**Dibujo de una persona

Descripción generada automáticamente con confianza baja**

***Ciberataques***



**Achraf El mahjouby Sourour**

ÍNDICE

Contenido

[**Introducción** 3](#_Toc183693106)

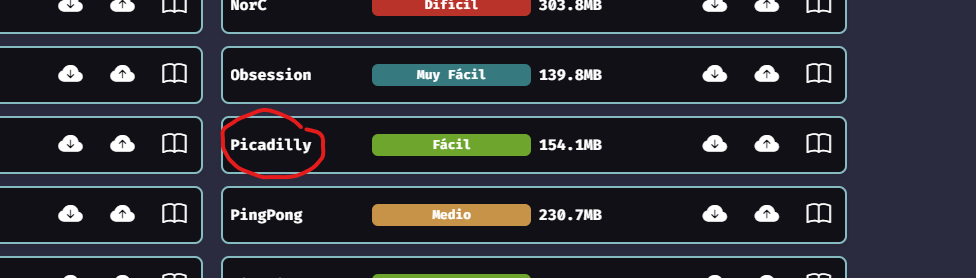
[**Escaneo del puerto 80** 7](#_Toc183693107)

[**Escaneo del puerto 443** 9](#_Toc183693108)

# **Introducción**

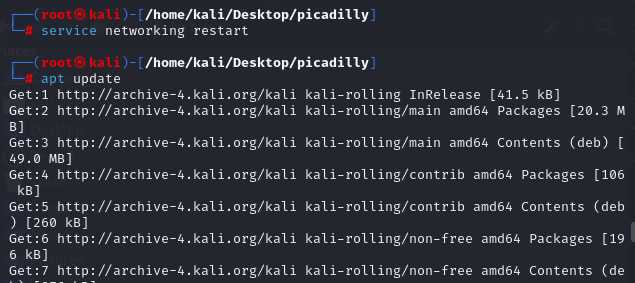
En la siguiente práctica, haremos un ejercicio para saber cómo hacer un ataque a maquinas preparadas para ser atacadas con el Dockerlabs.

En mi caso una vez ingresado en la página web de dockerlabs, me he decantado por esta máquina llamada picadilly.

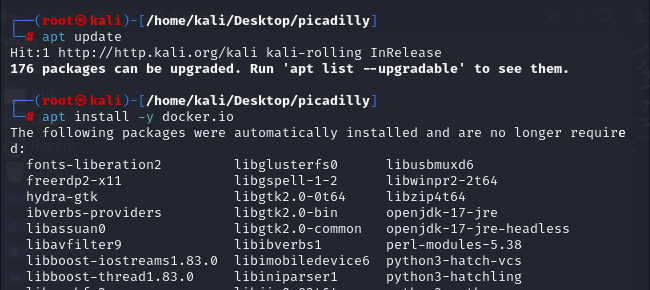


Lo que tenemos que hacer es descargarnos su script ejecutable para poder trabajar con la maquina dentro de la nuestra de Kali para ello he compartido una carpeta de la maquina real a la de Kali ara poder ver el archivo.zip

Una vez dentro de la máquina virtual de Kali y extraídos los archivos de pidadilly.zip lo siguiente que he hecho es actualizar todos los paquetes.



Una vez actualizados podíamos instalar Docker ya que es una herramienta que "empaqueta" una aplicación con todo lo necesario para que funcione igual en cualquier PC o servidor. Es como una caja portátil que garantiza que no falten componentes y que siempre corra sin problemas.



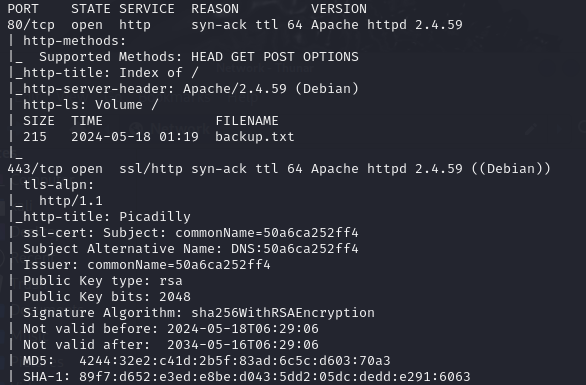
Todo esto lo tenemos que hacer con el usuario root, como podemos observar en la siguiente imagen ya estaríamos dentro de la máquina de picadilly y nos ha dado su dirección IP



Lo primero que hacemos es un escaneo con nmap para comprobar las vulnerabilidades en los puertos que estén abiertos, nos muestra información sobre ellos, y lo hacemos con el siguiente comando.

