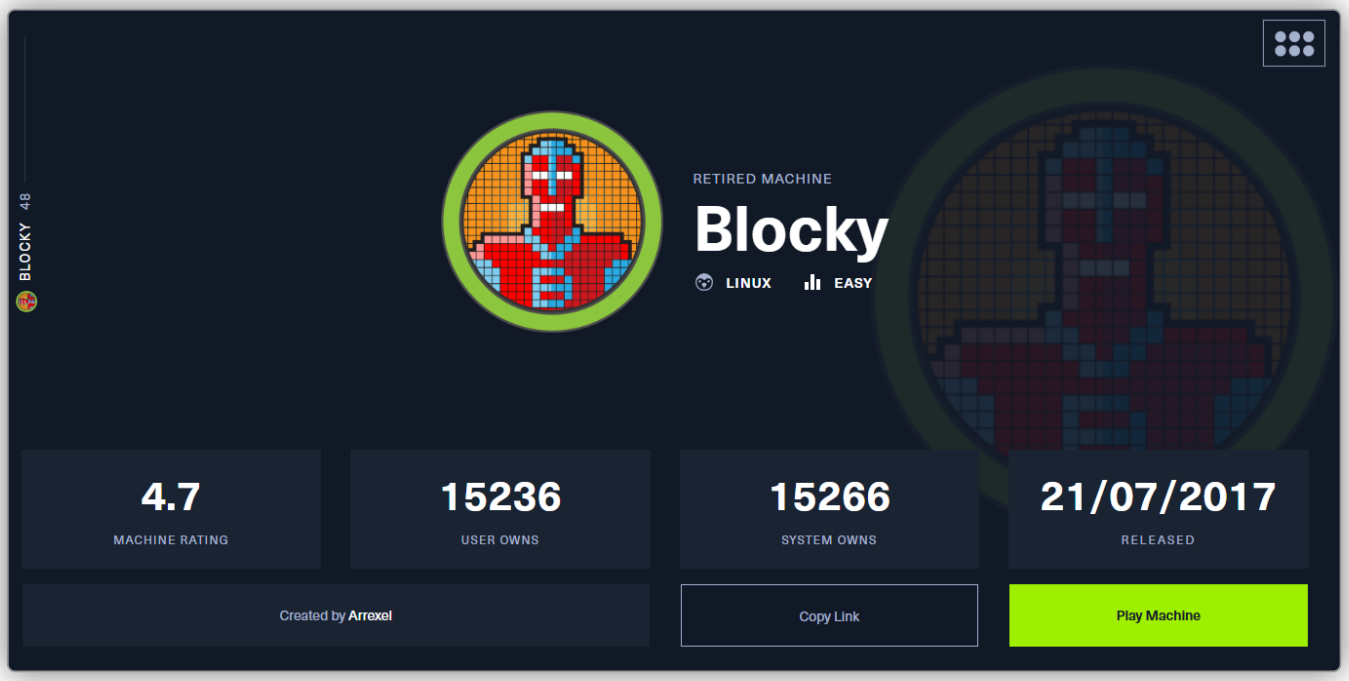
BLOCKY

1. BLOCKY

https://app.hackthebox.com/machines/Blocky

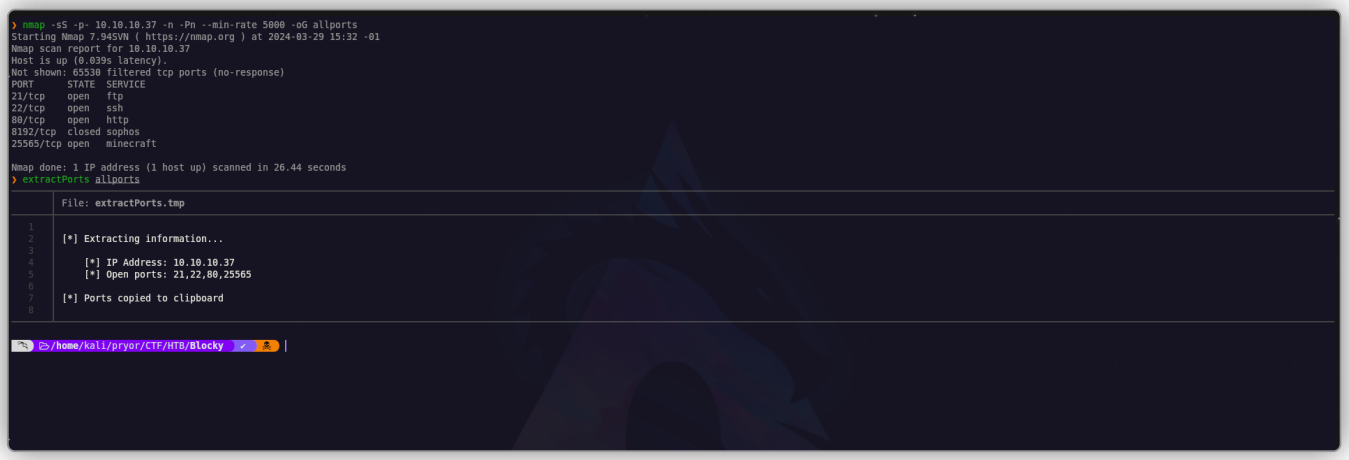


1.1. Preliminar

Comprobamos si la máquina está encendida, averiguamos qué sistema operativo es y creamos nuestro directorio de trabajo. Nos enfrentamos a una máquina *Linux*.

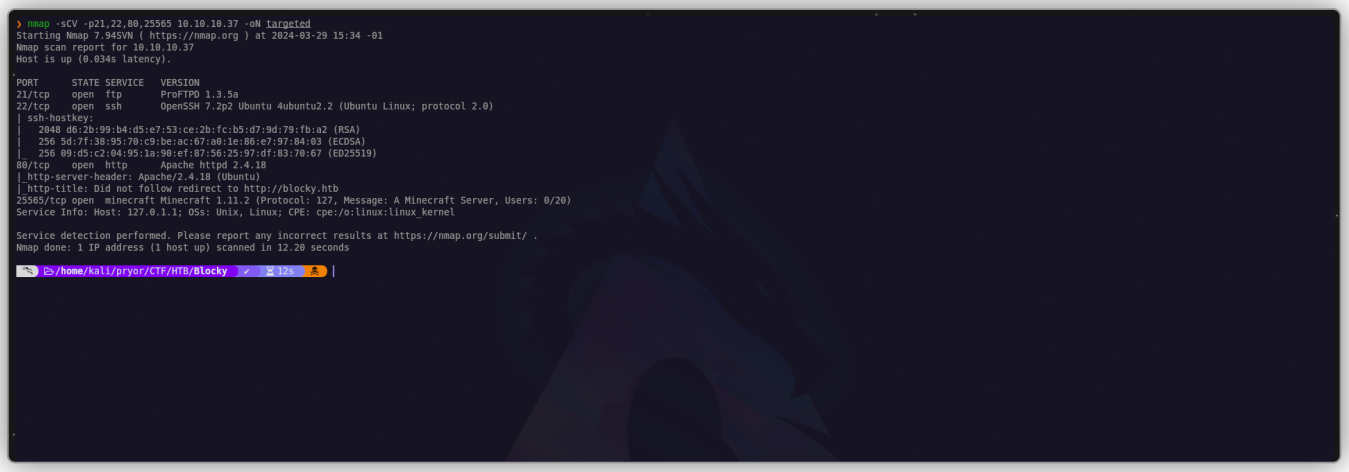
1.2. Nmap

Escaneo de puertos sigiloso. Evidencia en archivo *allports*. Tenemos, entre otros puertos: *21, 22 y 80* abiertos.



Escaneo de scripts por defecto y versiones sobre los puertos abiertos, tomando como input los puertos de *allports* mediante `extractPorts`. Curiosamente, tenemos *Minecraft 1.11.2* corriendo en un puerto. Añadimos el dominio *blocky.htb* a nuestro

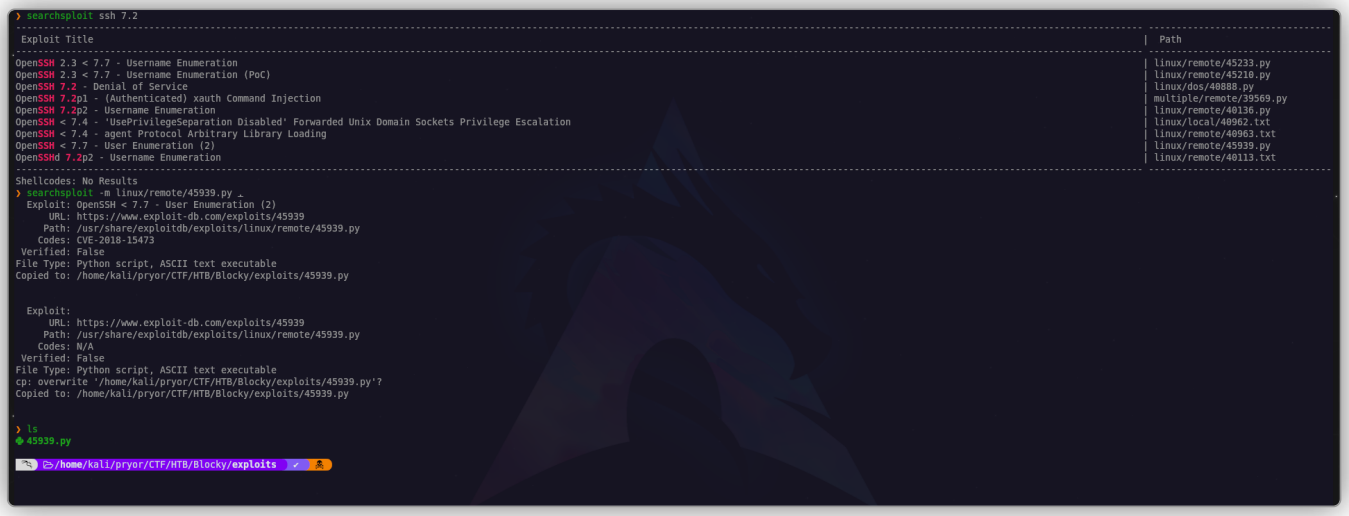
/etc/hosts para poder acceder desde el navegador.



1.3. SSH user enumeration

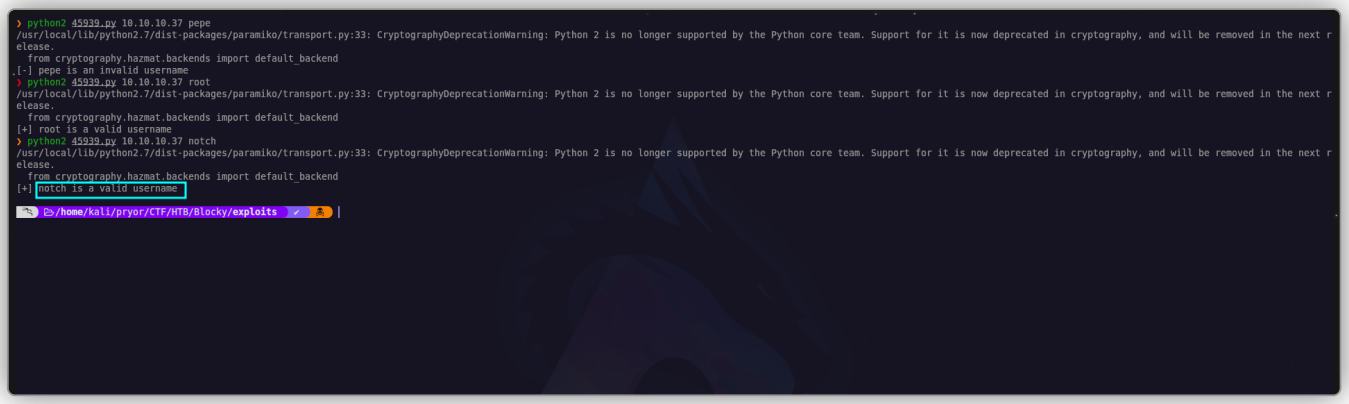
CVE-2018-15473:

Ya que tenemos *OpenSSH 7.2.p2*, que es una versión bastante obsoleta, podemos usar el siguiente exploit para enumerar usuarios válidos a nivel de sistema. Recordemos que las versiones vulnerables son inferiores a la *7.7*. Usamos este comando para traernos el exploit a nuestro directorio actual: `searchsploit -m linux/remote/45939.py .`.



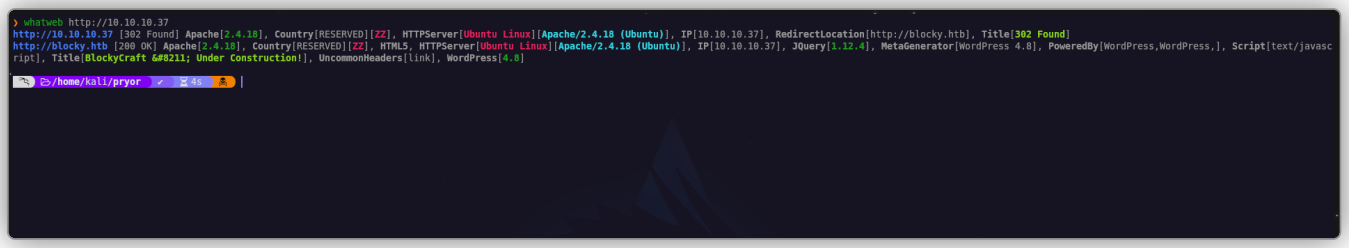
Podemos ejecutar el script, proporcionando la IP del objetivo y un usuario para comprobar si este es válido a nivel de sistema. Vemos que *root* y *notch* (creador de

Minecraft) son usuarios válidos a nivel de sistema.



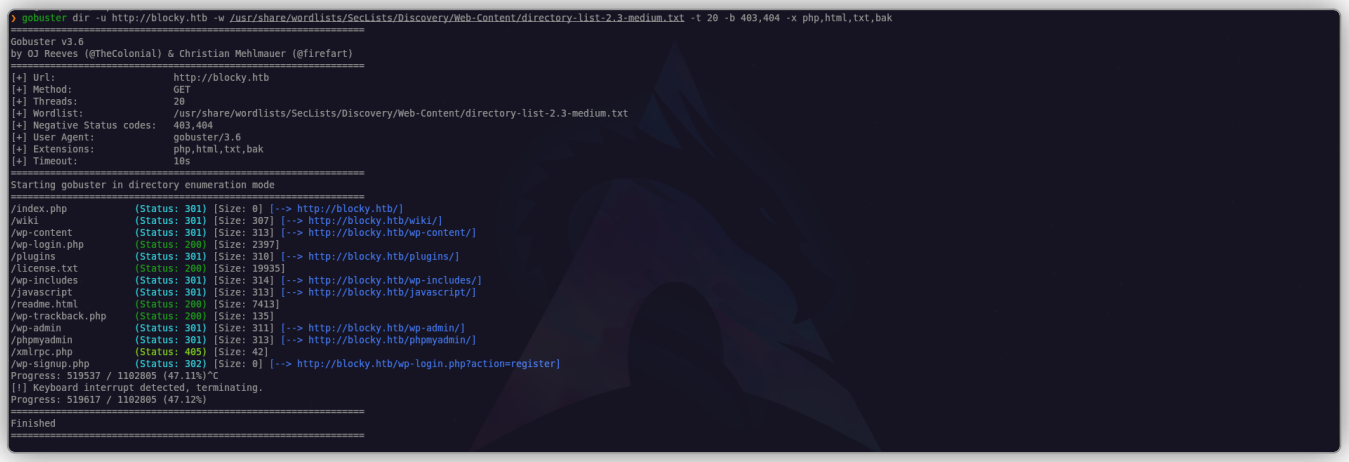
1.4. Tecnologías web

Whatweb: nos reporta lo siguiente. Entre otras cosas, vemos que nos enfrentamos a un *Wordpress 4.8*.



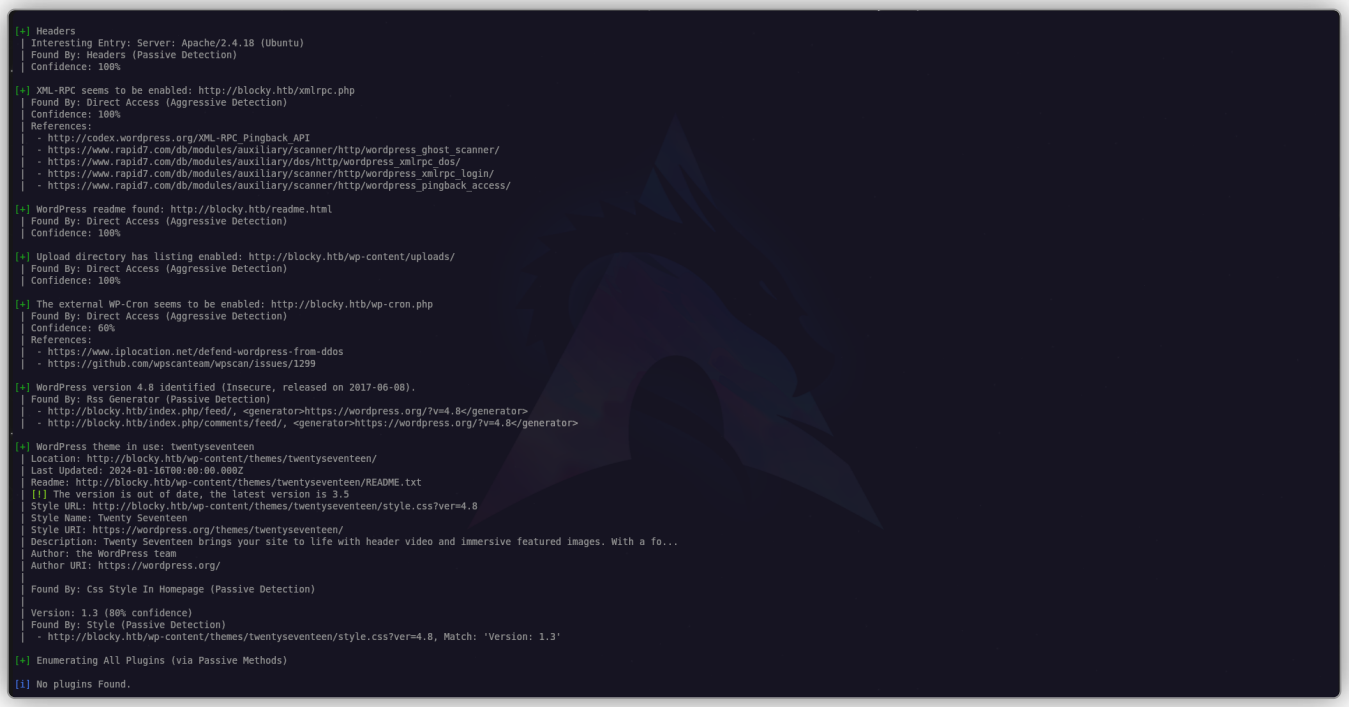
1.5. Fuzzing web

Gobuster: usamos esta herramienta para descubrir directorios. Encontramos varios directorios típicos de *Wordpress* que pueden resultar interesantes.



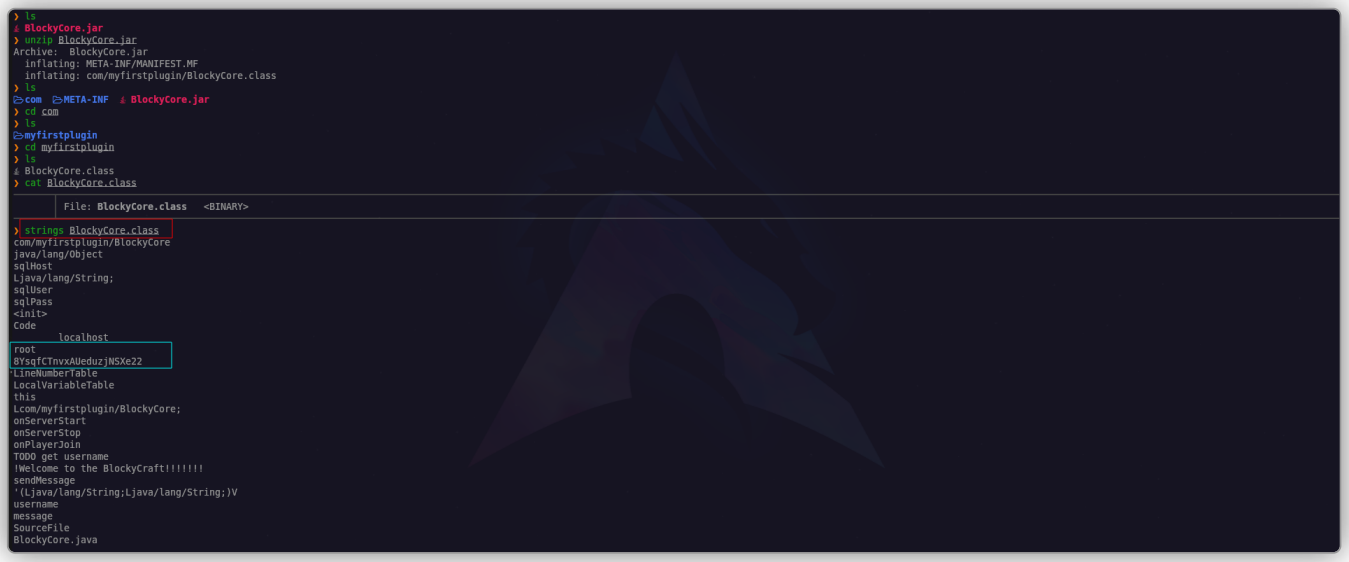
1.6. Wordpress enumeration

Wpscan: usamos esta herramienta para obtener más información sobre el CMS de Wordpress que está corriendo en el servidor. Buscamos exploits para las versiones y plugins encontrados, pero en principio, no encontramos nada relevante.

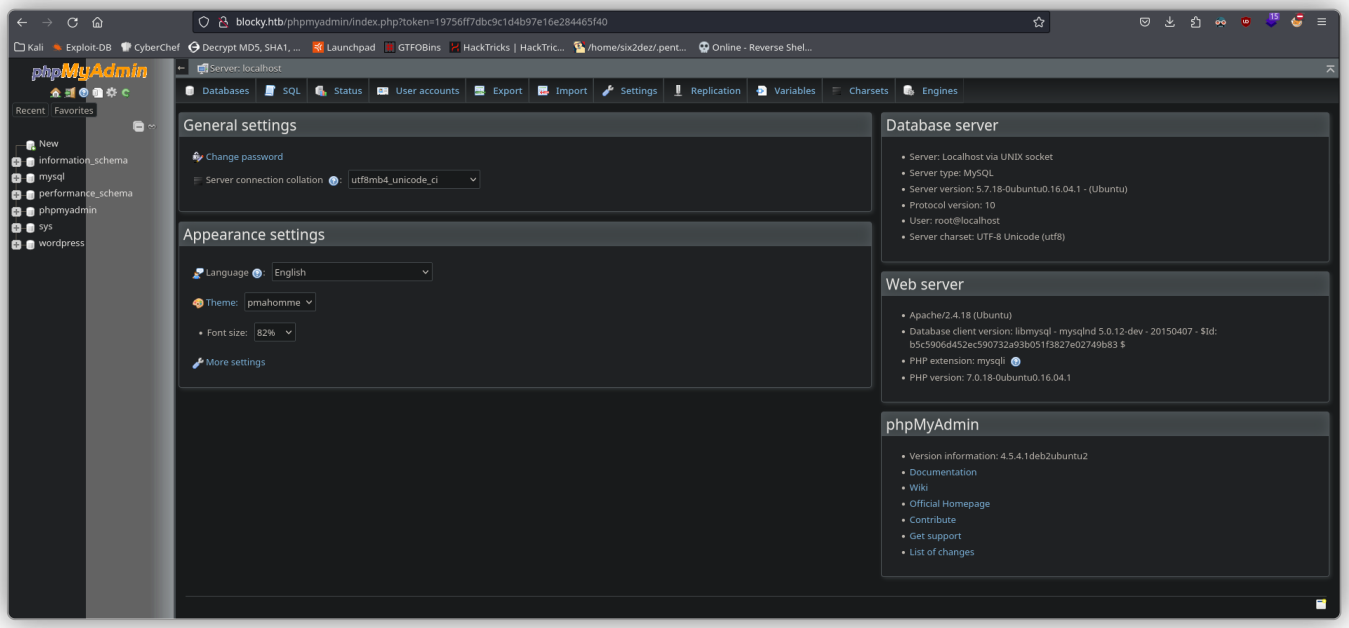


1.7. Information leakage

Tras explorar diferentes directorios, encontramos unas credenciales en un archivo llamado *BlockyCore.class*, el cual se encontraba en el directorio /plugin. Este es un archivo *.jar*, pero pudimos descomprimirlo igualmente con: `unzip BlockyCore.jar`.



Tratamos de conectarnos por SSH y FTP, pero estas credenciales resultaron ser de la base de datos MySQL, a la cual accedemos via web por /phpmyadmin. No obstante, no encontramos nada relevante en la base de datos.

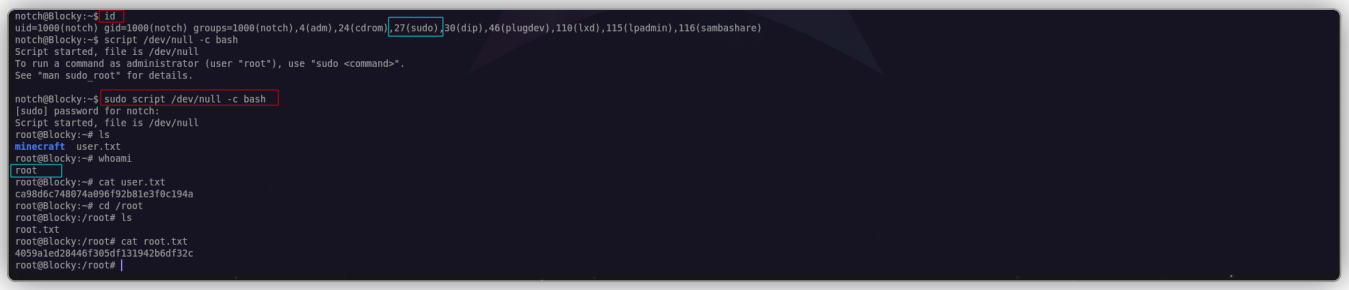


1.8. Privesc via sudo group

Buscamos otra alternativa para ganar acceso al sistema. Conseguimos acceso por SSH con el usuario *notch* y la contraseña que descubrimos previamente. Realizamos

el *tratamiento de la TTY*.

Descubrimos que estamos en el *grupo sudo*, por tanto, tan solo ejecutamos un comando y proporcionamos nuevamente la contraseña. Obtenemos acceso como **root**.



> También podríamos haber intentado escalar nuestros privilegios a través del *grupo lxd*.