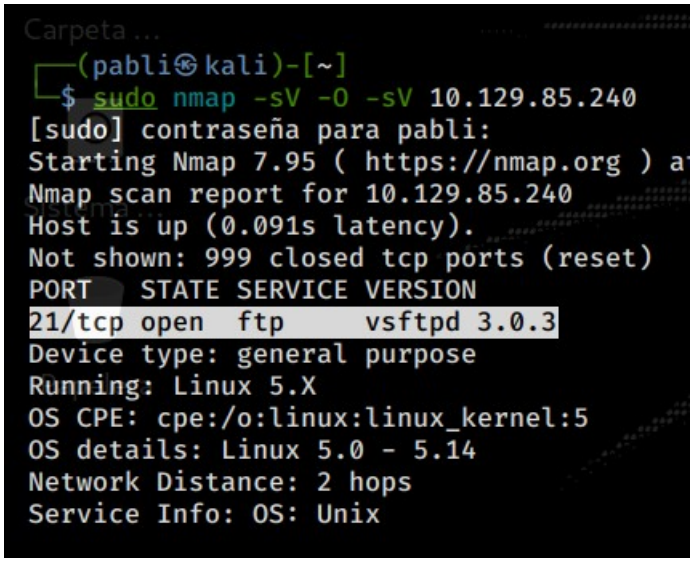
HackTheBox

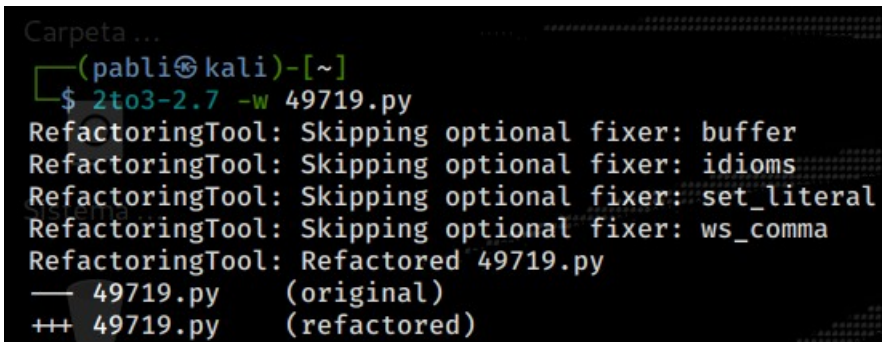
Máquina: Fawn
Pablo José Pérez Díez

Escaneo inicial:



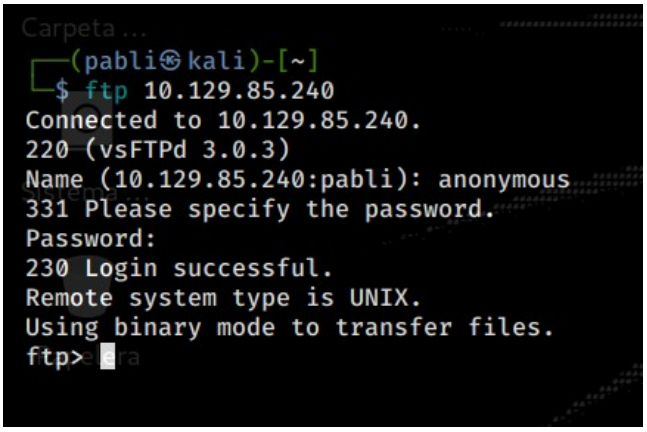
Observamos que existe un exploit para esta versión de FTP y lo descargamos al directorio actual:

Mediante la herramienta 2to3 actualizamos el script a python3:



Con la herramienta autopep8 normalizamos los espacios:

Analizando el contenido del exploit nos damos cuenta de que no nos es útil ya que se trata de un ataque de denegación de servicios, por lo que intentamos entrar de manera más sencilla:



Nos conectamos mediante el usuario anonymous sin especificar contraseña, ya que esto nos permite conectarnos al servidor mediante FTP sin credenciales.

Obtenemos la flag haciendo un get: