

系统安全平台第一次作业

第一题

操作题 (2小题, 共100分)

1.解密flag (50分)

题目描述:

以ssh方式, 账号test, 密码123登录到靶机。通过find读取文件, 解密test.py文件的答案并执行出来获得flag

答案:

已生成虚拟环境

前往远程桌面

删除虚拟环境

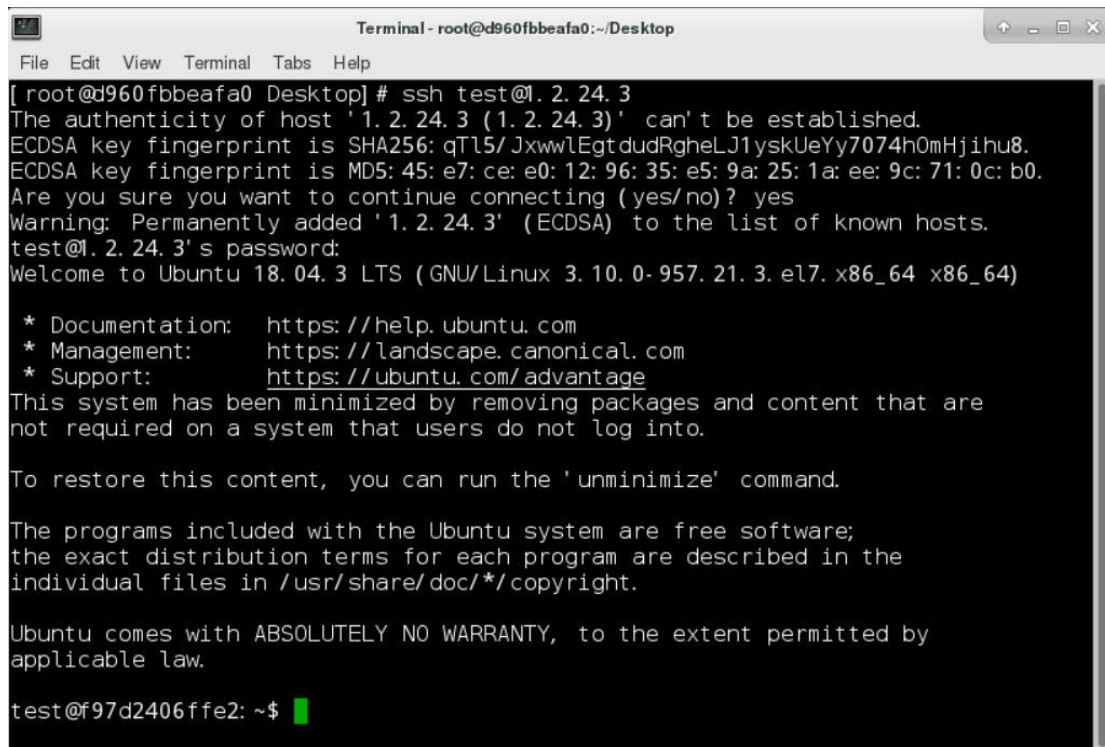
⌚ 倒计时: 0 小时, 59 分钟, 36 秒



根据提示, 利用 ssh 命令连接靶机, 格式为 “ssh 靶机名@靶机 IP”

```
Terminal - root@d960fbbeafa0:~/Desktop
File Edit View Terminal Tabs Help
[root@d960fbbeafa0 Desktop] # ssh test@1.2.24.3
The authenticity of host '1.2.24.3 (1.2.24.3)' can't be established.
ECDSA key fingerprint is SHA256: qTl5/ JxwwlEgtdudRgheLJ1yskUeYy7074h0mHjihu8.
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)? █
```

