBLE PASSWORD FIELD FOUND: password=bug

PARAM: security\_level=0

PARAM: form=submit

[\*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

Lo mejor de todo es que la víctima tiene acceso por completo a su sitio web sin ningún cambio inclusive hasta se cambia la dirección a la que corresponde.