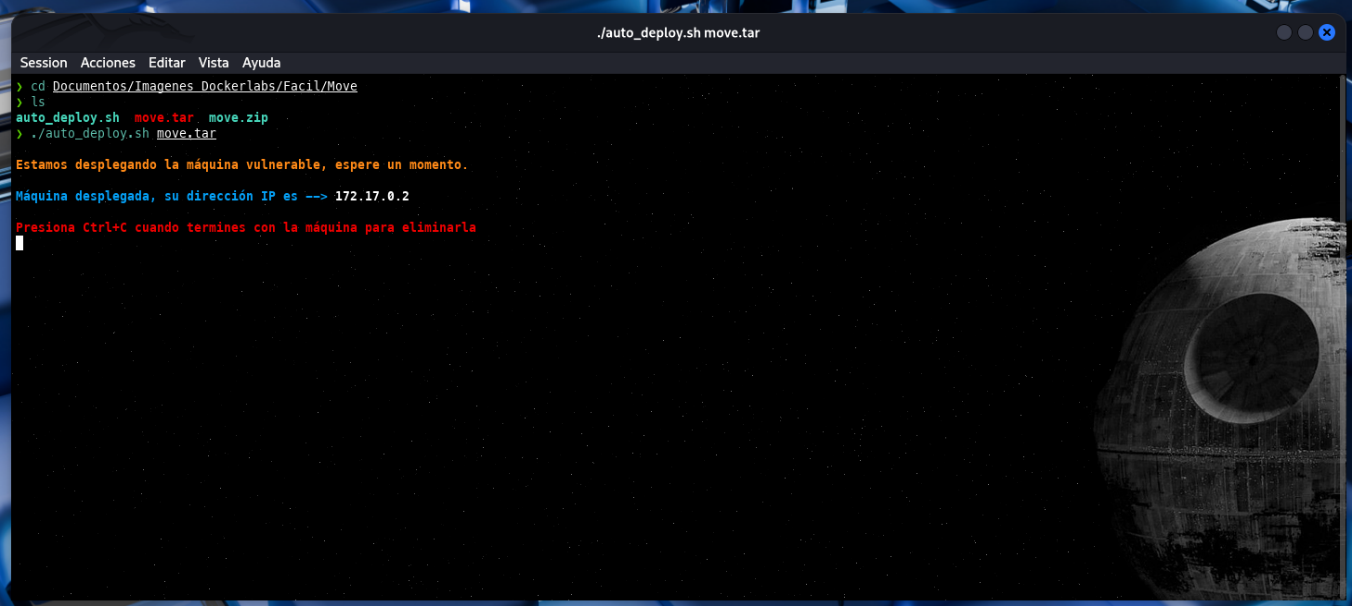
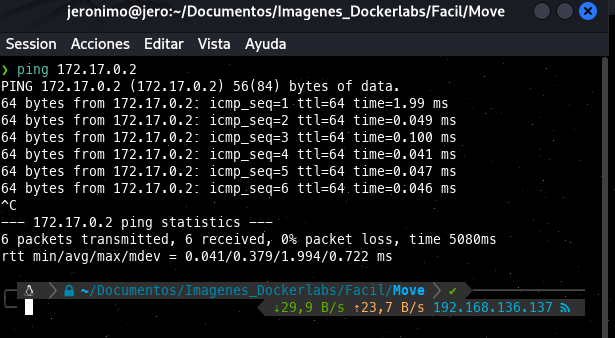
README MOVE

1. El primer paso es levantar la máquina, se utiliza el siguiente comando

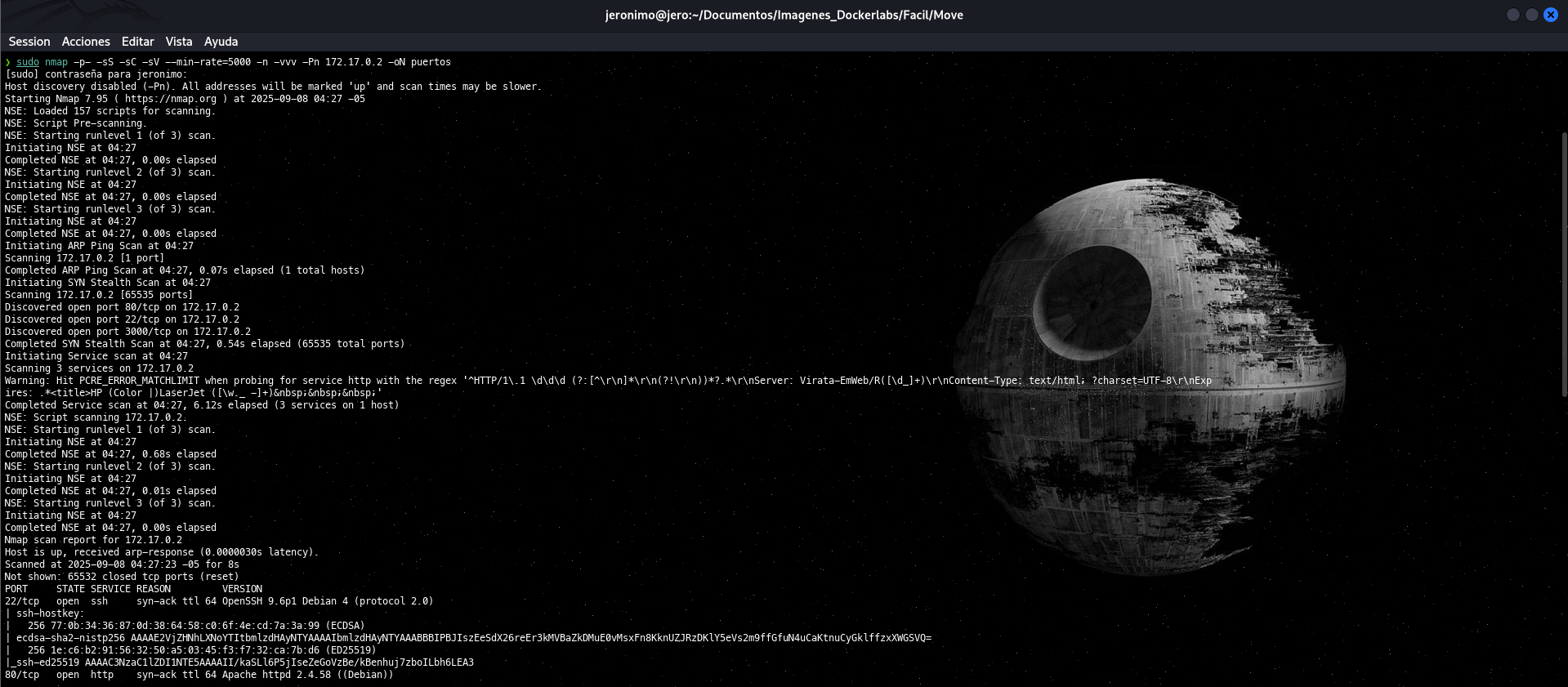


1. Realizamos ping con la máquina para saber si tenemos conexión.

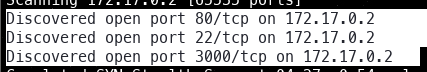


1. Utilizamos nmap para el escaneo de los puertos.

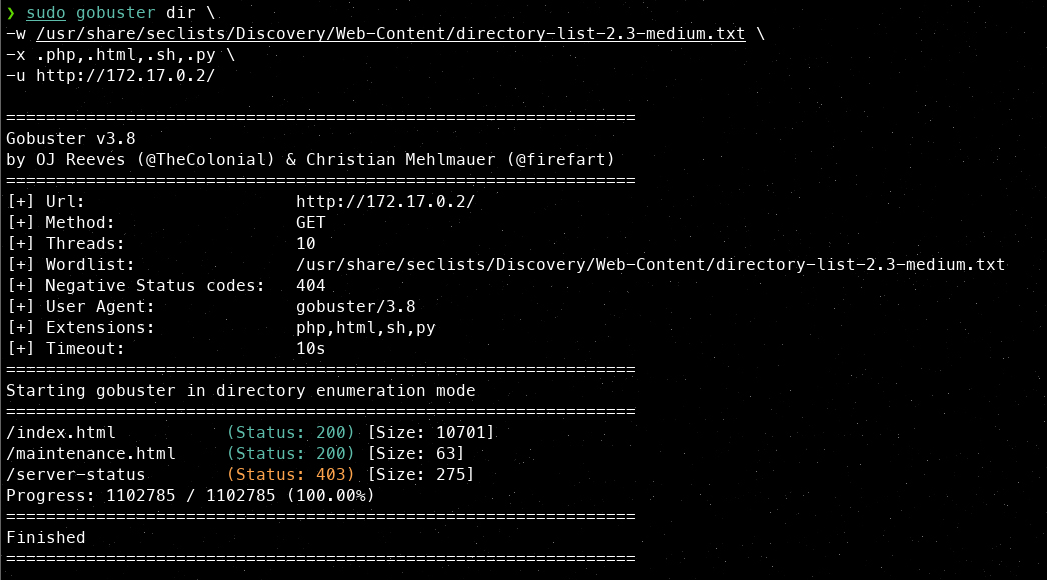
sudo nmap -p- -sS -sC -sV --min-rate=5000 -n -vvv -Pn 172.17.0.2 -oN puertos



