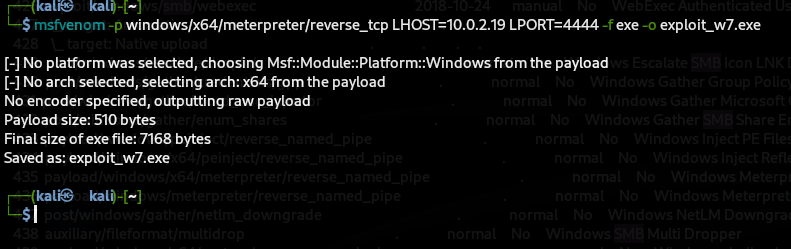


**EJERCICIOS MSFVENOM**

EJERCICIO 1 - MSFvenom y Metasploit

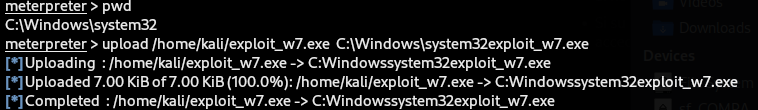
1.- Se Crea con MSFvenom un troyano adecuado para el sistema *Windowsploitable7:*



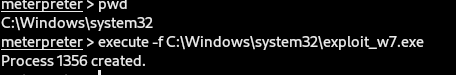
2.- Se Inicia sesión mediante una vulnerabilidad en maquina objetivo:



3.- Se procede a cargar el troyano en la máquina atacada:



4.- Se ejecuta en la maquina objetivo el exploit creado, mientras se encuentra a la escucha por el puerto 444 el multi/handler:

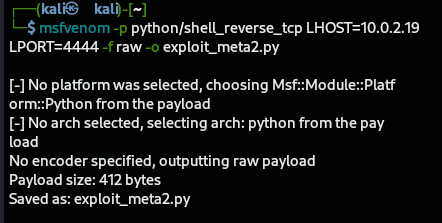


5.- Una vez se ejecuta el exploit, obtenemos una sesión multi/handler en la maquina objetivo



EJERCICIO 2 - MSFvenom y Metasploit

1.- Se crea con MSFvenom un troyano adecuado para el sistema Metasploitable2:

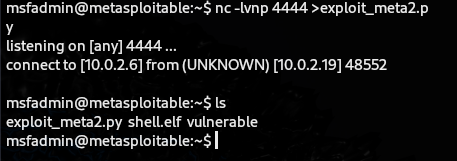


2.- Se carga el troyano en la máquina a través de ssh:

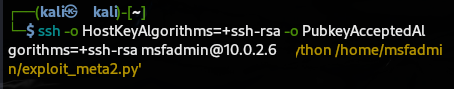
* Envío de Kali a Metaexploitable



* Recepción por parte del objetivo



3.- Se ejecuta el exploit creado en la maquina objetivo, una vez abierta la multi/handler en Metasploit:



4.- Se utiliza el exploit *multi/handler* para conseguir una sesión en la máquina víctima:

