

hACKING éTICO

Unidad 2. Actividad 10



29 de Noviembrebre de 2023

Carlos DÍAZ MONTES

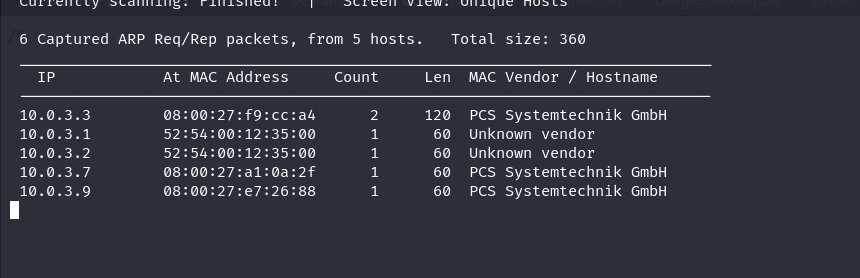
ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Ejercicio 1. 1](#_Toc152183703)

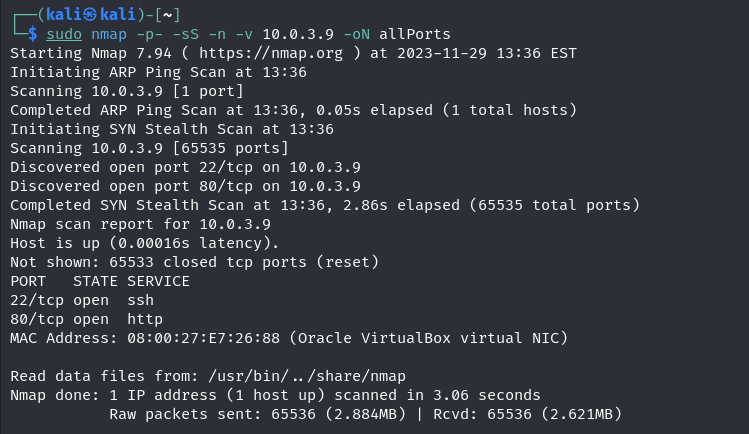
# Ejercicio 1.

Lo primero que he realizado es saber su ip:



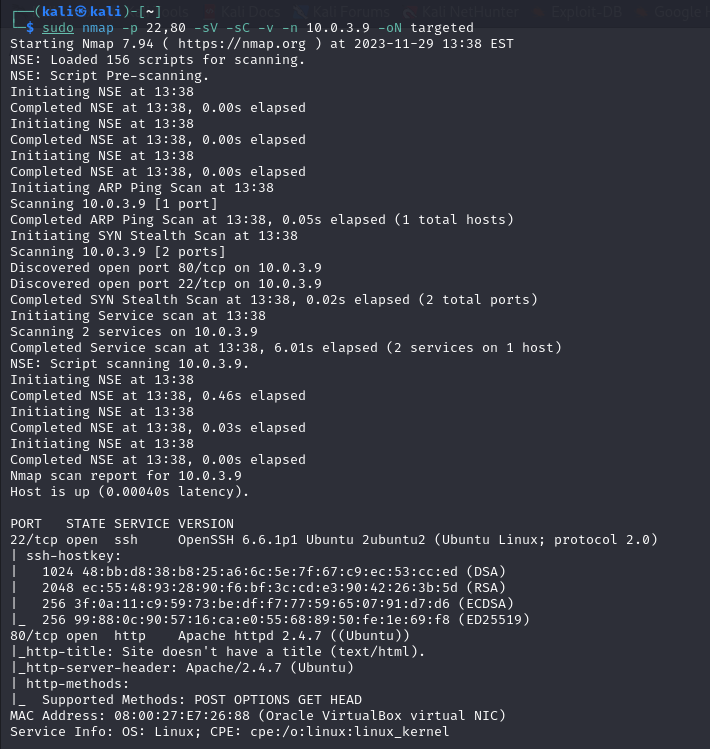
Tiene que ser la .9 ya que la .7 es la otra máquina.

