Ingeniería Social. SET -> Social Engineering Toolkit

Bien, vamos a explicar como se hace un ataque de phishing usando un correo electrónico fraudulento. Y ¿Qué es esto del phishing?, pues es una técnica de ingeniería social mediante la cual hacemos creer a la víctima mediante un correo o una web manipulada que somos quien realmente no somos con el objeto habitual de que nos den ellos mismos sus contraseñas para acceder a sus cuentas bancarias, o bien sus contraseñas para acceder a sus correos electrónicos y redes sociales y así poder victimizarlo y manipularlo posteriormente con otros fines.

El planteamiento del ataque será el siguiente.

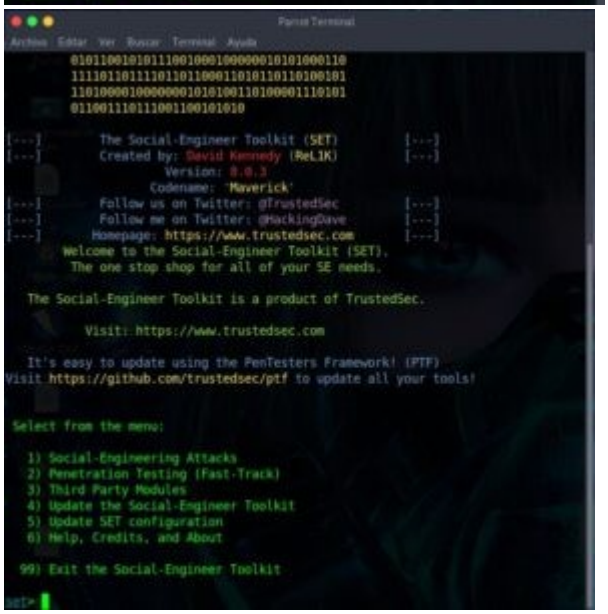
1. selecciono la víctima de la cual conozco su correo electrónico, y a la cual me dirigiré vía email con la intención de que pique el anzuelo.
2. enviaré un email fraudulento al correo de la víctima. Este será el email de ataque.
3. clonaré la web legítima de www.gmail.com de tal forma que, cuando la víctima abra el correo fraudulento que le he enviado desde el email de ataque, ella verá que es gmail quien le escribe y le pide pinchar en un enlace.
4. con la excusa de un nuevo servicio o la prevención de un fraude, se le pide a la víctima que entre en su gestor de correo de email (la web clonada de gmail.com) para hacer una pequeña comprobación.
5. En la web clonada la víctima introducirá su usuario y contraseña que nos aparecerá en la consola de nuestra máquina de ataque linux parrot y así ya habremos obtenido lo que queremos de la víctima,
6. Lo que suceda posteriormente es indiferente. Se le dirige a la web legítima, se le muestra una página de error, etc, pero que no sospeche.

Este es un ataque de ingeniería social. Si sustituyen las palabras "ingeniería social" por "engañar a la víctima como a un chino" tendrán un significado mas preciso de lo que queremos decir.

Como habéis visto necesitamos varias cosas: generar el email fraudulento y clonar la web anzuelo entre otras cosas. Esto no es fácil hacerlo, pero en nuestro laboratorio de hacking, y en concreto en la máquina linux parrot, aunque también está en la máquina kali, disponemos de una herramienta que se encarga de automatizar este proceso.

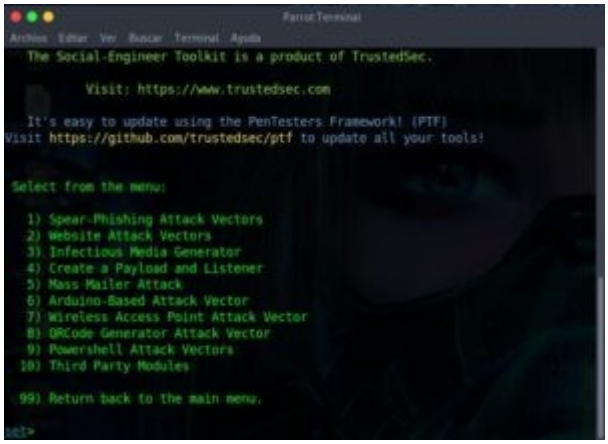
Esta herramienta se llama Social Engineer Toolkit o SET. Entramos en nuestra máquina parrot y nos vamos al menú:

Arrancamos la herramienta SET:



En primer lugar clonamos la web de gmail. Para ello, desde el menú principal de SET, pulsamos:

1.social engineering attack



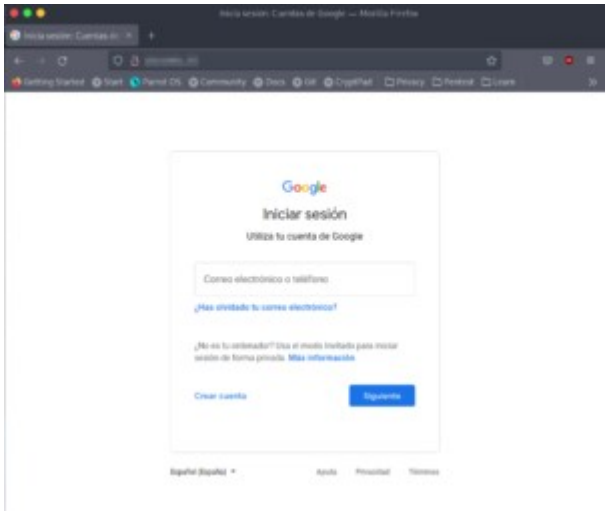
luego pulsamos 2, website attack vectors

Luego pulsamos 3, credential harvester attack method

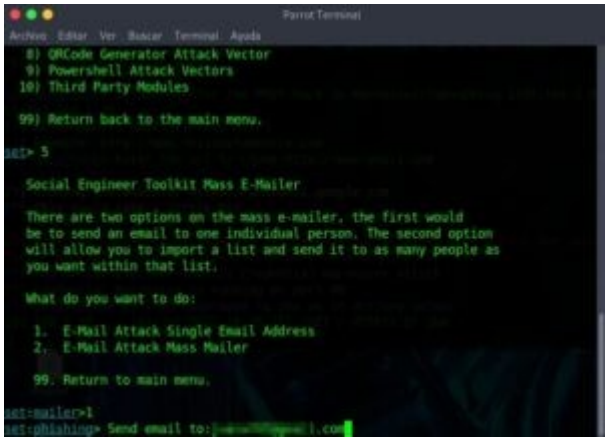
Luego pulsamos 2, site cloner:

A continuación se nos pedirá la dirección IP de nuestra máquina atacante linux parrot. Yo la he pixelado por motivos de seguridad. Vosotros deberéis meter la dirección IP de vuestra máquina de ataque, máquina en la que recibiréis el usuario y la contraseña de la víctima en el momento en que muerda el anzuelo con el correo. Después de meter la IP, hay que introducir el sitio web que vamos a clonar. Como hemos dicho al principio, este será www.gmail.com. El SET ejecuta el site clonado en la dirección <IP de ataque>:80 es decir que si navegamos desde firefox a nuestra IP en el puerto 80 veremos el site clonado fraudulento donde el usuario introducirá

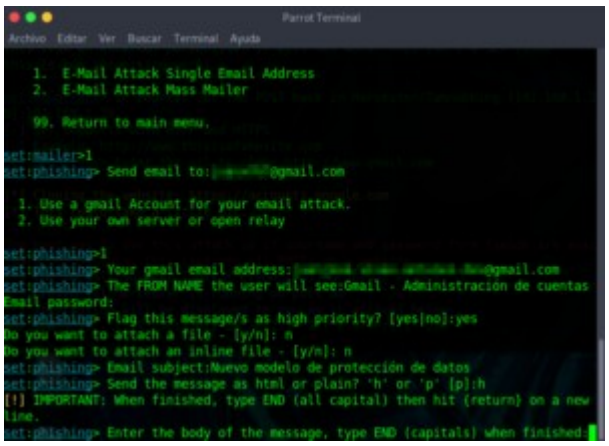
su usuario y contraseña. Dicho site tiene un lector de claves y los valores que introduzca la víctima saldrán en la misma consola de linux donde acabamos de clonarlo (ver última imagen), tal y como pone la última frase:
"information will be displayed to yoa as it arrives below:"
pues justo debajo empezará a displayarse los echos de la actividad de SET, así que ese terminal ha de estar abierto.
Así pues, abrimos firefox en nuestra máquina linux parrot y navegamos a nuestra IP de ataque y veremos el site fraudulento:



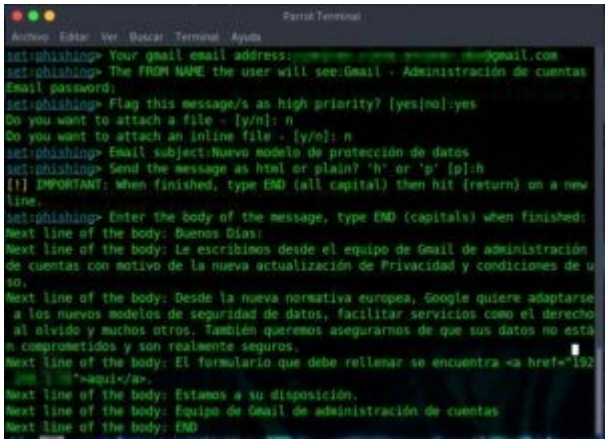
Ya tenemos montada la primera parte de nuestro ataque. Ahora vamos con el tema de los correos. Ojo, este asunto practicarlo en vuestro laboratorio y con vuestros correos electrónicos. No se os ocurra hacerlo por ahí que podéis oler barrotes.
En primer lugar el correo que vamos a enviar a la víctima:



En segundo lugar, montamos el correo desde el que vamos a engañar a la víctima:



Continuamos redactando y finalizamos el correo:



Cuando pulsamos END, se habrá generado el correo electrónico y se habrá enviado al buzón de la víctima. Si la víctima pica en el anzuelo, en cuanto entre en la web fraudulenta, nos parecerá el usuario y la clave.