

hACKING éTICO

Unidad 2. Actividad 9



29 de NOVIEMbre de 2023

Carlos DÍAZ MONTES

ESPECIALIZACIÓN DE CIBERSEGURIDAD

Índice

[Ejercicio 1. Nivel de seguridad medio. 2](#_Toc152178006)

[Ejercicio 2. Comandos de weevely. 4](#_Toc152178007)

[Ejercicio 3: Meterpreter. 6](#_Toc152178008)

# Ejercicio 1. Nivel de seguridad medio.

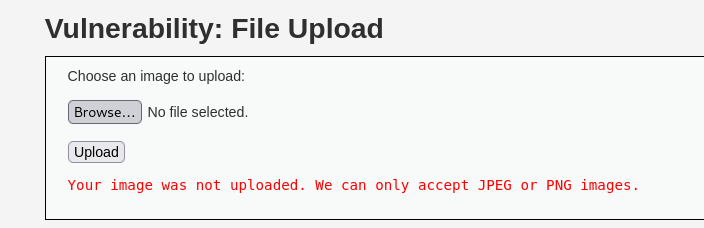
Ponemos la seguridad en médium:



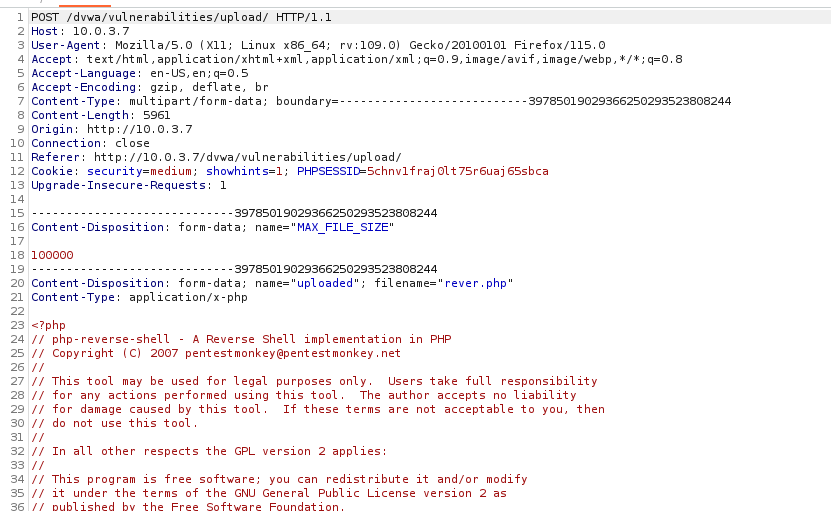
Borramos todo el contenido de hackable/uploads:



- Sube la shell reversa que tenías de antes. La que copiaste de /usr/share/webshells/php. No te va a dejar. Verás el error “Your image was not uploaded. We can only accept JPEG or PNG images.”



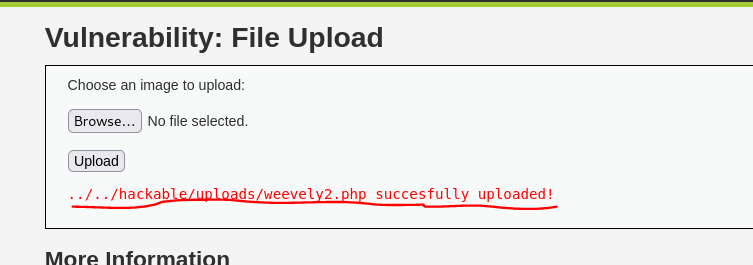
- Vuelve subirlo, pero esta vez, intercepta la llamada con Burp Suite. Fíjate bien en el cuerpo del mensaje (lo que viene después de las cabeceras HTTP en una request de tipo POST).



