“死亡笔记”

主机发现

`172.16.170.54`

端口扫描

`nmap -p- -sV -sT -O 172.16.170.54`

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2
(protocol 2.0)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
MAC Address: 00:0C:29:1C:F2:B2 (VMware)
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
```

漏洞扫描

`nmap --script=vuln --min-rate=10000 172.16.170.54`

```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
|_http-stored-xss: Couldn't find any stored XSS
vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
| http-enum:
|   /wordpress/: Blog
|   /robots.txt: Robots file
|   /wordpress/wp-login.php: Wordpress login page.
|_  /manual/: Potentially interesting folder
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

尝试访问网站，需要修改dns hosts文件，使用sudo打开

首页提示，需要找到note.txt文件，还有L的评论

wordpress 使用wpscan，

wp版本 `WordPress version 5.8`

根据目录，在路径 `http://deathnote.vuln/wordpress/wp-content/uploads/2021/07/` 发现了note.txt和user.txt

getshell

```
death4
death4life
death4u
death4ever
death4all
death420
death45
death4love
death49
death48
death456
death4014
1death4u
yaydeath44
thedeath4u2
thedeath4u
stickdeath420
reddeath44
megadeath44
megadeath4
killdeath405
hot2death4sho
death4south
death4now
death4l0ve
death4free
death4elmo
death4blood
death499Eyes301
death498
death4859
death47
death4545
death445
death444
death4387n
death4332387
death42521439
death42
death4138
death411
death405
death4me
```

user.txt

```
KIRA
L
ryuk
rem
misa
siochira
light
takada
near
mello
l
kira
RYUK
REM
SIOCHIRA
LIGHT
NEAR
```

根据目标端口开放情况，和wpcms作者KIRA尝试登录ssh

轮番破解得到用户名：l 密码：death4me

提权

ssh登录，发现ook

```
++++++++++[>+>+++>+++++++>++++++++++<<<<-]>>>>+++++.
<<++.>>++++++++++.------------.+.+++++.---.
<<.>>++++++++++.<<.>>--------------.++++++++.+++++.<<.>>.-
-----------.---.<<.>>+++++++++++++++.-----------.--
-.+++++++..<<.++++++++++++.------------.>>---------
-.++++++++++++++++++.-.<<.>>+++++.----------.++++++.
<<.>>++.--------.-.++++++.<<.>>------------------.+++.
<<.>>----.+.++++++++++.-------.<<.>>++++++++++++++++.-----.
<<.>>----.--.+++..<<.>>+.--------.
<<.++++++++++++++.>>+++++++.--.+++++++++.-----------------.
```

解密得到：

```
i think u got the shell , but you wont be able to kill me
-kir
```

没什么用

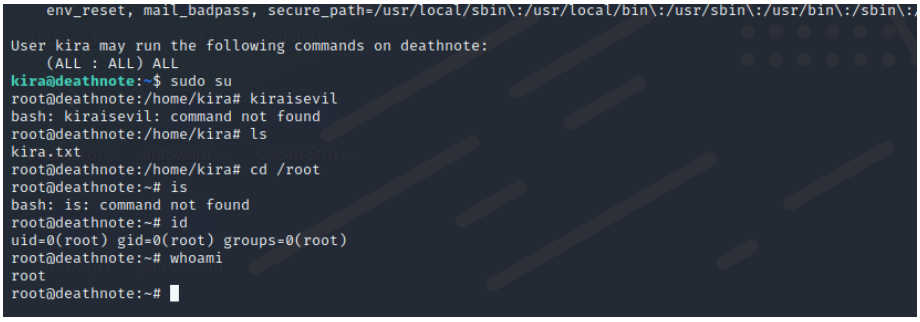
查找文件在/opt/L/下找到提示使用cyberchef

case.wav

```
6347467a6333646b49446f6761326c7959576c7a5a585a706243413d

cGFzc3dkIDoga2lyYWlzZXZpbCA=

kiraisevil
```



切换到kira再sudo su得到shell

root