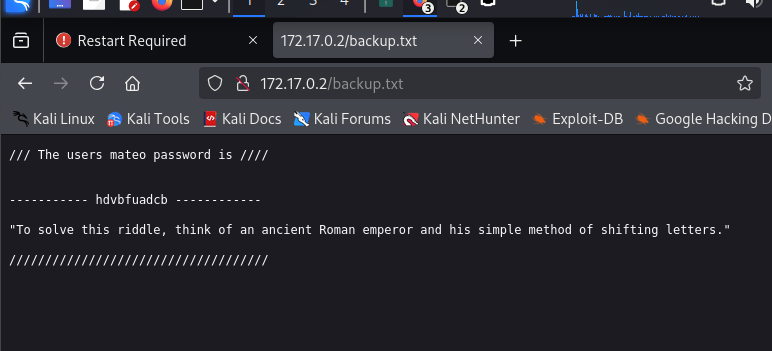


Una vez realizado nos ha sacado que tenemos 2 puertos abiertos el puerto 80 y el 443.



## **Escaneo del puerto 80**

Vamos a comenzar con el escaneo del puerto 80 y ver la información que nos proporciona, en ese puerto como podemos comprobar tenemos un archivo.txt llamado backup.txt y para saber que es lo que contiene en el navegador ponemos lo siguiente, pero sin cerrar el nmap 172.17.0.2/backup.txt y nos ha devuelto lo siguiente.



Nada mas entrar ya nos dice un nombre de usuarios en este caso es “mateo” y su contraseña es la que vemos de la siguiente manera -------(PASSWORD)------- debajo podemos leer que es un acertijo y podemos observar que parece un mensaje encriptado, por lo que vamos a desencriptarlo.

Para poder desencriptarlo entramos a esta pagina web que nos ayuda a hacerlo <https://www.dcode.fr/identificador-cifrado>.

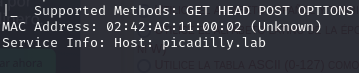
Copiamos y pegamos la contraseña y cómo podemos observar arriba a la derecha nos da una pista de lo que podría ser “easycrazy”.



Como ya sabemos el usuario y la contraseña de mateo necesitamos hacer un proceso de investigación del puerto 443.

## **Escaneo del puerto 443**

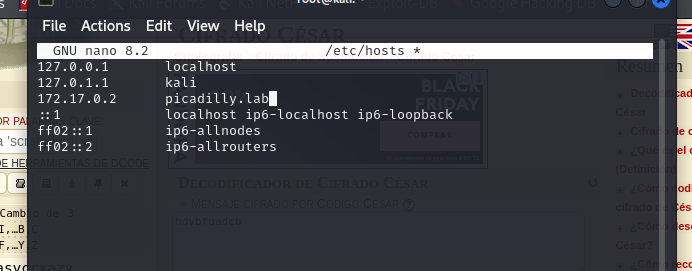




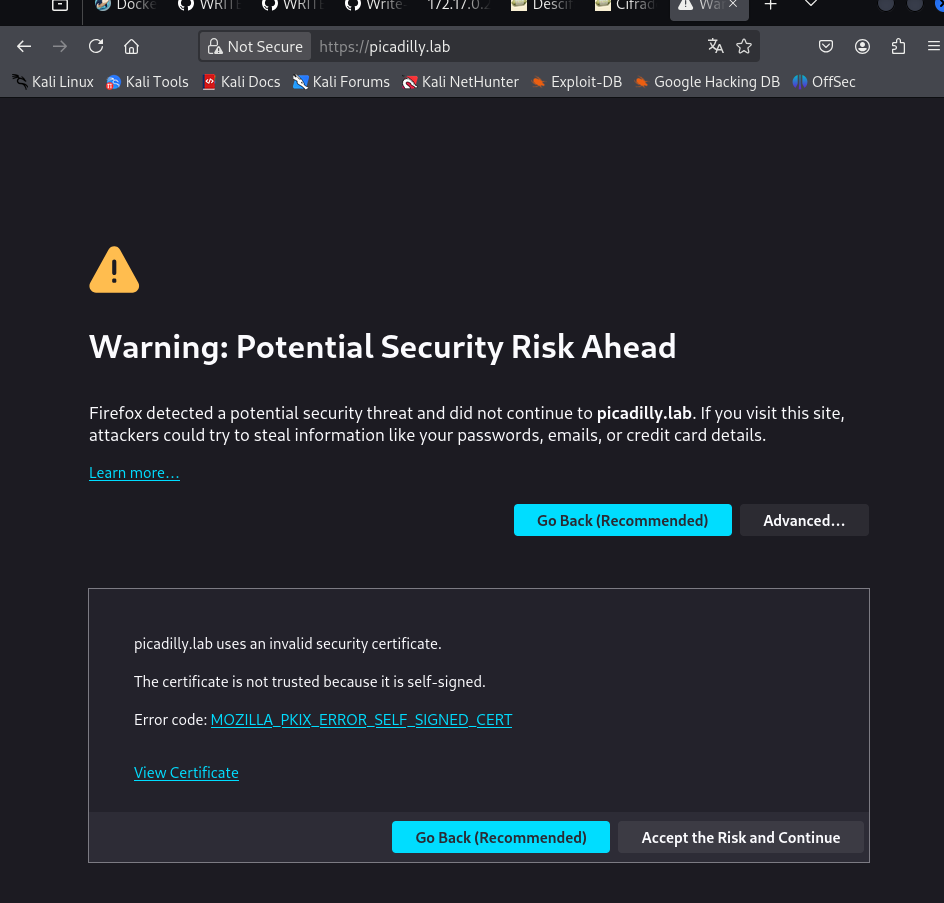
En el final del nmap podemos observar que hay otra parte de la web que no hemos visto por lo que tenemos que meter la IP de la maquina en el archivo /etc/hosts



