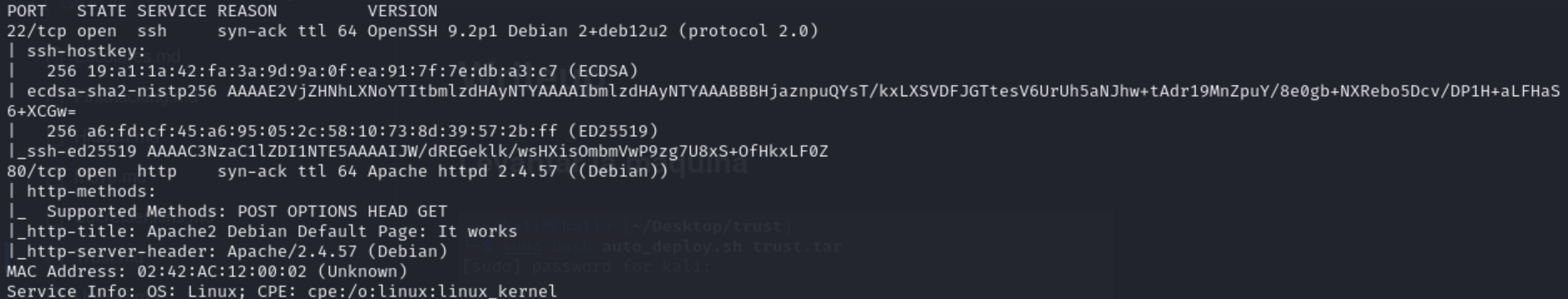
Writeup de la máquina Trust de Dokerlabs

1. Encendemos la máquina Trust.

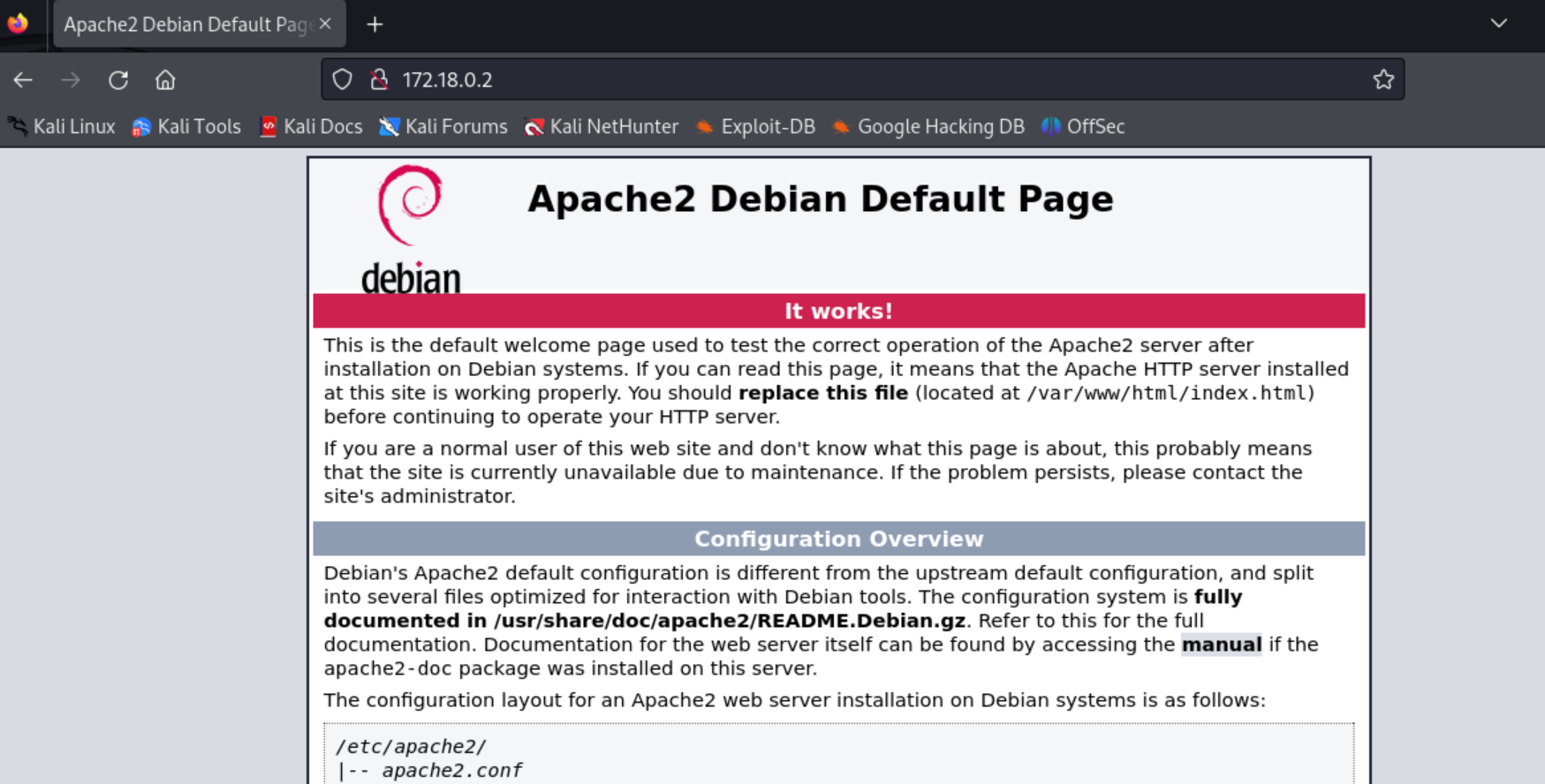


1. Vamos a escanear puertos de la IP de la máquina (172.18.0.2) con “nmap”.

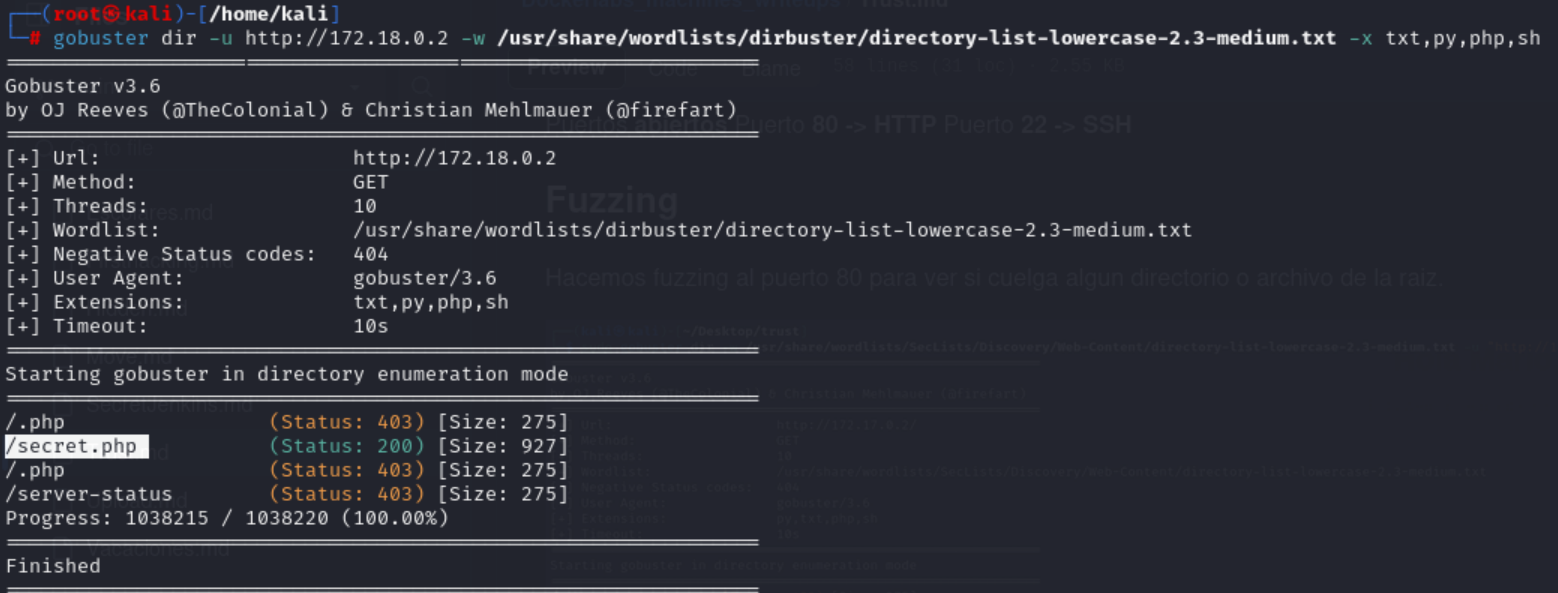




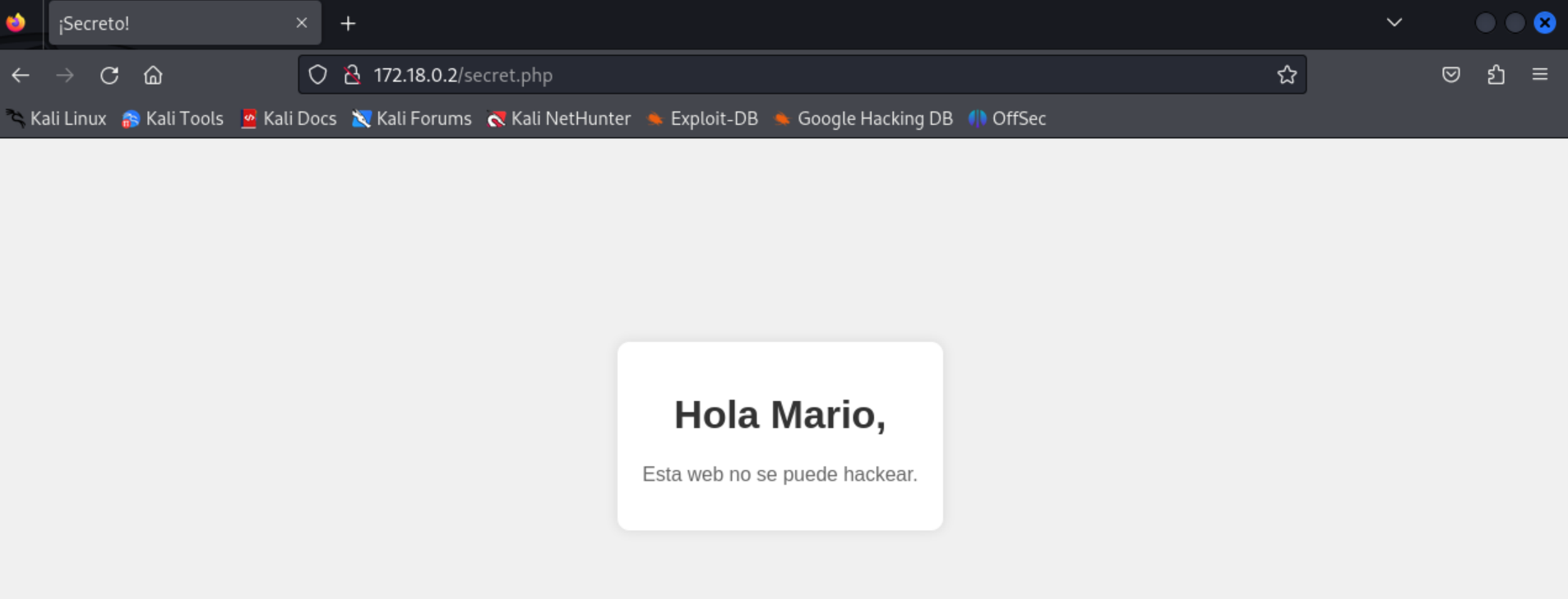
1. Nos muestra que tenemos los puertos 22 y 80 abiertos. Abriremos el Firefox de nuestra máquina atacante y pondremos en el navegador la IP de la máquina víctima.



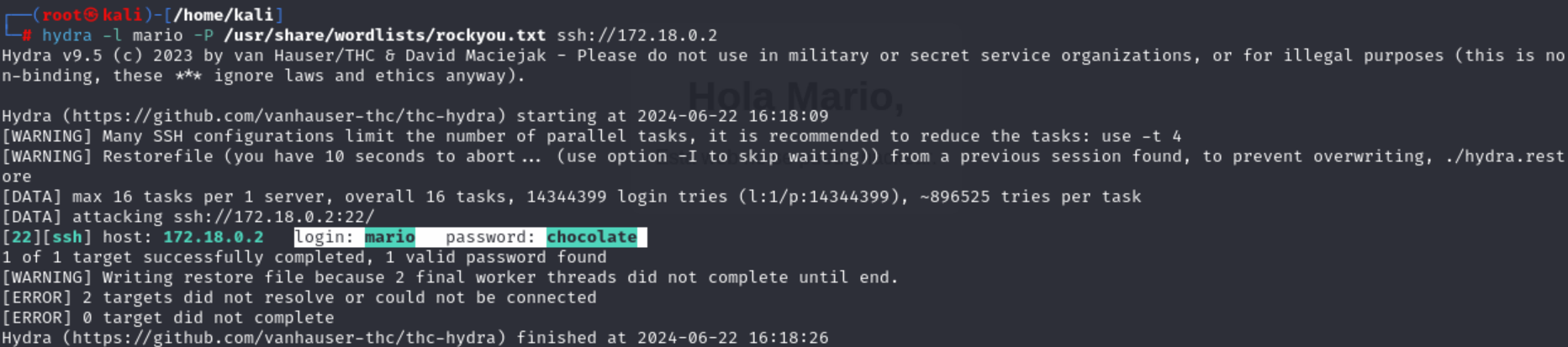
1. Vemos que por el puerto 80 corre un servidor Apache. Haremos Fuzzing con “gobuster” para ver si hay algún subdominio.



1. Agregamos el subdominio “/secret.php” seguido de la IP de la máquina víctima en Firefox.

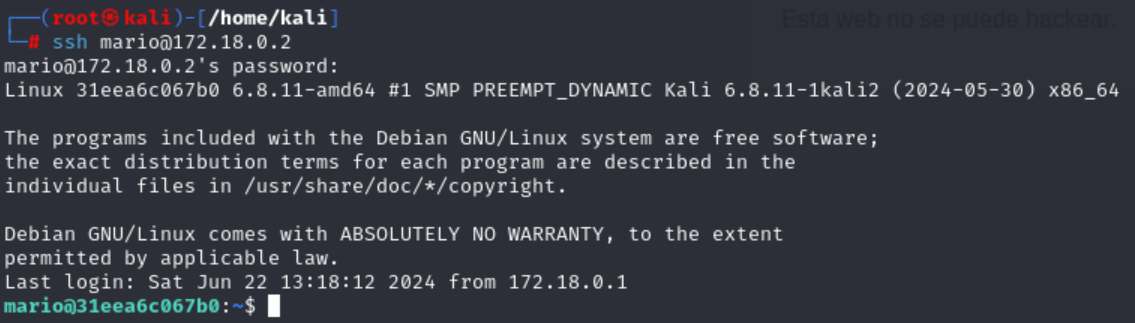


1. Descubrimos el mensaje “Hola Mario, esta web no se puede hackear.” Este mensaje nos da la pista de que Mario puede ser el usuario de la máquina, vamos a intentar hacer un ataque de fuerza bruta con “hydra” para sacar la contraseña, ya que tenemos el puerto “ssh” abierto, la IP de la máquina víctima y un posible usuario, “Mario”.



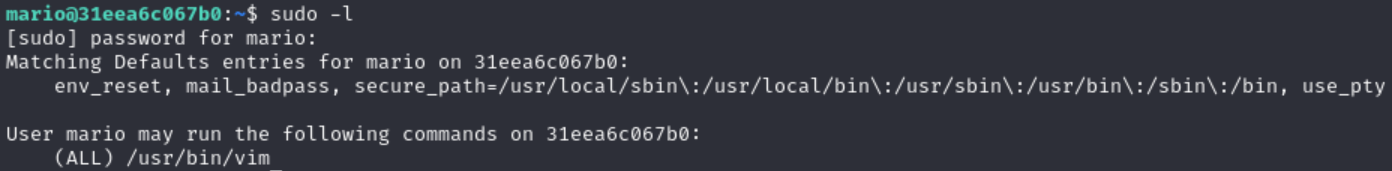


1. Una vez que tenemos el usuario y la contraseña, vamos a realizar una conexión “ssh” con la máquina víctima.

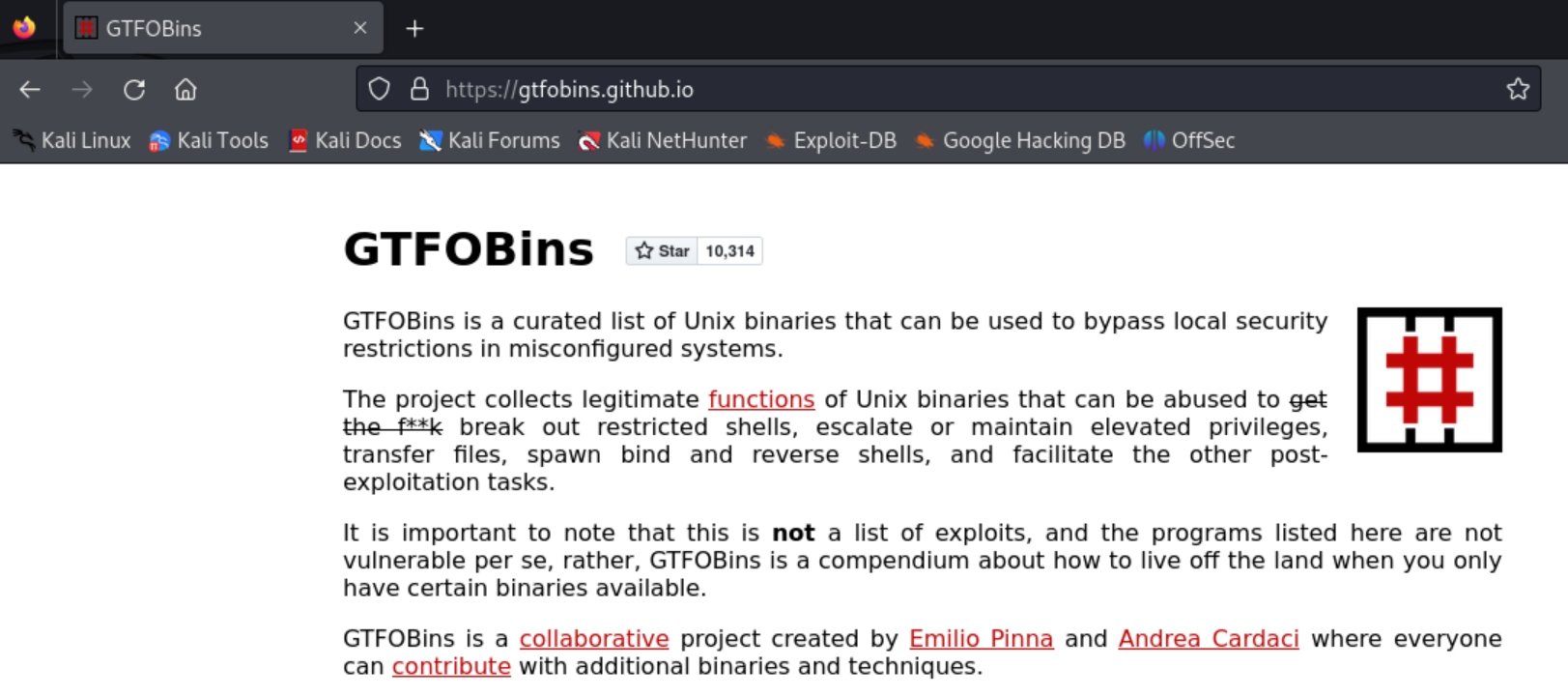


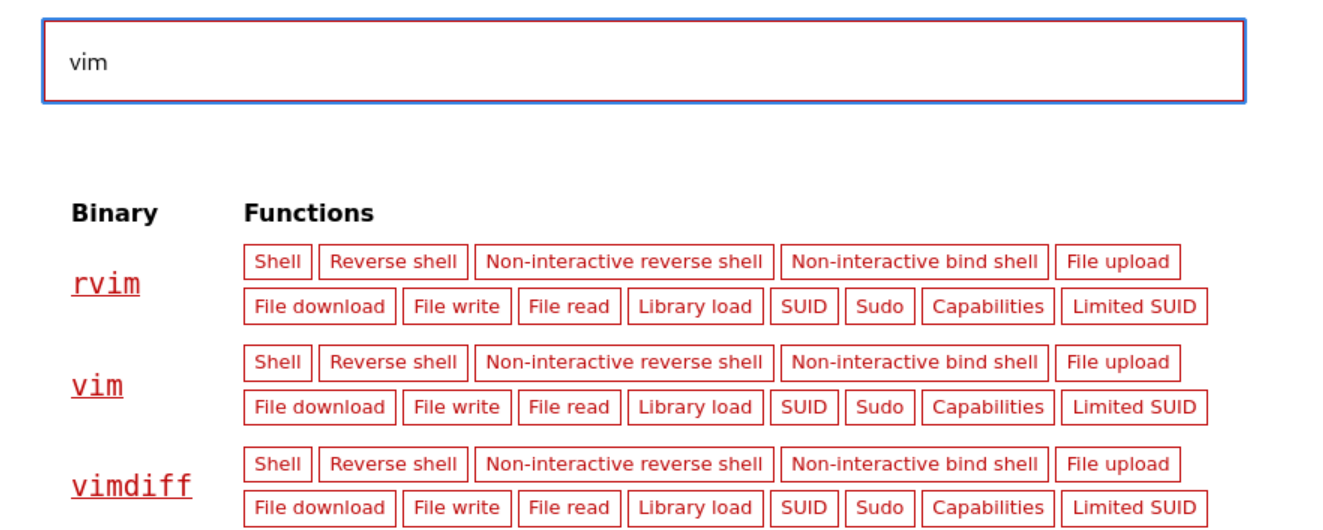


1. Ya estamos dentro de la máquina víctima. Por último, vamos a intentar escalar privilegios para pasar de usuario normal a root. Para ello vamos a buscar binarios con el comando “sudo -l”.

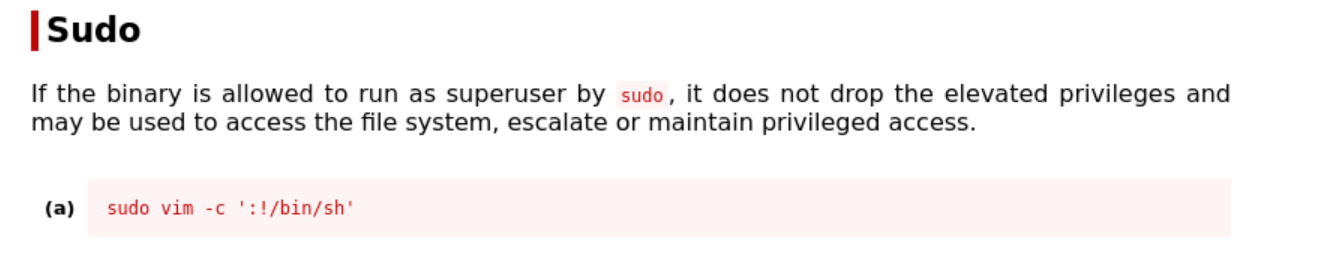


9-Con la ruta absoluta “/usr/bin/vim” podemos escalar privilegios. Entramos en la página “GTFOBins” en nuestro navegador y escribimos el último directorio de la anterior ruta absoluta (“vim”).

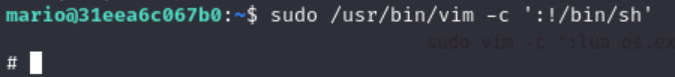




1. Vemos que se puede ascender a root por medio de SUDO.



1. Por último, introducimos en la terminal con conexión “ssh” los comandos de la página GTFOBins, pero cambiando el comando “vim” por la ruta absoluta que nos aparecía en “sudo -l”.



1. Comprobamos con el comando “whoami” si ya somos root.