Vemos los siguientes puertos abiertos:



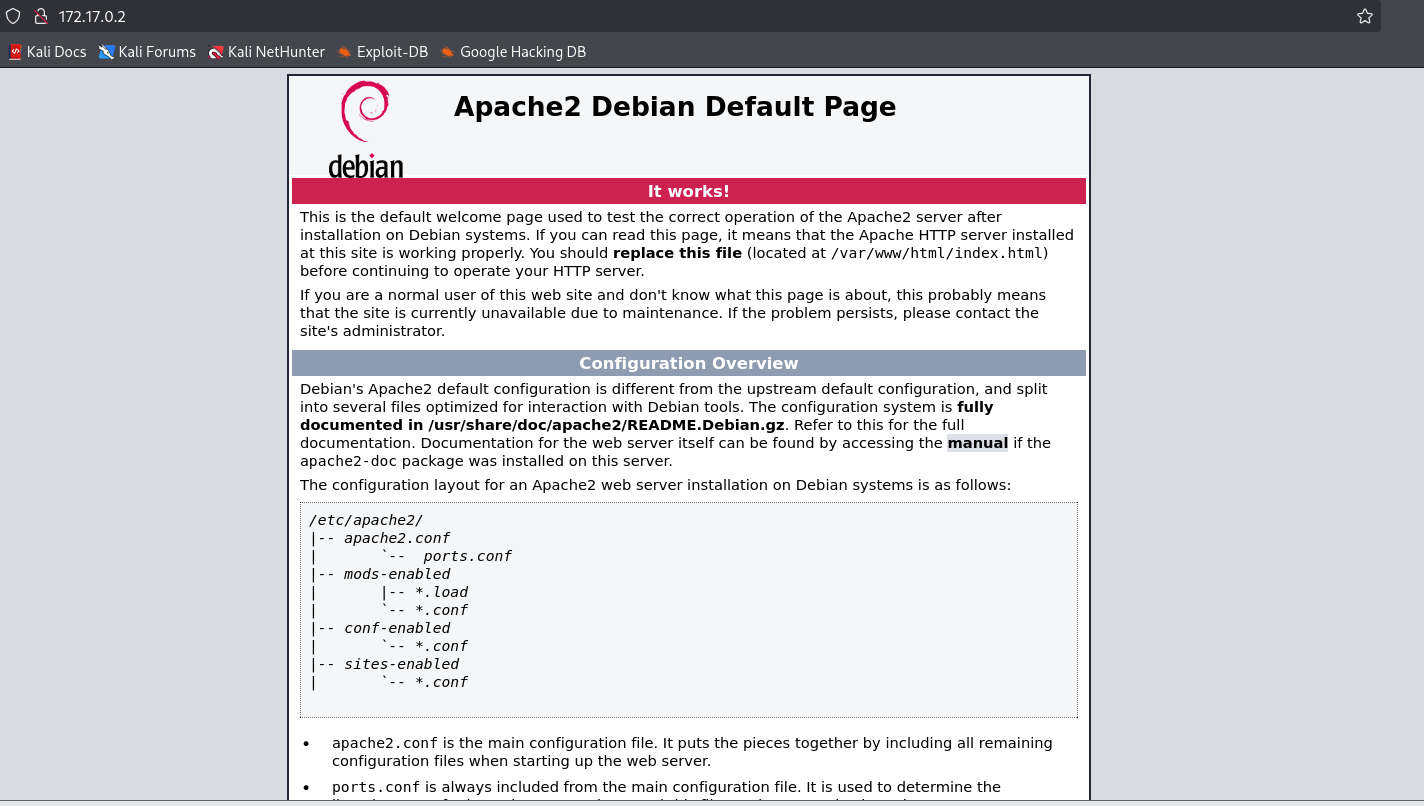
1. Se utiliza el **fuzzing** con la herramienta gobuster.  
   El cual consiste en probar automáticamente listas de palabras para descubrir directorios o archivos ocultos en un servidor web.



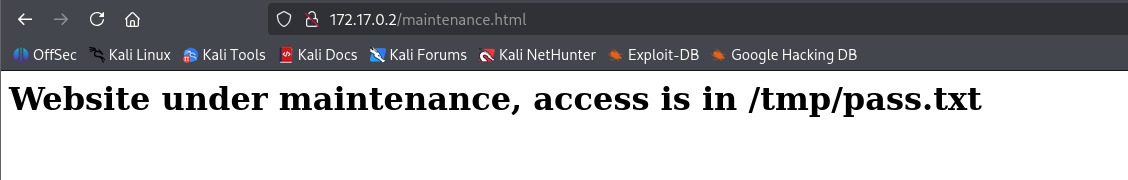
Vemos lo siguiente:



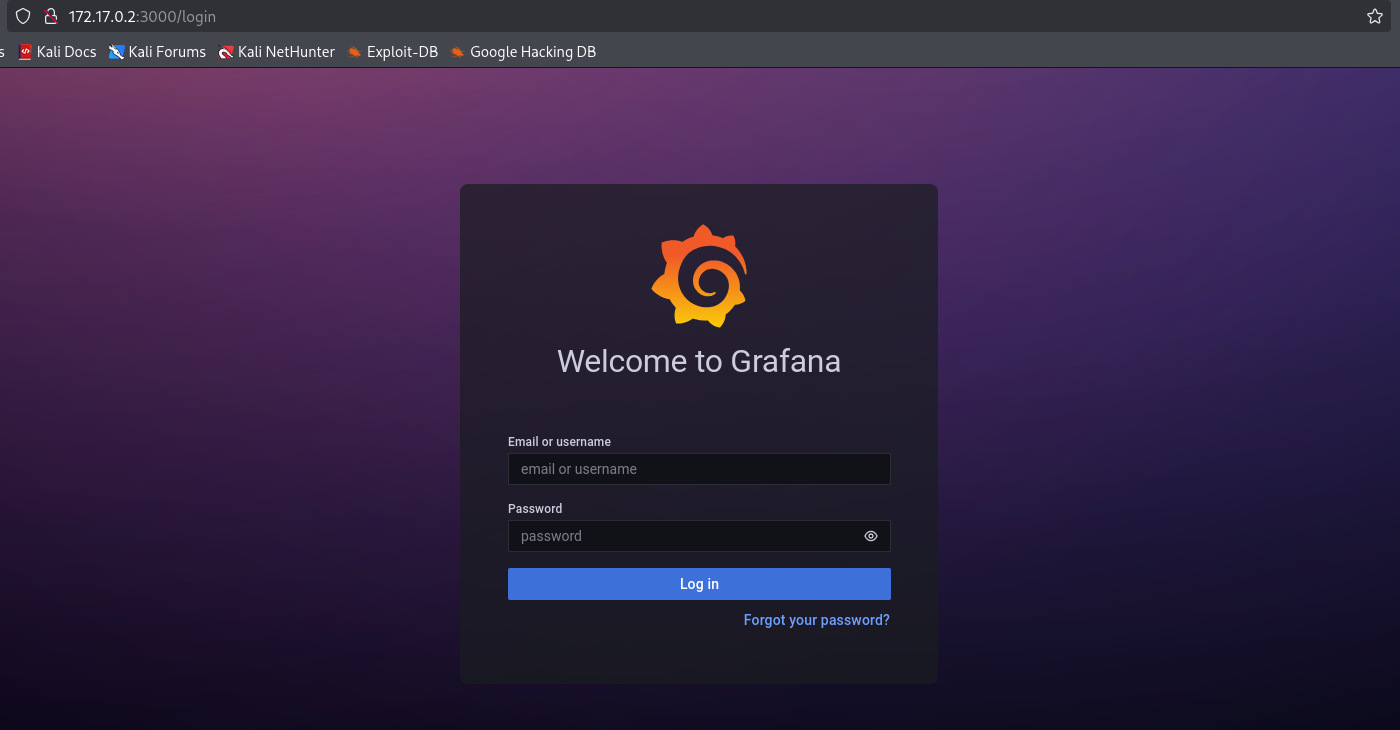
El cual entramos desde un navegador



Si ponemos solo la url sin el /maintenance se abrirá la página default de apache2

