

系统安全平台第九次作业

第一题

1.寻找特权程序 (50分)

题目描述:

利用Guacamole登录到操作机中, 账号为学生姓名, 密码为学生一卡通号。

靶机配置了ssh, 可以账号test、密码123通过ssh登录到靶机进行攻击。(靶机IP地址见题目中网络拓扑图)

在Linux系统中文件的权限是很重要的。通常的权限由读、写、执行三位组成。对每个文件都指定了文件所有者、同用户组的权限和其它非本用户组的权限。同时Linux中还有特殊的suid、sgid权限。设置了suid/sgid权限的文件, 任何用户在执行该文件时, 都将拥有文件属主/属组账号对应的权限。

在靶机环境中, 设置有一个属于root用户, 同时设置了suid权限的文件, 只需要找到它并执行即可获取flag。

答案:

已生成虚拟环境

前往远程桌面

删除虚拟环境

倒计时: 0 小时, 59 分钟, 55 秒



老规矩, 还是 ssh 登录靶机。

```
Terminal - root@1429f0fc9c7a:~
File Edit View Terminal Tabs Help
ECDSA key fingerprint is MD5: c3: 90: b1: 3f: 86: 0e: 4e: b1: 75: d5: a7: 3d: af: 20: 48: 1e.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '1.0.82.3' (ECDSA) to the list of known hosts.
test@1.0.82.3's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 4.4.0-146-generic x86_64)

* Documentation:  https://help.ubuntu.com/

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

test@1517694f9090: ~$
```

根据题目提示, 用 find 扫一下特权程序。

```
Terminal - root@1429f0fc9c7a:~  
File Edit View Terminal Tabs Help  
test@1517694f9090: ~$ find / -perm -u=s -type f  
/bin/mount  
/bin/ping  
/bin/ping6  
/bin/su  
/bin/umount  
/etc/super  
find: '/etc/ssl/private': Permission denied  
find: '/proc/tty/driver': Permission denied  
find: '/proc/1/task/1/fd': Permission denied  
find: '/proc/1/task/1/fdinfo': Permission denied  
find: '/proc/1/task/1/ns': Permission denied  
find: '/proc/1/fd': Permission denied  
find: '/proc/1/map_files': Permission denied  
find: '/proc/1/fdinfo': Permission denied  
find: '/proc/1/ns': Permission denied  
find: '/proc/7/task/7/fd': Permission denied  
find: '/proc/7/task/7/fdinfo': Permission denied  
find: '/proc/7/task/7/ns': Permission denied  
find: '/proc/7/task/10/fd': Permission denied  
find: '/proc/7/task/10/fdinfo': Permission denied  
find: '/proc/7/task/10/ns': Permission denied  
find: '/proc/7/task/11/fd': Permission denied
```

发现“/etc/super”，运行一下即可。

```
Terminal - root@1429f0fc9c7a:~  
File Edit View Terminal Tabs Help  
find: '/proc/59/task/59/ns': Permission denied  
find: '/proc/59/fd': Permission denied  
find: '/proc/59/map_files': Permission denied  
find: '/proc/59/fdinfo': Permission denied  
find: '/proc/59/ns': Permission denied  
find: '/proc/68/task/68/fd/5': No such file or directory  
find: '/proc/68/task/68/fdinfo/5': No such file or directory  
find: '/proc/68/fd/5': No such file or directory  
find: '/proc/68/fdinfo/5': No such file or directory  
find: '/root': Permission denied  
/usr/bin/chfn  
/usr/bin/chsh  
/usr/bin/gpasswd  
/usr/bin/newgrp  
/usr/bin/passwd  
/usr/bin/sudo  
/usr/lib/eject/dmccrypt-get-device  
/usr/lib/openssh/ssh-keysign  
find: '/var/cache/ldconfig': Permission denied  
find: '/var/spool/cron/crontabs': Permission denied  
find: '/var/spool/rsyslog': Permission denied  
test@1517694f9090: ~$ /etc/super  
Success! Your flag is :72263304  
@test@1517694f9090: ~$
```

第二题

2.密码提示破解密码 (50分)

题目描述:

寻找特权程序, 然后执行该程序, 根据执行的程序提示获取flag

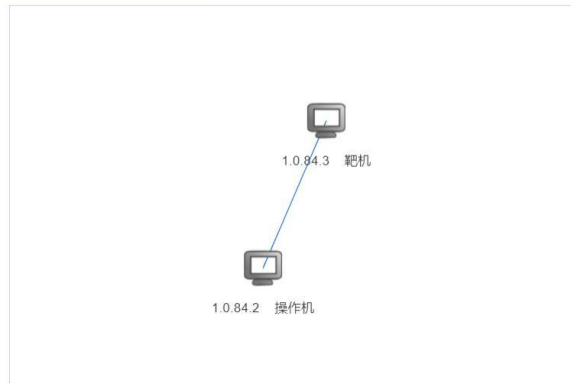
答案:

已生成虚拟环境

前往远程桌面

删除虚拟环境

① 倒计时: 0 小时, 59 分钟, 54 秒



ssh 登录靶机。

```
Terminal - root@351a81d0bd53:~
File Edit View Terminal Tabs Help
ECDSA key fingerprint is MD5: 45: e7: ce: e0: 12: 96: 35: e5: 9a: 25: 1a: ee: 9c: 71: 0c: b0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '1.0.84.3' (ECDSA) to the list of known hosts.
test@1.0.84.3's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 3.10.0-957.21.3.el7.x86_64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

test@f7885d4e4f92: ~$ ls
__pycache__  build  dist  flag.txt  test.py  test.spec
test@f7885d4e4f92: ~$
```

看一下文件目录, 和之前做过的题型相似。

```
Terminal - root@351a81d0bd53:~  
File Edit View Terminal Tabs Help  
ECDSA key fingerprint is MD5: 45: e7: ce: e0: 12: 96: 35: e5: 9a: 25: 1a: ee: 9c: 71: 0c: b0.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '1.0.84.3' (ECDSA) to the list of known hosts.  
test@1.0.84.3's password:  
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 3.10.0-957.21.3.el7.x86_64 x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/advantage  
This system has been minimized by removing packages and content that are  
not required on a system that users do not log into.  
  
To restore this content, you can run the 'unminimize' command.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
test@f7885d4e4f92:~$ ls  
__pycache__ build dist flag.txt test.py test.spec  
test@f7885d4e4f92:~$
```

还是先用 find 扫一下特权程序，发现了可执行程序目录
“/home/test/dist/test”。

```
Terminal - root@351a81d0bd53:~  
File Edit View Terminal Tabs Help  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
  
test@f7885d4e4f92:~$ ls  
__pycache__ build dist flag.txt test.py test.spec  
test@f7885d4e4f92:~$ find / -perm -u=s -type f  
/bin/mount  
/bin/su  
/bin/umount  
find: /etc/ssl/private: Permission denied  
/home/test/dist/test  
find: /proc/tty/driver: Permission denied  
find: /proc/1/task/1/fd: Permission denied  
find: /proc/1/task/1/fdinfo: Permission denied  
find: /proc/1/task/1/ns: Permission denied  
find: /proc/1/fd: Permission denied  
find: /proc/1/map_files: Permission denied  
find: /proc/1/fdinfo: Permission denied  
find: /proc/1/ns: Permission denied  
find: /proc/7/task/7/fd: Permission denied  
find: /proc/7/task/7/fdinfo: Permission denied  
find: /proc/7/task/7/ns: Permission denied  
find: /proc/7/task/10/fd: Permission denied  
find: /proc/7/task/10/fdinfo: Permission denied
```

看一下 test.py 的内容，发现运行后需要输入一个数字，模 3 余数为
0 时可得到 flag。

A screenshot of a terminal window titled "Terminal - root@351a81d0bd53:~". The window has a menu bar with "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal displays Python code for a number guessing game. The code imports 'os' and 'sys', uses a try-except block to handle input errors, and attempts to open a file at "/root/.flag.txt". The status bar at the bottom shows the filename "test.py" as read-only, with line 14 and column 17 highlighted. The cursor is positioned at the end of the last line of code.

```
import os
import sys

try:
    temp = input('input a number:')
    guess = int(temp)
    if (guess%3) != 0:
        print('input another one')
    else:
        f=open("/root/.flag.txt",'r')
        a=f.read()
        print(a)
except:
    print('buzhidao')
```

"test.py" [readonly] 14L, 17C

```
Terminal - root@351a81d0bd53:~
File Edit View Terminal Tabs Help

find: /proc/238/fd': Permission denied
find: /proc/238/map_files': Permission denied
find: /proc/238/fdinfo': Permission denied
find: /proc/238/ns': Permission denied
find: /proc/239/map_files': Operation not permitted
find: /proc/245/task/245/fdinfo/5': No such file or directory
find: /proc/245/map_files': Operation not permitted
find: /proc/245/fdinfo/6': No such file or directory
find: /root': Permission denied
/usr/bin/chfn
/usr/bin/chsh
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/passwd
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
find: /var/cache/apt/archives/partial': Permission denied
find: /var/cache/ldconfig': Permission denied
test@f7885d4e4f92: ~$ vi test.py
test@f7885d4e4f92: ~$ ./dist/test
input a number: 3
41027792

test@f7885d4e4f92: ~$
```