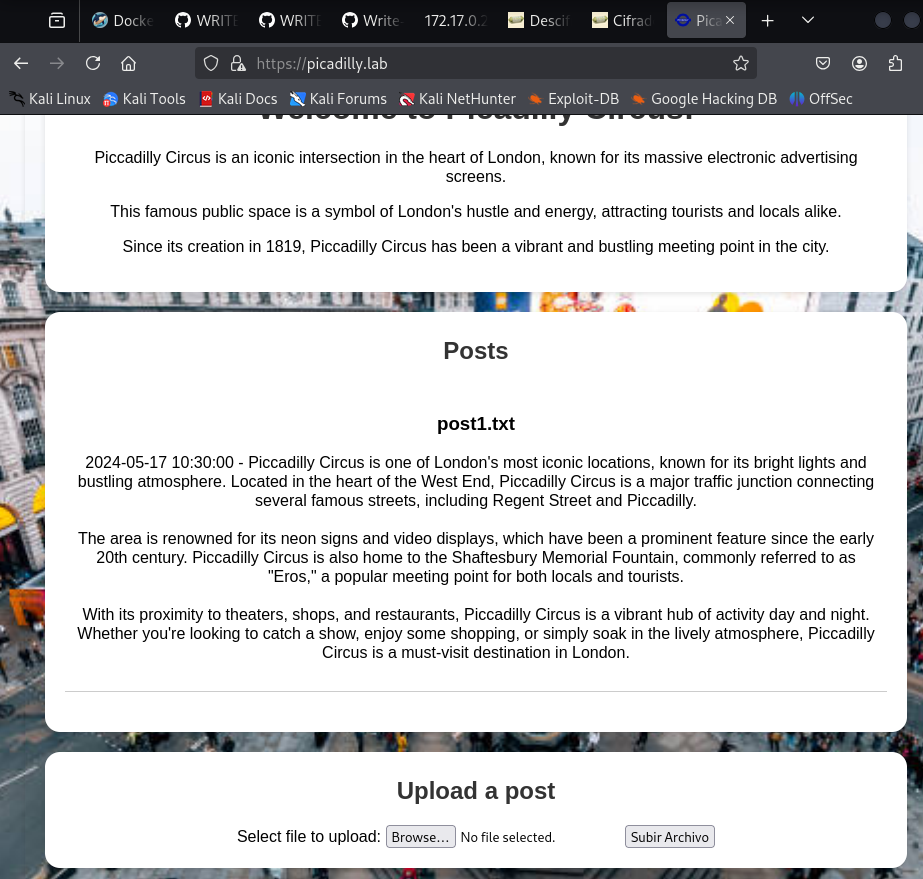
Y aquí la añadimos la IP del laboratorio.



Como esto está en el puerto 443 y que está corriendo allí por lo que ponemos lo siguiente en el navegador y aceptamos los riesgos.



Y como podemos observar, vemos una pagina web en la que podemos subir archivos y si queremos sacar algo de allí lo mas normal es subir un archivo en este caso php malicioso.