Ahora comprobamos los puertos:

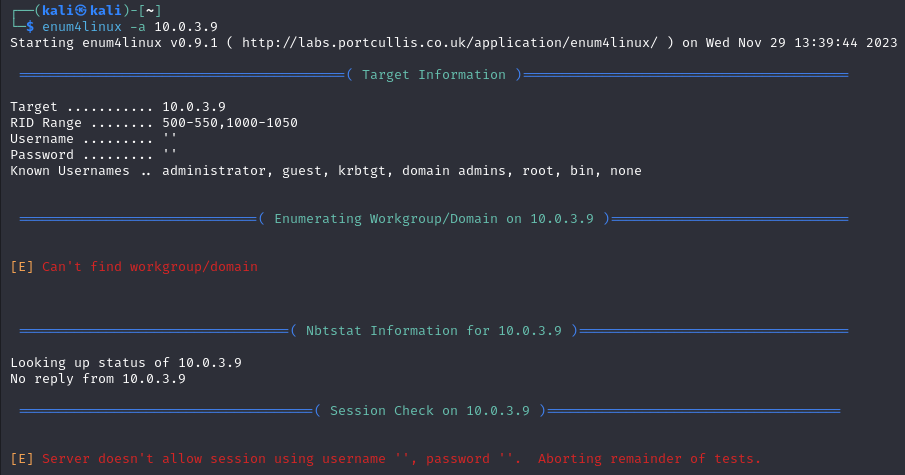


Como vemos tiene el puerto 22 y el 80 abierto.

Ahora vamos a hacer un escaneo específico a esos puertos:



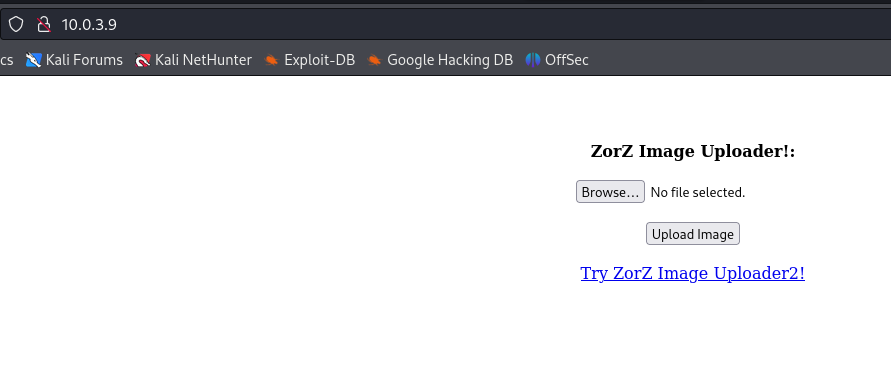
Buscamos posible información con enum4linux, como por ejemplo los usuarios que contiene la máquina:



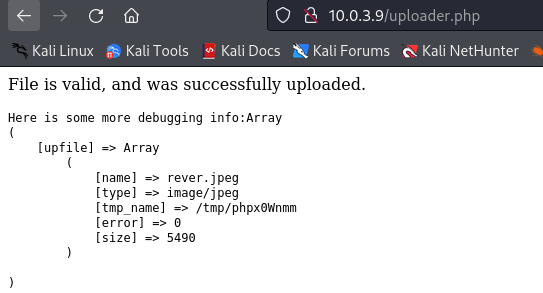
Comenzamos.

**Nivel 1**

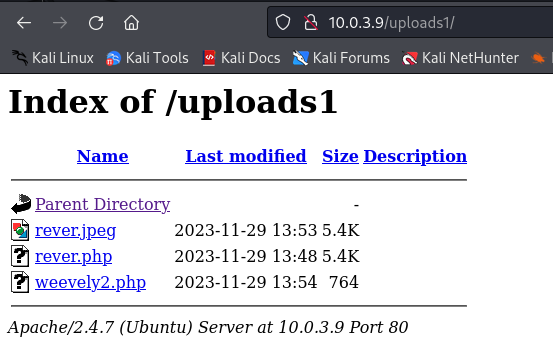
Primero vamos a irnos a su url con la ip que tiene y vemos que tiene una pagina para insertar fotos.



