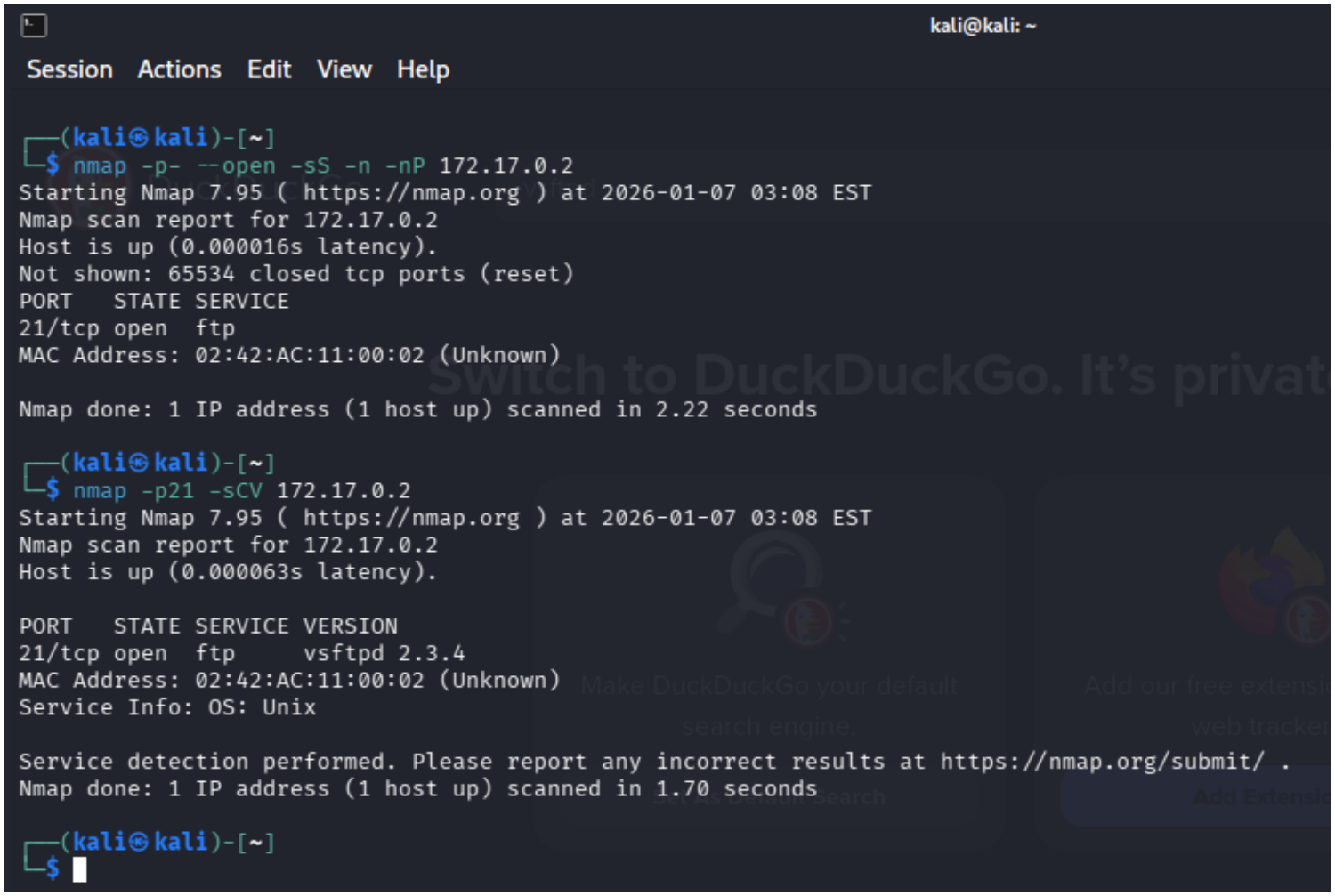
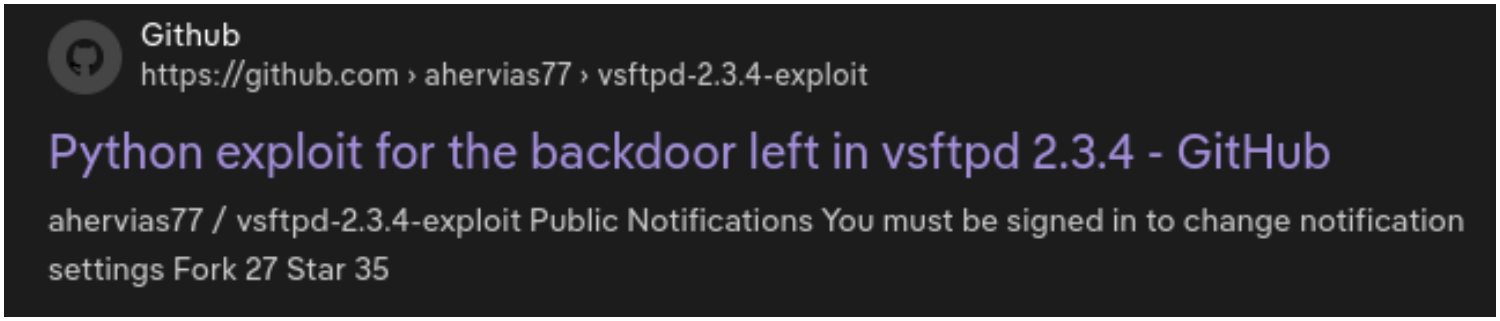