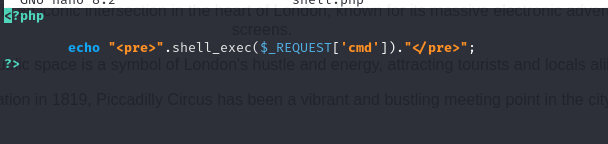


Por lo que creamos un archivo.php.

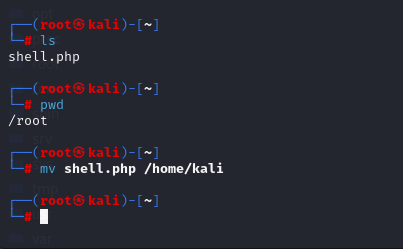


Dentro del archivo.ph y escribimos la siguiente configuración del comando PHP

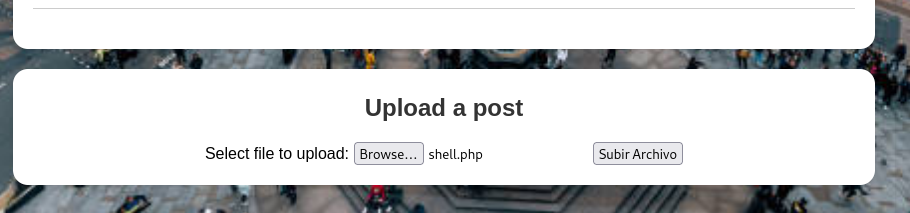




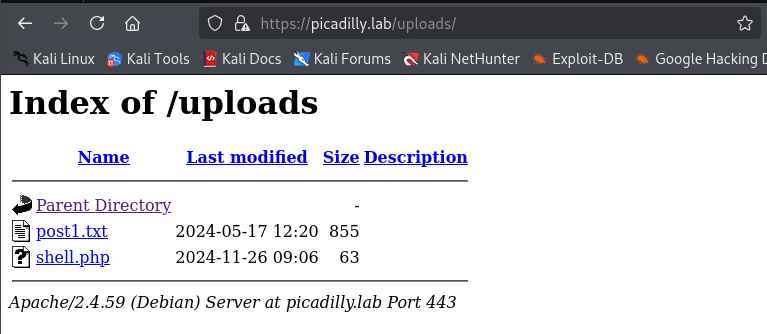
Una vez guardamos los cambios y todo como lo hemos creado con el usuario root para poder subirlo tenemos que mover el archivo al usuario de Kali.



Como podemos observar ya podemos subirlo



Para comprobar si nos lo ha subido correctamente dentro del laboratorio ingresamos Uploads es decir cosas subidas y cómo podemos observar se ha subir correctamente el archivo Shell.php



¿Y por último podemos comprobar que funcione poniendo el Shell.phpcmd=id? al final para ejecutarlo y comprarlo y cómo podemos observar

Primera Imagen En la primera imagen, se ha escrito un script PHP sencillo llamado shell.php.

Este script ejecuta comandos del sistema operativo que el atacante (o desarrollador) introduce a través de una solicitud HTTP.

Ejecuta el comando del sistema operativo proporcionado en el parámetro cmd y devuelve el resultado.

Este script es muy peligroso si está expuesto en un servidor, ya que permite ejecutar cualquier comando del sistema operativo directamente a través de la URL.

https://picadilly.lab/uploads/shell.php?cmd=id

Aquí: shell.php es el script previamente creado y subido al servidor. El parámetro cmd=id pasa el comando id al script PHP.

uid=33(www-data) gid=33(www-data) groups=33(www-data) Este es el resultado del comando id ejecutado en el servidor a través del script PHP (shell.php).

El comando id en sistemas basados en Linux o Unix muestra información sobre el usuario y los grupos bajo los cuales se está ejecutando el comando.

Explicación de cada elemento uid=33(www-data): uid significa User ID o Identificador de Usuario.

El valor 33 es el identificador numérico del usuario en el sistema.

www-data es el nombre del usuario asociado al ID 33.

Este usuario es utilizado por los servidores web para ejecutar procesos web de forma aislada, limitando el acceso al sistema.

gid=33(www-data): gid significa Group ID o Identificador de Grupo.

Al igual que el uid, el valor 33 es el identificador del grupo en el sistema.

www-data también es el nombre del grupo principal al que pertenece el usuario. groups=33(www-data): Aquí se listan los grupos adicionales a los que pertenece el usuario que ejecuta el comando. En este caso, el usuario www-data pertenece únicamente al grupo www-data con el ID 33.