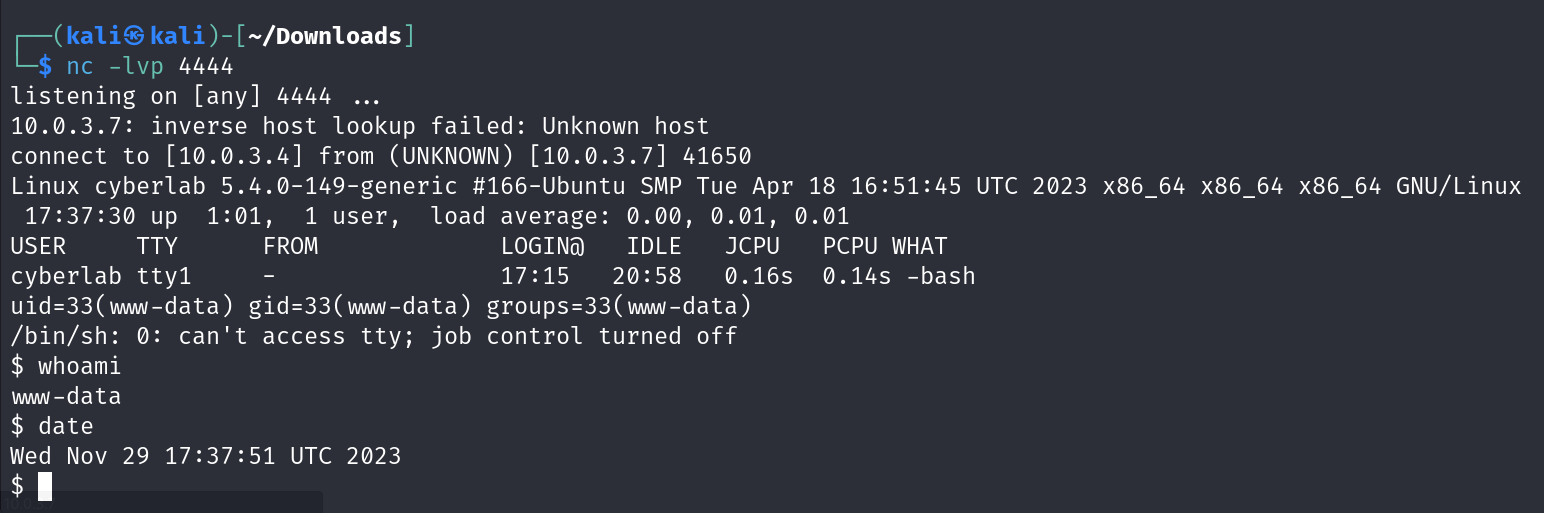
- Dentro del cuerpo, fíjate en la parte en la que envías el php en sí. Content-Type es ese tipo MIME que le ha asignado tu navegador… ¿Y si lo cambias a uno que le guste más a DVWA? …



Ahora como vemos me sale:



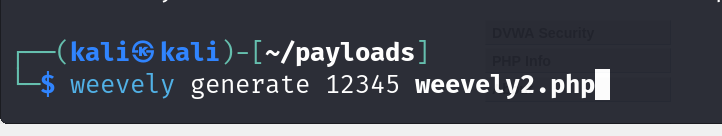
Ahora comprobamos que me deja hacer la Shell reversa:



# Ejercicio 2. Comandos de weevely.

Usamos weevly para hacer una Shell inversa.

Para hacer esto tenemos primero que generar un clave:

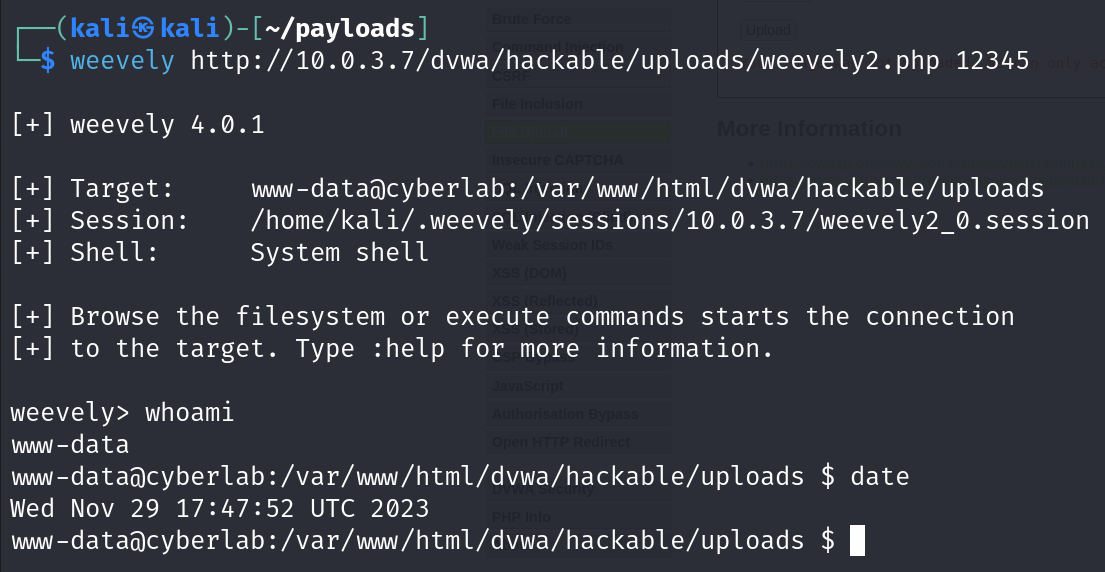


En esta clave tenemos como contraseña 12345 y se guarda en el archivo weevely2.php.