输入靶机登录密码后出现如下界面即为连接成功,可以获知靶机所使用的 Ubuntu 版本号为 18.04.3



```
Terminal - root@d960fbbefa0:~/Desktop
File Edit View Terminal Tabs Help
[root@d960fbbefa0 Desktop]# ssh test@1.2.24.3
The authenticity of host '1.2.24.3 (1.2.24.3)' can't be established.
ECDSA key fingerprint is SHA256:qTl5/JxwwLEgtdudRgheLJ1yskUeYy7074h0mHjiHu8.
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 '1.2.24.3' (ECDSA) to the list of known hosts.
test@1.2.24.3'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.

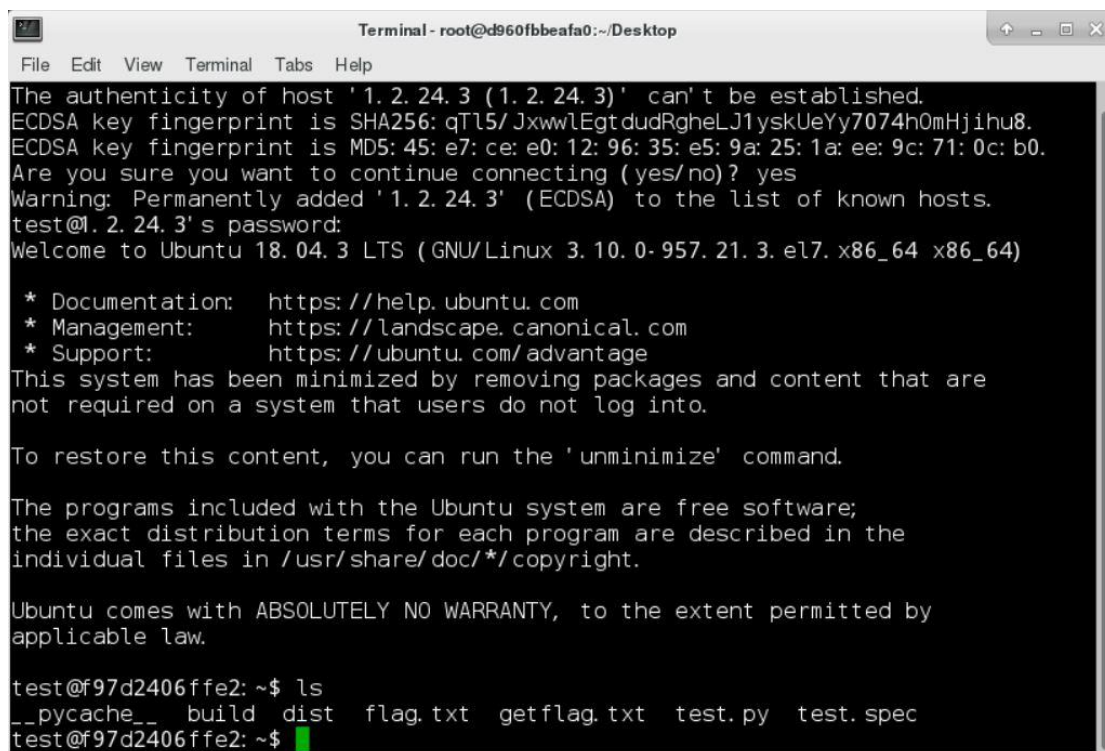
To restore this content, you can run the 'unminimize' command.

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@f97d2406ffe2:~$
```

在当前 test 目录下查看文件,可以看到题目中提到的 getflag.txt



```
Terminal - root@d960fbbefa0:~/Desktop
File Edit View Terminal Tabs Help
The authenticity of host '1.2.24.3 (1.2.24.3)' can't be established.
ECDSA key fingerprint is SHA256:qTl5/JxwwLEgtdudRgheLJ1yskUeYy7074h0mHjiHu8.
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 '1.2.24.3' (ECDSA) to the list of known hosts.
test@1.2.24.3'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@f97d2406ffe2:~$ ls
__pycache__  build  dist  flag.txt  getflag.txt  test.py  test.spec
test@f97d2406ffe2:~$
```

查看 `getflag.txt` 的内容，查找 ASCII 的对照表可知字符 1 对应的值为 49，所以 `getflag.txt` 中表达式的值为 91

[illegible]