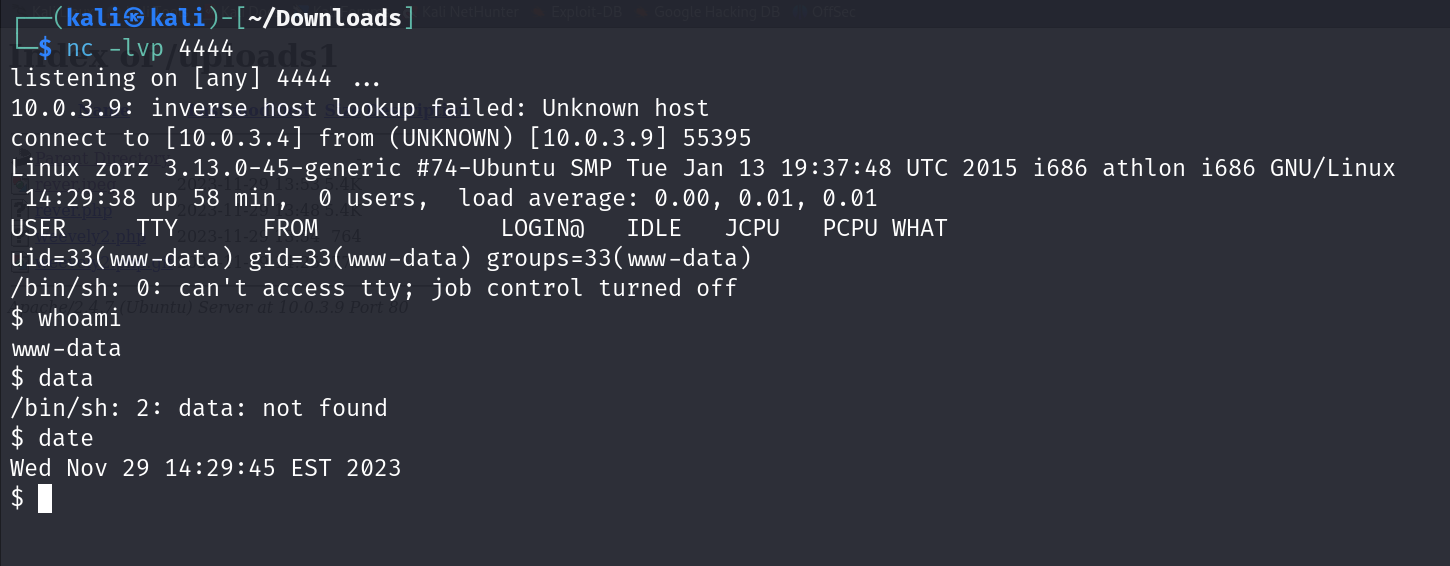
Ahora vamos a usar burpsuite para enviar un archivo php:



Ahora comprobamos que lo hemos podido subir:

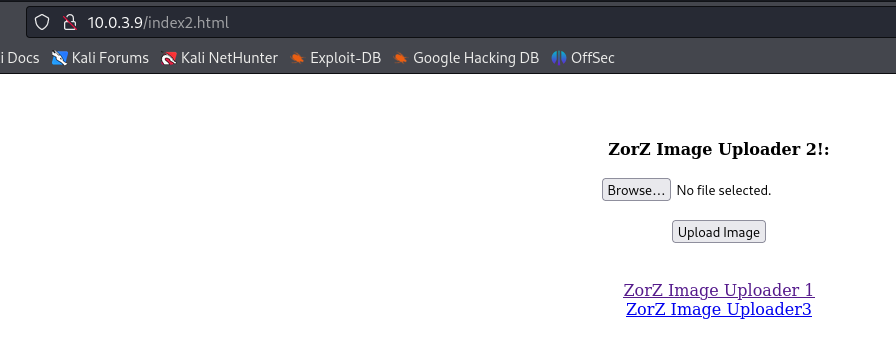


Por último comprobamos la Shell reversa:

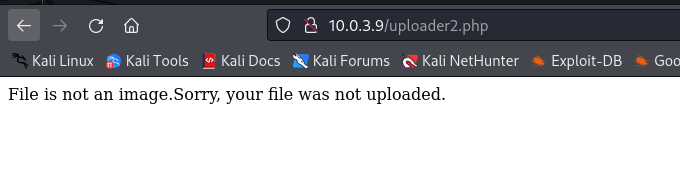


**Nivel 2**

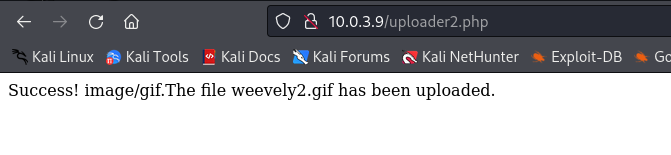
Para el nivel dos buscamos index2.html:



He probado el mismo truco que antes peroasi no funciona:



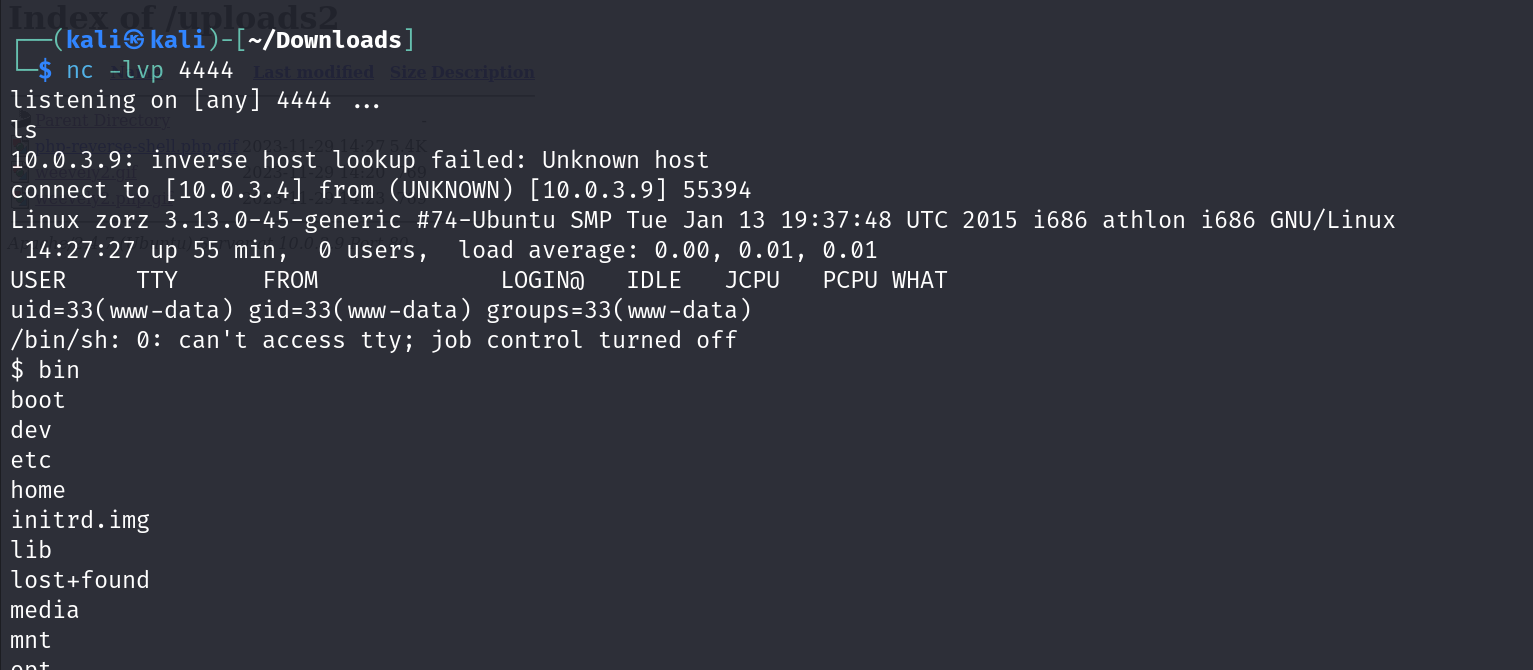
Ahora he probado a cambiar el formato del archivo:



Aquí comprobamos que esta el archivo:

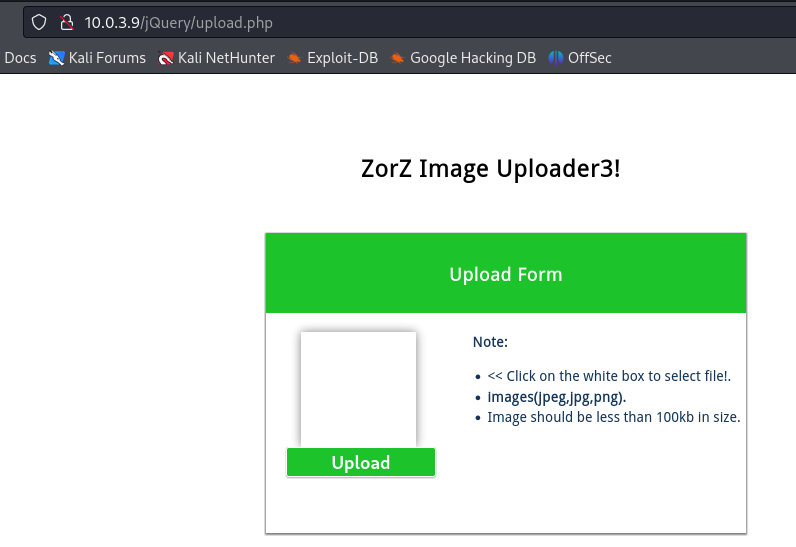


Una vez pinchamos en el nos hace la Shell reversa:

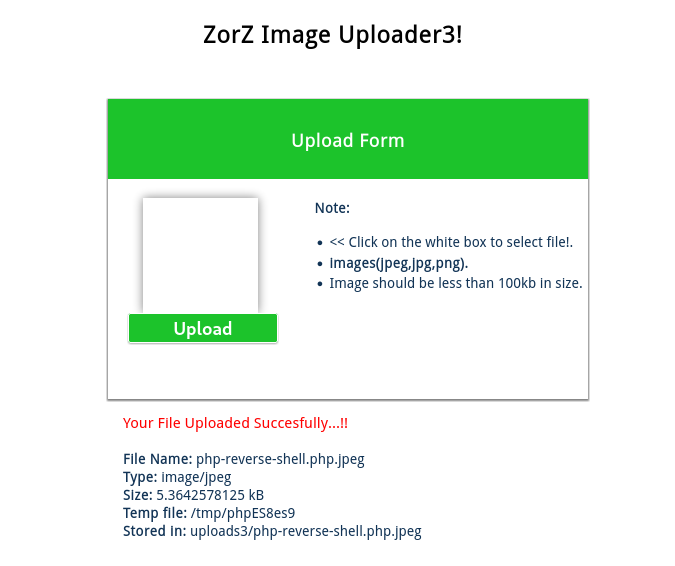


**Nivel 3**

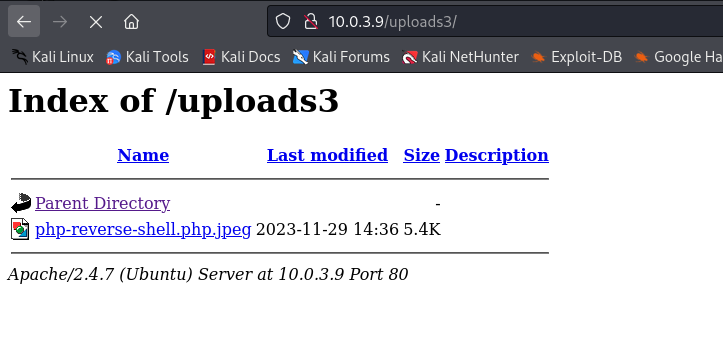
En el nivel 3 vemos que cambia un poco.



Ahora vamos a probar a cambiar la extensión del archivo a jpeg:



Como vemos podemos ver como ha aceptado el archivo, ahora simplemente lo abrimos:



Al abrirlo vemos que deja conectarse:

