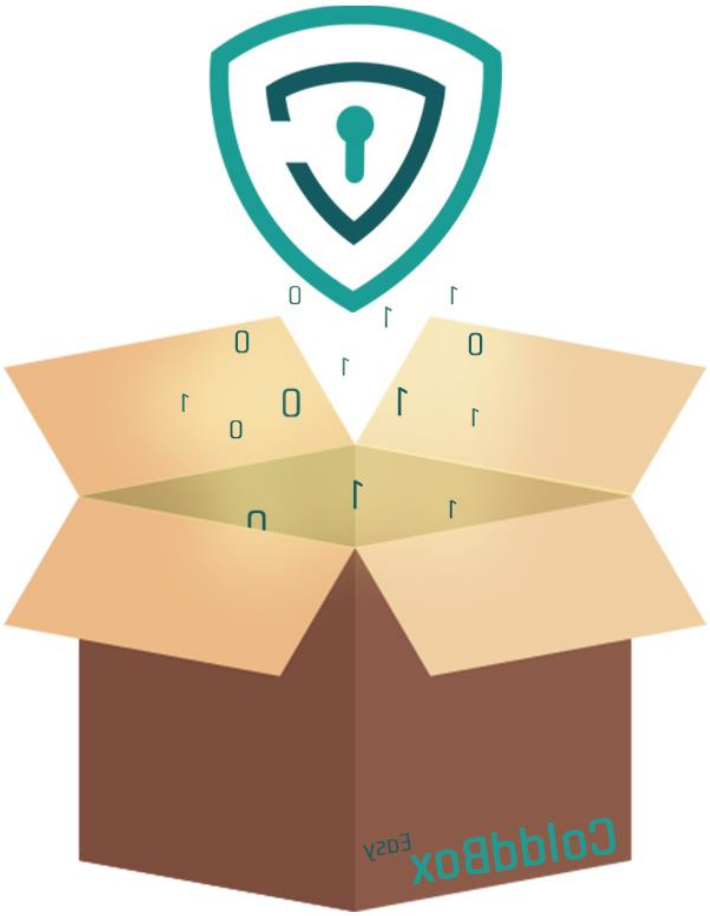
ColddBox: Easy Writeup

MrG3tty



Contents

Nmap Scan

Nmap 7.80 scan initiated Wed Jan 6 19:18:25 2021 as: nmap -v -sV -p- -oN allportsnmap.txt 10.10.219.55

Increasing send delay for 10.10.219.55 from 0 to 5 due to 572 out of 1906 dropped probes since last increase.

Nmap scan report for 10.10.219.55

Host is up (0.12s latency).

Not shown: 65522 closed ports

PORT   STATE   SERVICE   VERSION

80/tcp   open   ssl/http   Apache/2.4.18 (Ubuntu)

2098/tcp filtered dialog-port

2544/tcp filtered novell-zen

3776/tcp filtered dvcprov-port

4512/tcp open   ssh   OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)

9266/tcp filtered unknown

18932/tcp filtered unknown

25989/tcp filtered unknown

27205/tcp filtered unknown

33772/tcp filtered unknown

33890/tcp filtered unknown

35405/tcp filtered unknown

62480/tcp filtered unknown

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

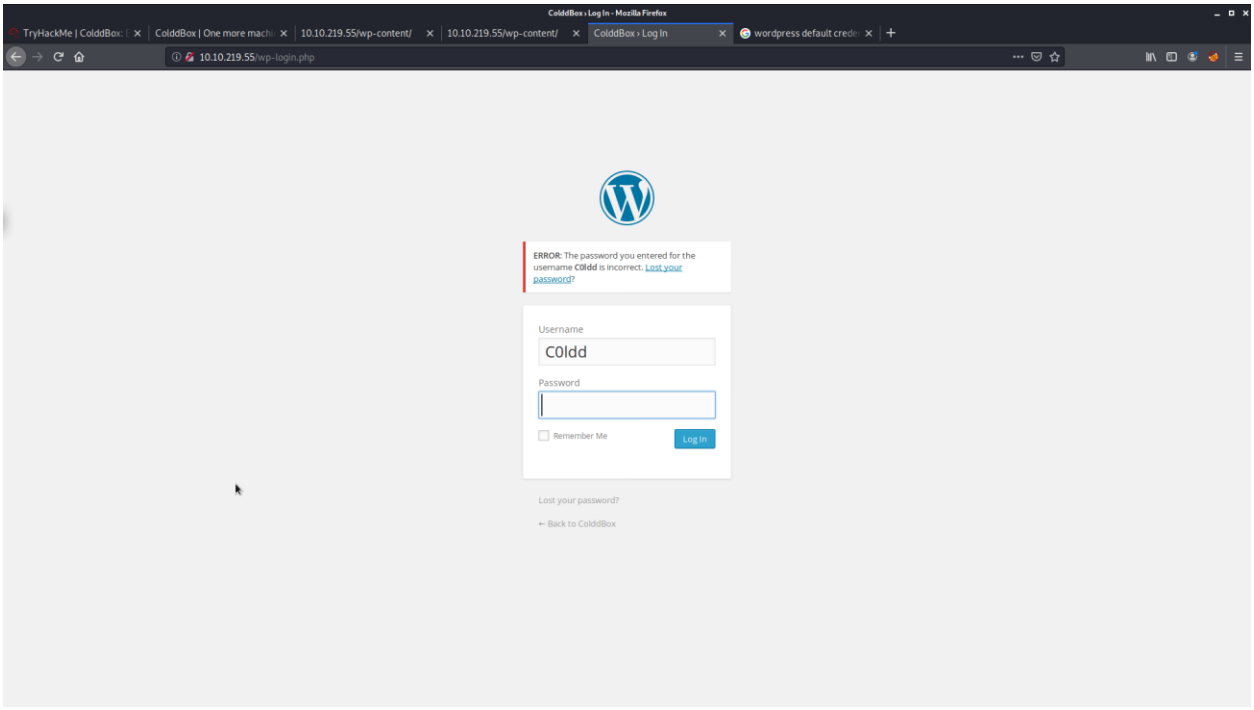
Read data files from: /usr/bin/../share/nmap

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

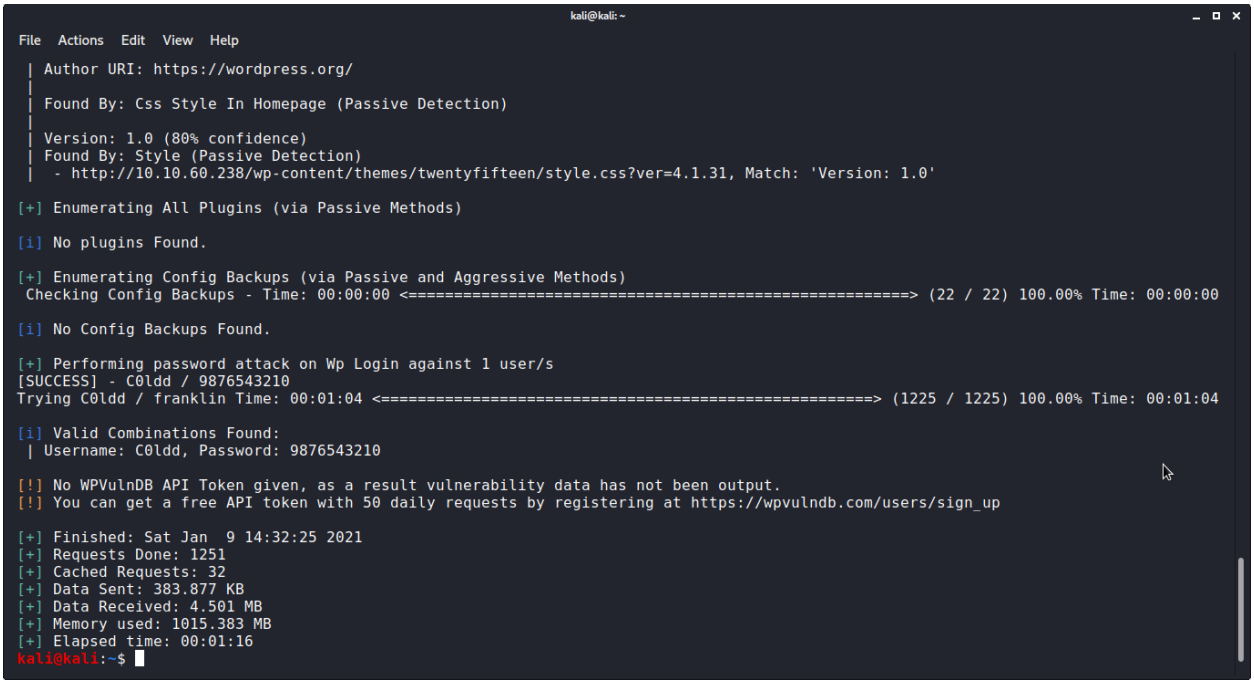
Nmap done at Wed Jan 6 19:31:41 2021 -- 1 IP address (1 host up) scanned in 796.61 seconds

Webpage Enumeration

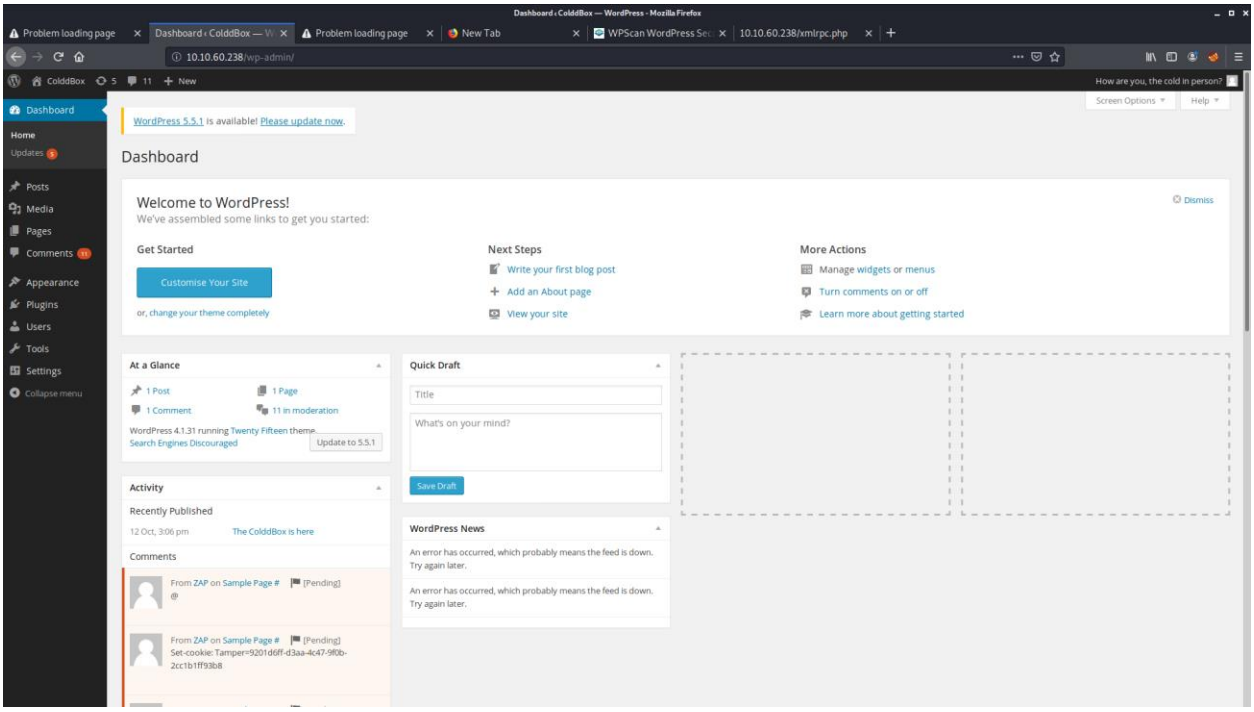
The only real interesting find here, is port 80. After running scans using a medium dirbuster wordlist in OWASP ZAP I found the wp-admin login page. After searching around on the webpage, a comment was found, I used this username in the wp-login page:



The error message that is thrown confirms that the username has been registered on the wp-admin dashboard. Using wp-scan I easily obtained credentials for this user:



After logging in, I now have access to the wp-admin dashboard.

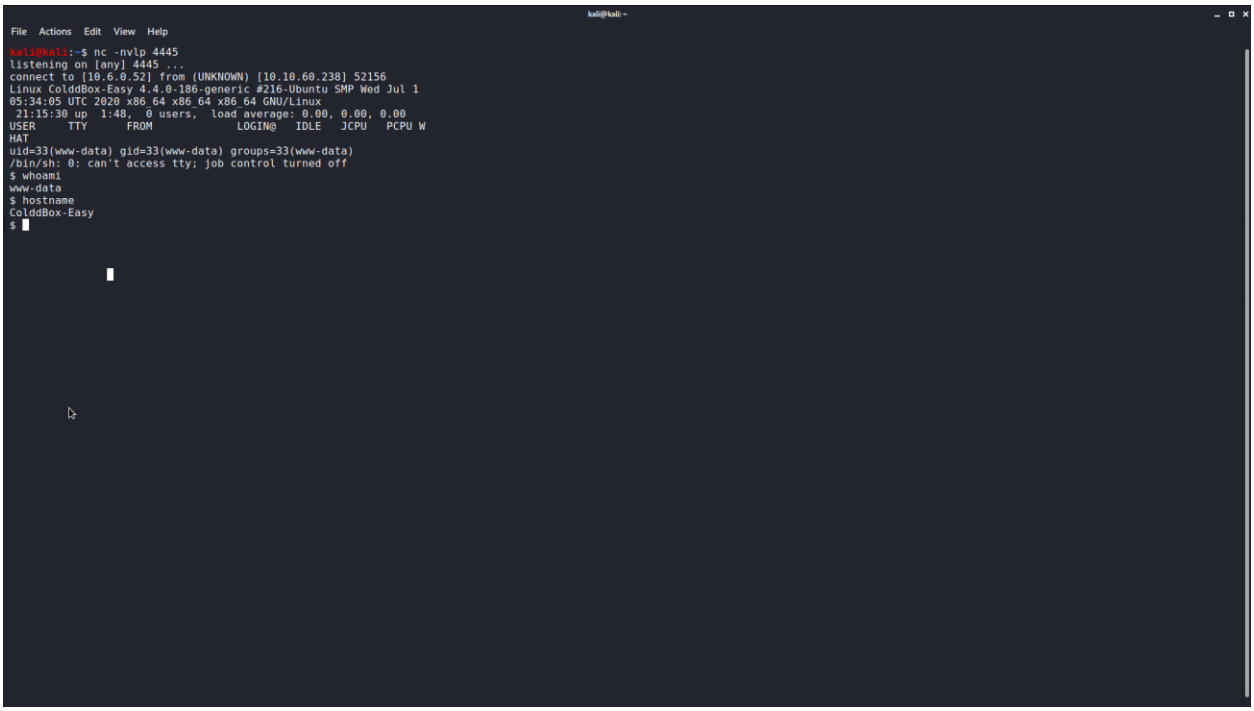


1

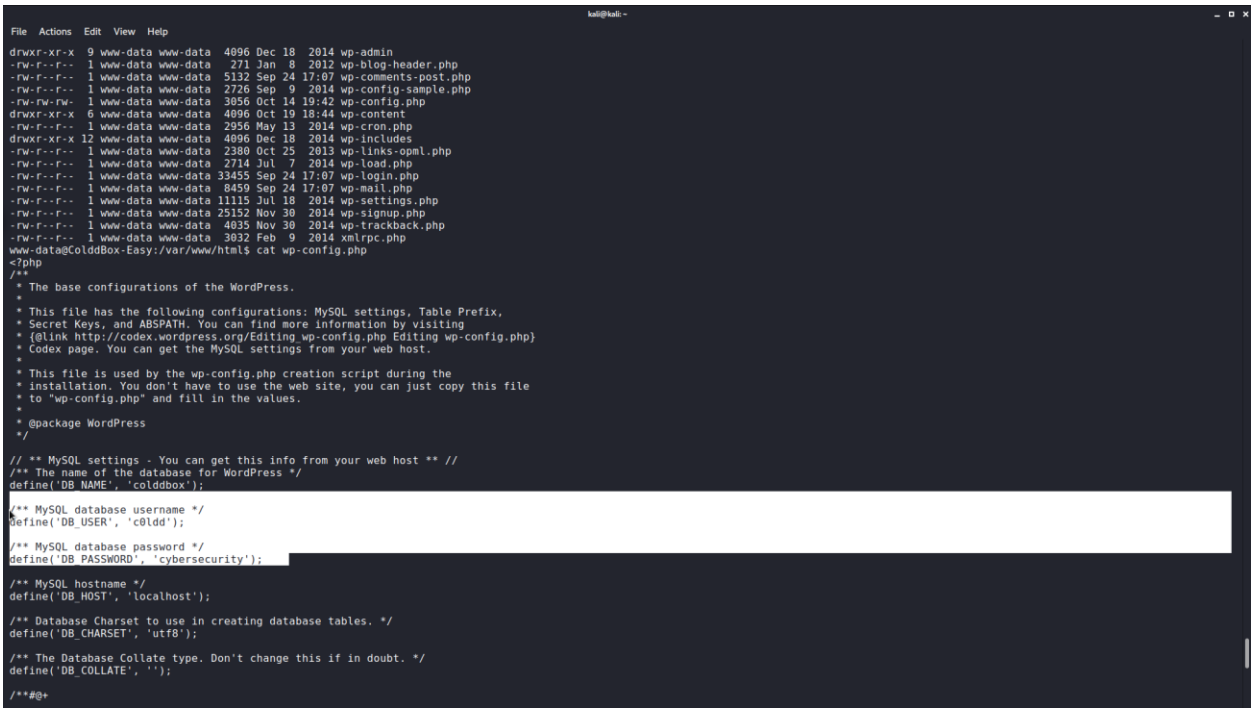
Initial foothold

By navigating to appearance, editor, 404 templates, and then inserting our own php code. After starting a netcat listener on port 4445, I then entered the directory with my malicious code, and triggered a reverse shell.

[1] https://www.hackingarticles.in/wordpress-reverse-shell/

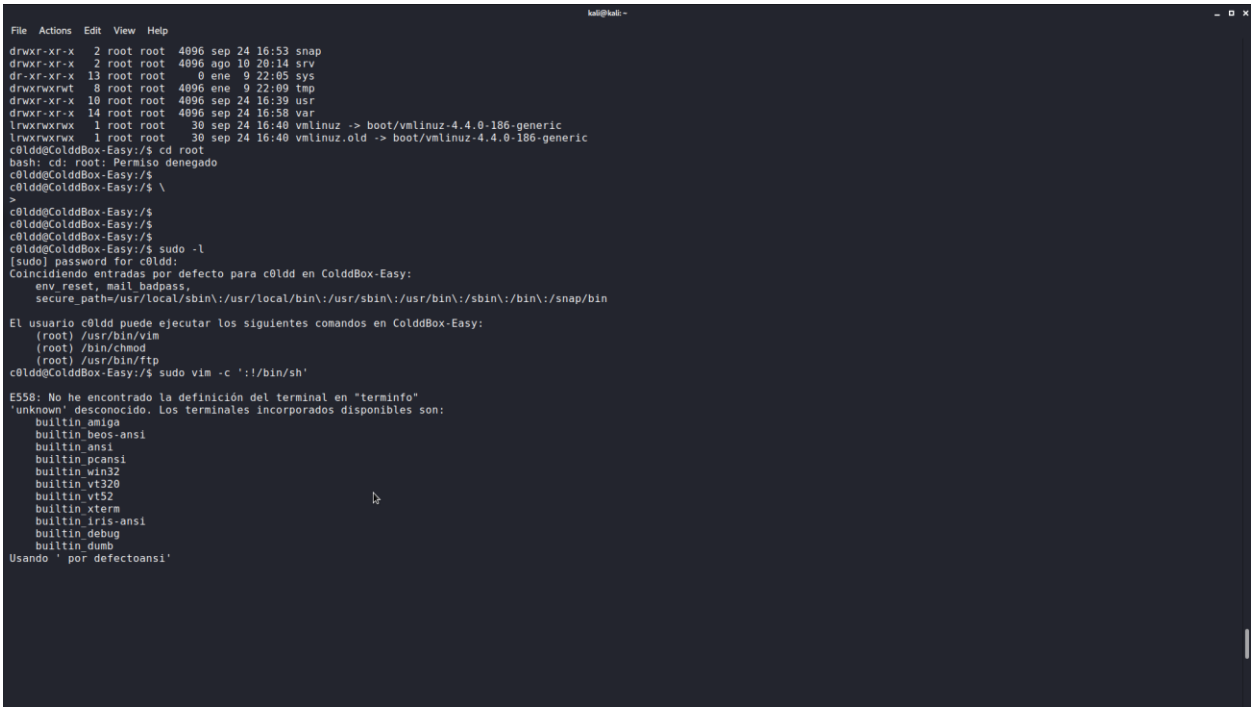


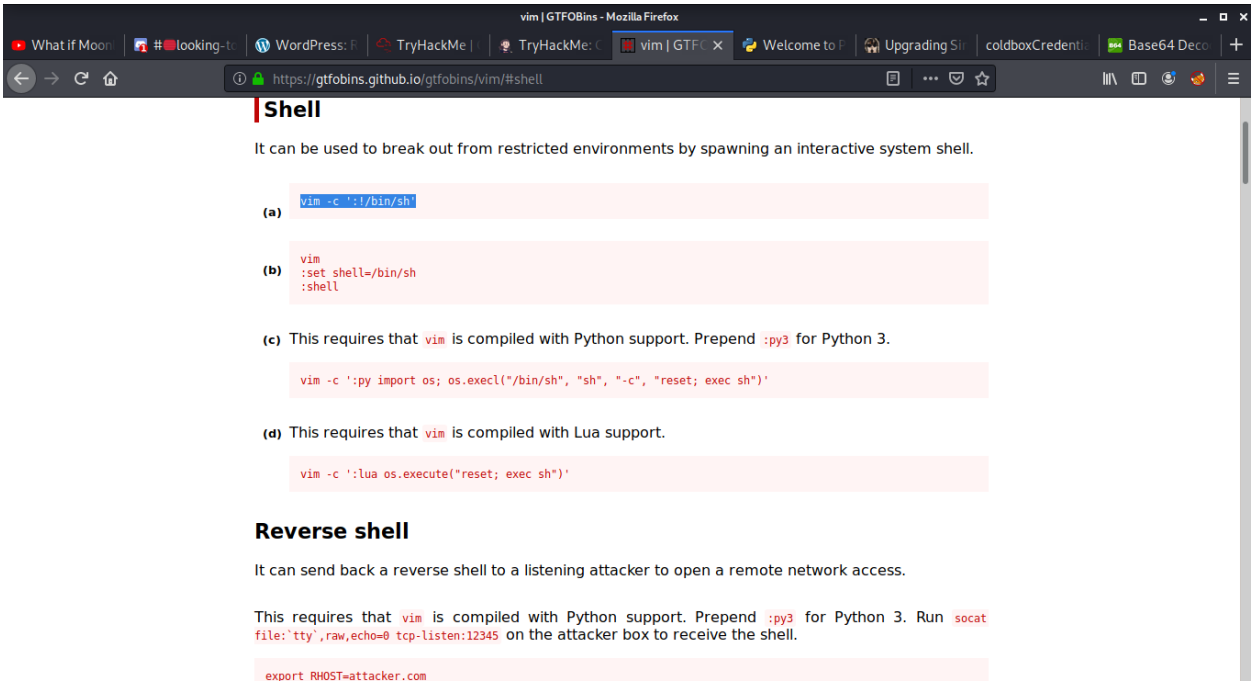
As can be seen in the screenshot, we have access to the host machine as the www-data user. As this user, our privileges are limited. After enumerating we find the coldd user. The credentials I used on the wp-admin page did not work when trying to switch to this user. After further enumeration, I was able to find the reused credentials in /var/www/html/wp-config.php

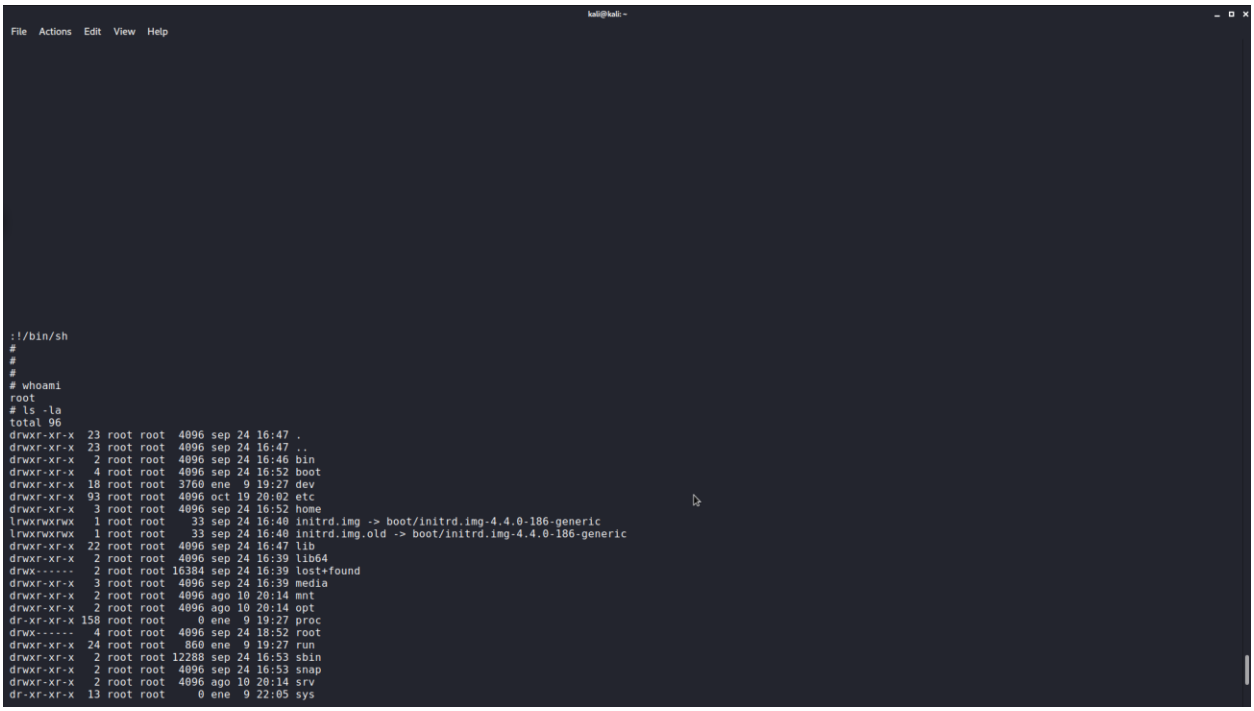


Path to Root

Once logged in the user c0ldd, its time to enumerate the user's privileges.







By running the command highlighted in gtfobins, I obtained root control over the host machine.