Ahora subimos el archivo weevely2.php:

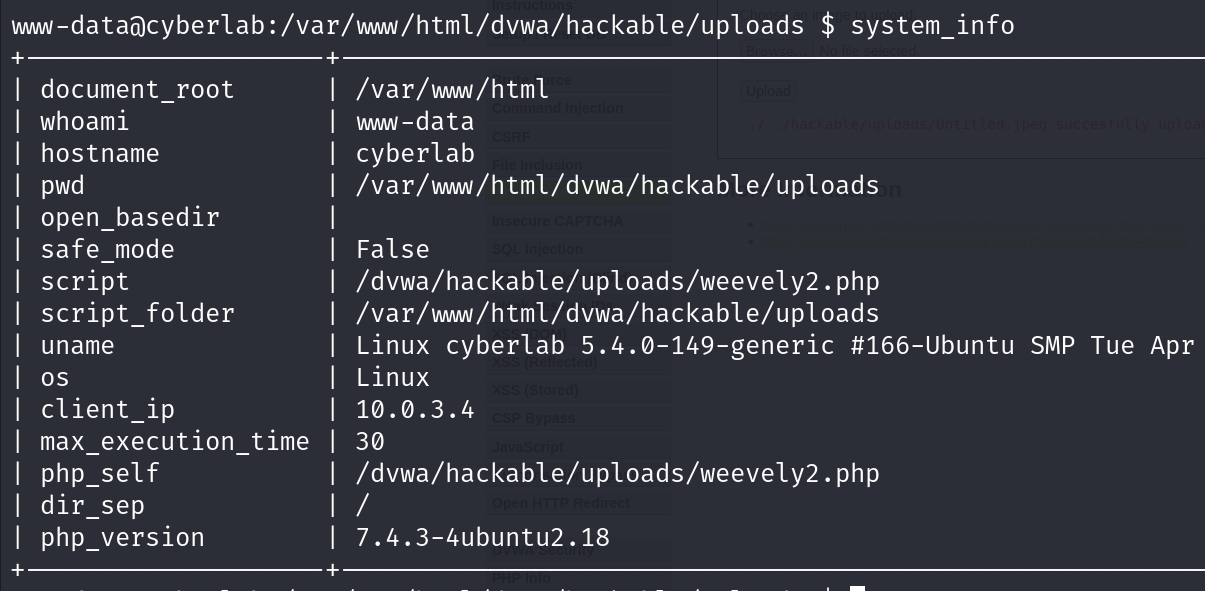


Ahora podemos poner el comando siguiente para conectarnos:



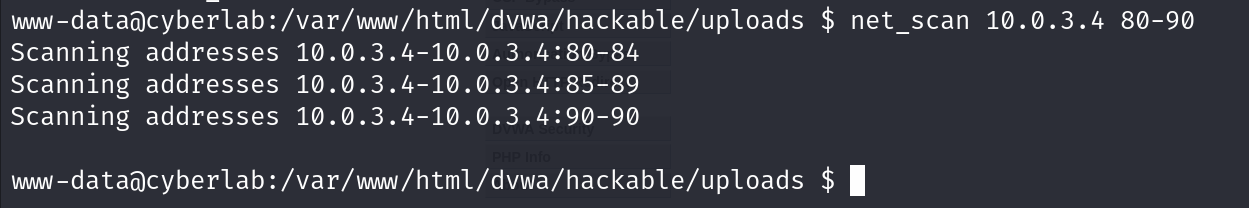
Ahora vamos a probar dos comandos. El primero es system\_info:

Este sirve para darnos información sobre la maquina a la que nos hemos conectado:



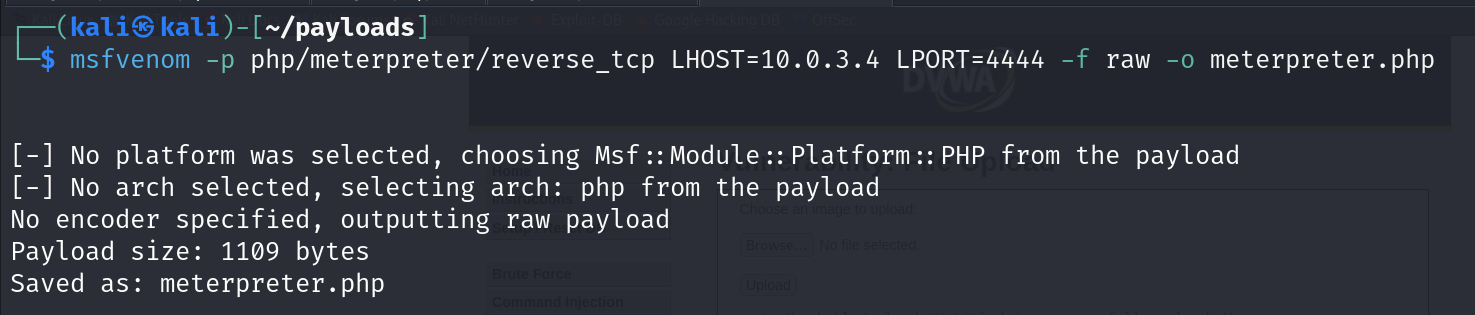
El segundo es net\_scan

Te hace un escaneo de puertos:

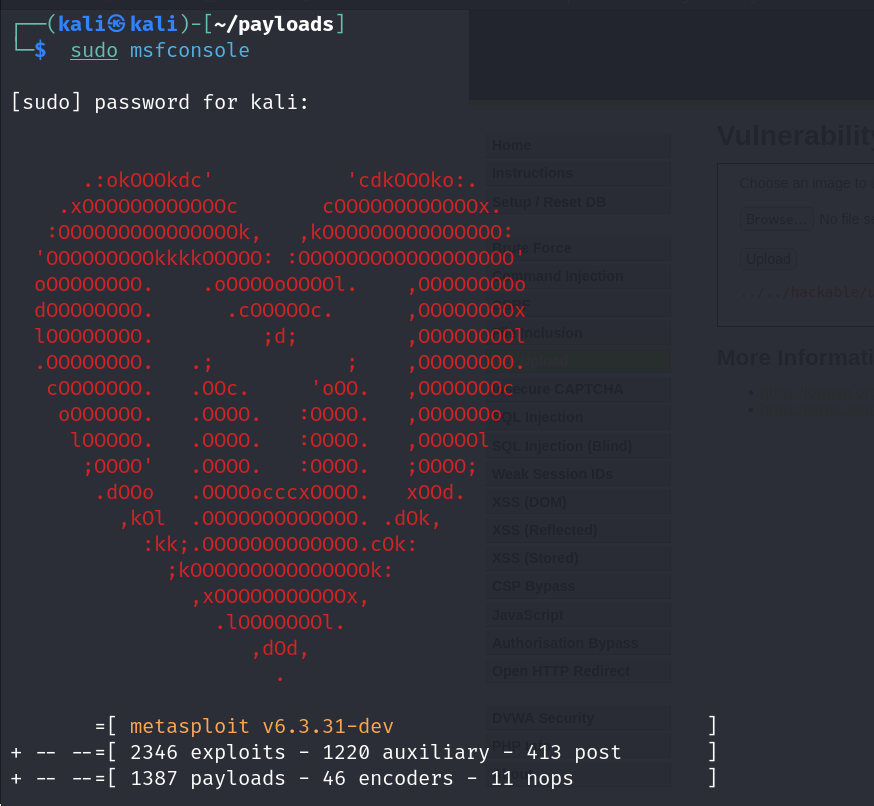


# Ejercicio 3: Meterpreter.

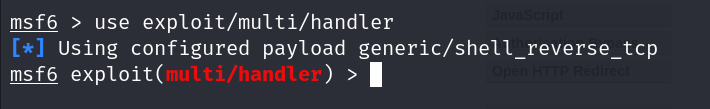
Paso 1: generar el payload a subir.



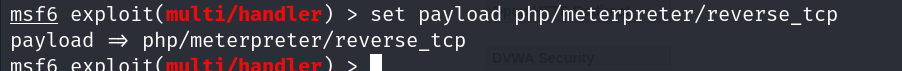
Iniciamos metasploit:



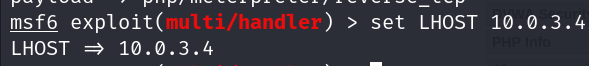
Carga el módulo exploit/multi/handler



Modifica el payload para que coincida con el que pusiste con msfvenom:



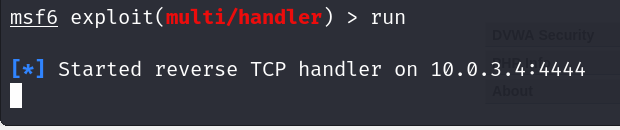
Especifica cuál es la IP en la que vas a escuchar:



Especifica el puerto:



Lo lanzamos:



Comprobamos que funciona (no pongo captura de los pasos previos que he realizado, son los mismos que en el 1 y 2)