esto aparecerá al colocar /maintenance.html

1. Ahora desde el navegador entraremos al puerto 3000



Nos redirige a un inicio de sesión de Grafana

1. Vamos a buscar un exploit es y lo localizamos



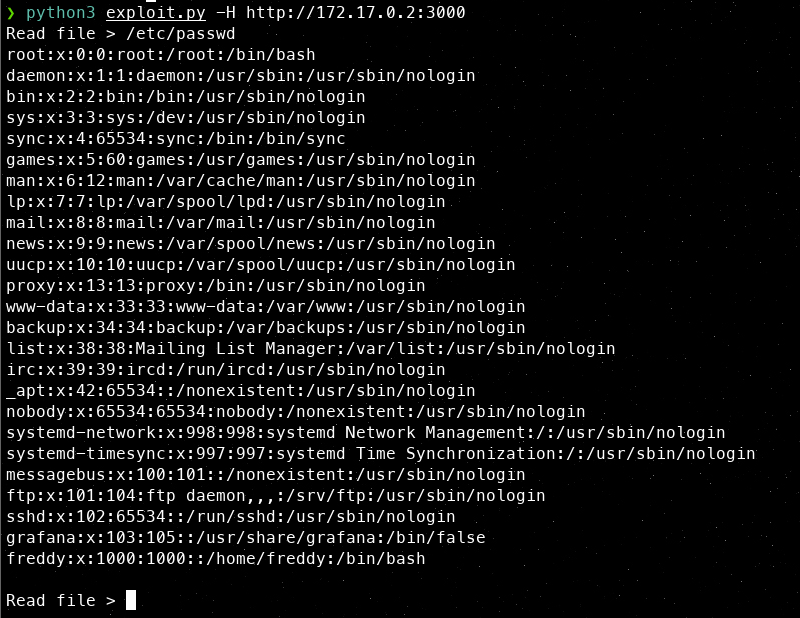
Lo copiamos



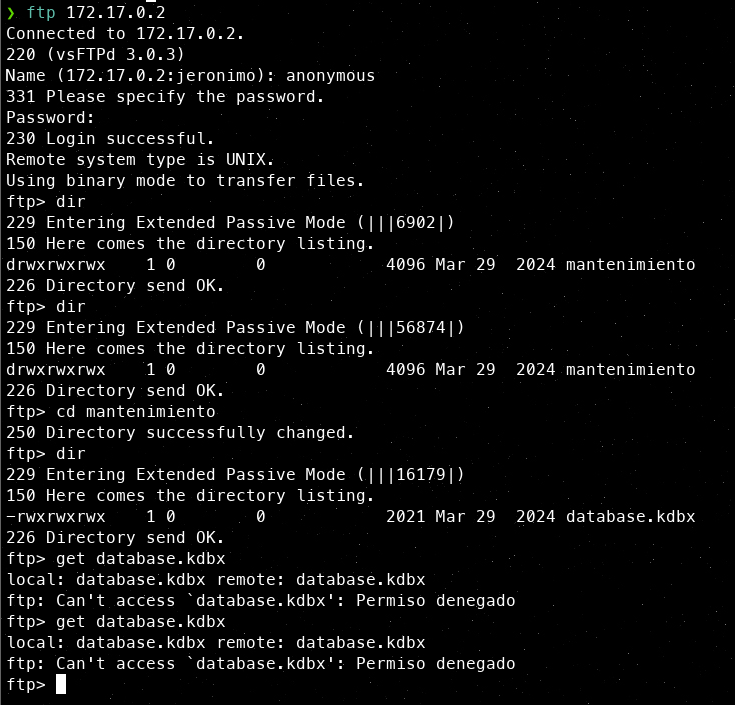
Y después con el siguiente comando indicaremos el puerto 3000 que es por donde está corriendo Grafana. Y este exploit lo que hace es leer archivos del sistema.



1. Vemos que al colocar /etc/passwd, vemos archivos internos del servidor



Observamos el usuario freddy

1. Tratamos de entrar mediante anonymous, pero no podemos acceder o descargar la base de datos