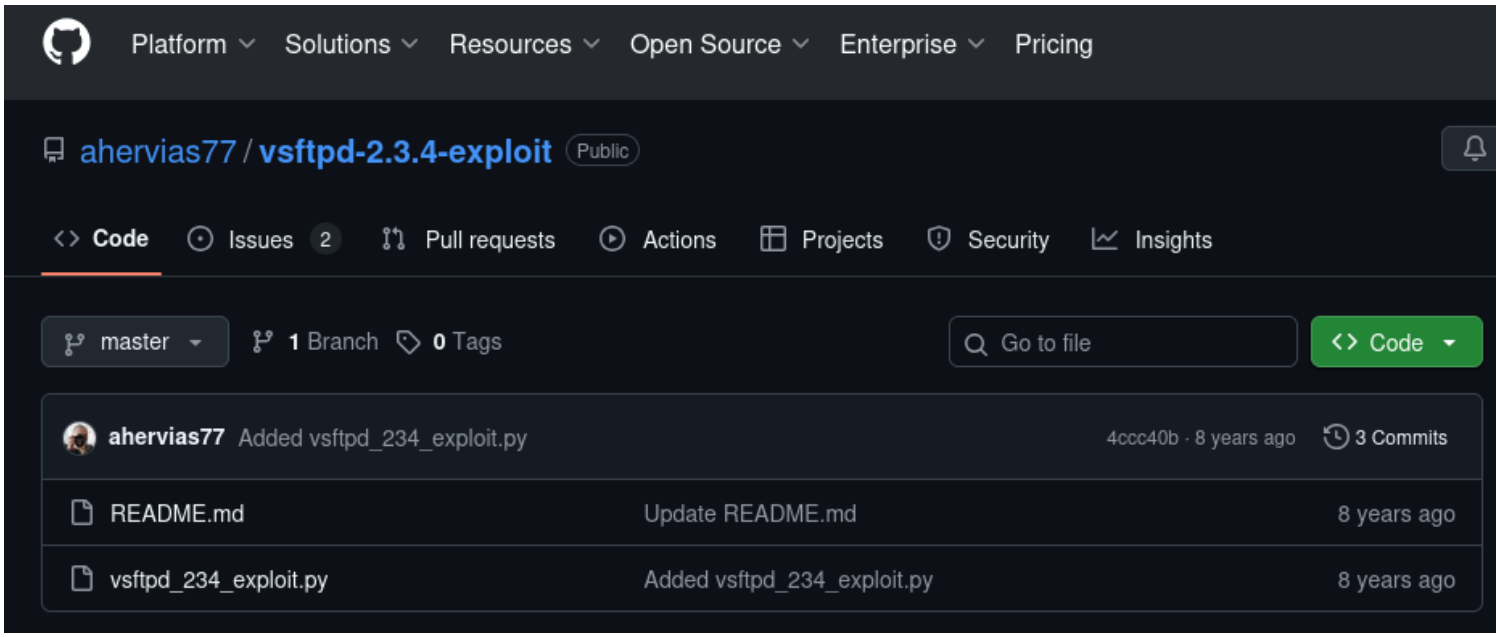
firsthacking (DockerLabs)

En primer lugar vemos con ***nmap*** los puertos abiertos.
Parece que solo el 21 (FTP), así que volvemos a ejecutarlo sobre ese puerto concreto con la opción -sV para ver la versión del servicio.
Parece ser vsftp 2.3.4.

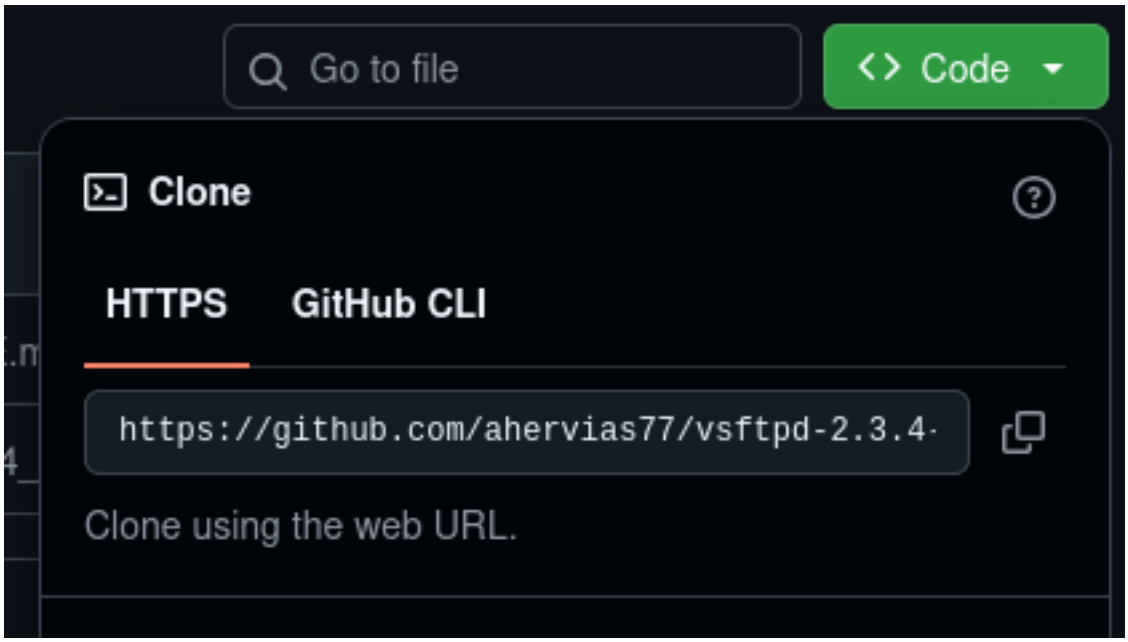


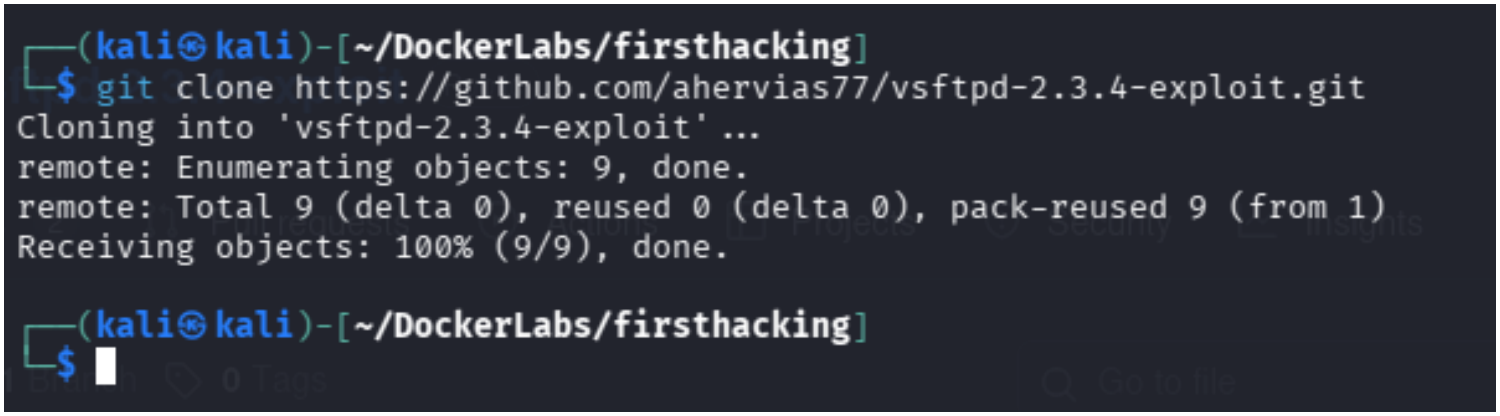
Buscamos un exploit para esta conocida vulnerabilidad. Como soy un forofo de Python, intentaré encontrar un exploit en ese lenguaje, y lo encontramos en GitHub:





Vamos a clonar el código en la carpeta de nuestro proyecto:





Por último miramos a ver cómo se usa el exploit y lo ejecutamos contra la máquina vulnerable:

README

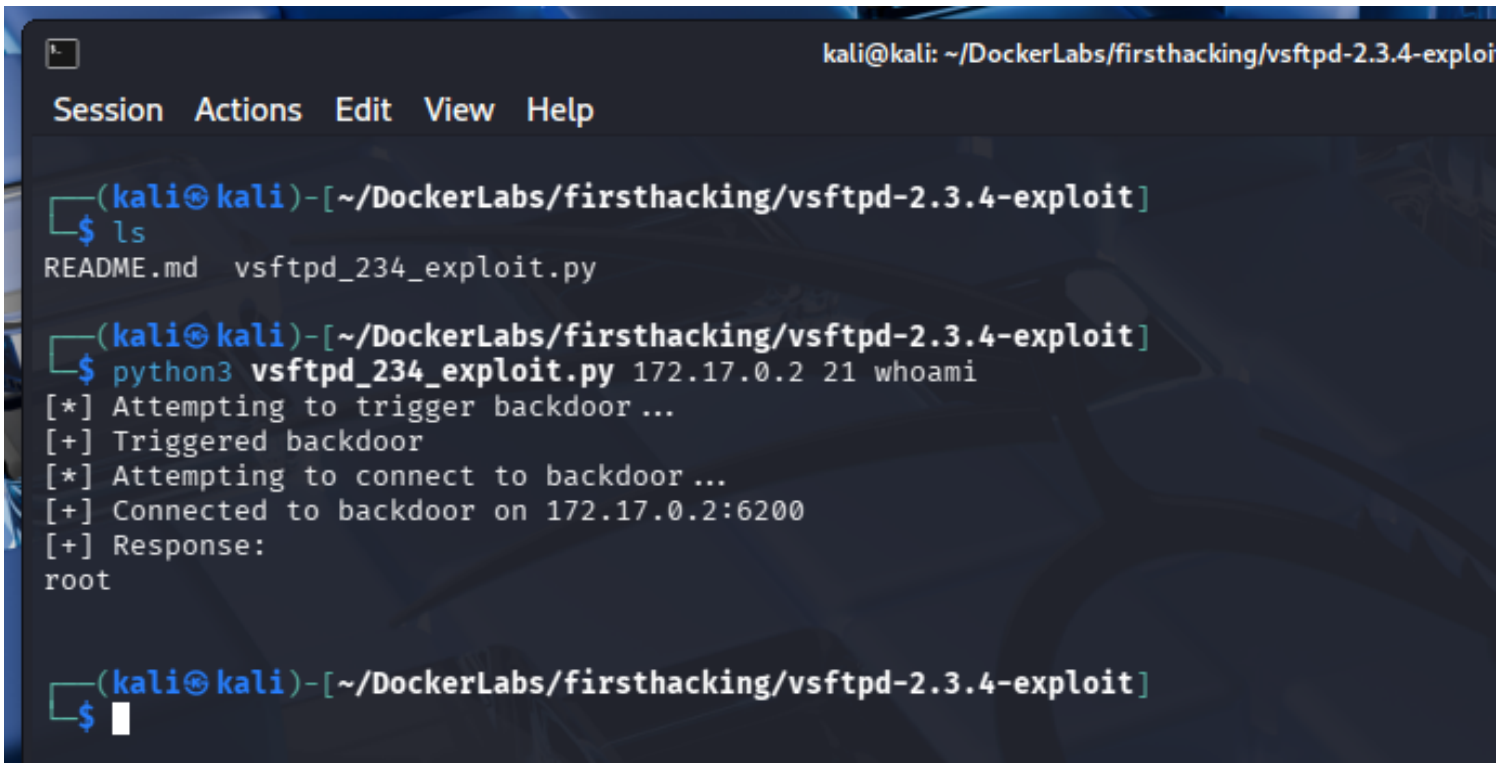
vsftpd 2.3.4 Exploit (Python)

Python exploit for the backdoor left in vsftpd 2.3.4

Triggers the vsftpd 2.3.4 backdoor and prints the supplied command's output

Usage: ./vsftpd_234_exploit.py [IP address] [port] [command] *Example:* ./vsftpd_234_exploit.py 192.168.1.10 21 whoami

Sencillo, sólo hay que indicar la IP de la máquina víctima, el puerto (21) y un comando, en este caso usaremos 'whoami'.
Entramos en la carpeta donde se clonó y lo ejecutamos:



Listo, somos root :-)