查看 test.py 的内容，是一个猜数程序，若回答的值为 91，则会显示
“/root/flag.txt” 的内容，可能就是我们要的答案

```
Terminal - root@d960fbbeafa0:~/Desktop
File Edit View Terminal Tabs Help

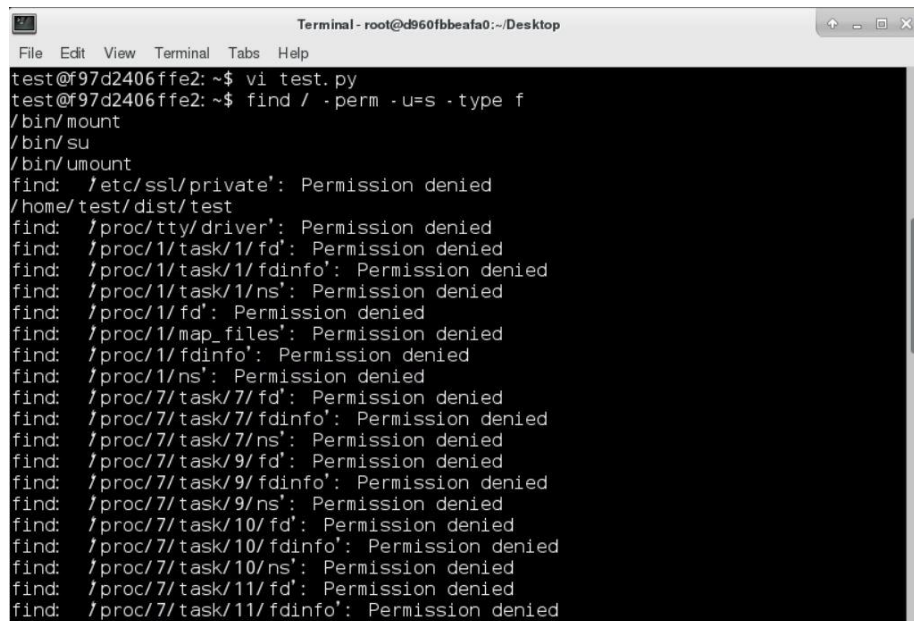
import os
import sys

try:
    temp = input('the answer of flag:')
    guess = int(temp)
    if guess != 91:
        print('answer is wrong')
    else:
        f = open("/root/flag.txt", 'r')
        a = f.read()
        print(a)
except:
    print('wrong')

~
~
~
~
~
~
~
~
~
~
~

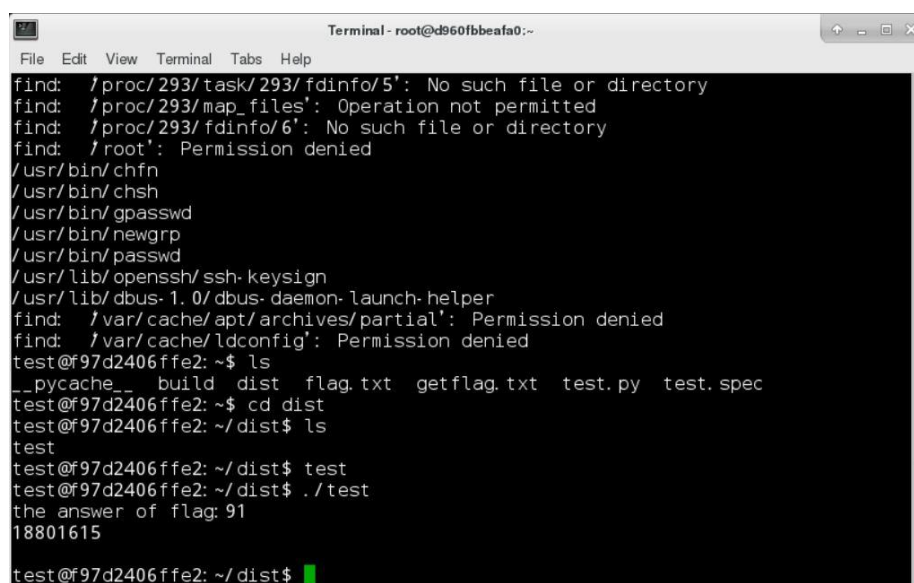
"test.py" [readonly] 14L, 221C 1.1 All
```

但是有一个问题,靶机中没有安装 python,我们也不知道 root 密码,这个 py 文件无法运行,我们看到题目中提示用 find 读取文件,于是使用命令“find / -perm -u=s -type f”查看特权程序,发现了一个特殊的路径“/home/test/dist/test”,猜测可能是我们想要的“猜数程序”



```
Terminal - root@d960fbbeafa0:~/Desktop
File Edit View Terminal Tabs Help
test@97d2406ffe2: ~$ vi test.py
test@97d2406ffe2: ~$ 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/9/fd': Permission denied
find: '/proc/7/task/9/fdinfo': Permission denied
find: '/proc/7/task/9/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
find: '/proc/7/task/11/fdinfo': Permission denied
```

进入到路径下,利用“./test”运行 test 文件,根据前面的提示输入 91,即可得到 flag



```
Terminal - root@d960fbbeafa0:~/Desktop
File Edit View Terminal Tabs Help
find: '/proc/293/task/293/fdinfo/5': No such file or directory
find: '/proc/293/map_files': Operation not permitted
find: '/proc/293/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@97d2406ffe2: ~$ ls
__pycache__ build dist flag.txt getflag.txt test.py test.spec
test@97d2406ffe2: ~$ cd dist
test@97d2406ffe2: ~/dist$ ls
test
test@97d2406ffe2: ~/dist$ test
test@97d2406ffe2: ~/dist$ ./test
the answer of flag: 91
18801615
test@97d2406ffe2: ~/dist$
```

第二题

2.根据特权程序提示获取flag (50分)

题目描述:

以ssh方式, 账号test, 密码123登录到靶机。利用find指令查找特权程序。向test目录下的test.txt中写入任意两位数, 并执行特权程序, 根据返回信息推测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, 50 秒



还是以同样的方法连接靶机

```
Terminal - root@1cdb3183eb3f:~  
File Edit View Terminal Tabs Help  
ECDSA key fingerprint is MD5: b1: ea: 78: 98: d1: 22: e3: b2: fa: 92: ce: cf: 28: f0: b0: 04.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '1.2.32.3' (ECDSA) to the list of known hosts.  
test@1.2.32.3'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@b9f2b6a03c8c: ~$
```

尝试在 `test.txt` 中写入一个两位数，此处设为 10，在保存时使用“:wq!”可以越权保存

Terminal - root@1cdb3183eb3f:~

File Edit View Terminal Tabs Help

10

: wq!

继续使用 find 命令查看特权程序，发现了“/etc/en”

```
Terminal - root@1cdb3183eb3f:~
File Edit View Terminal Tabs Help

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

test@b9f2b6a03c8c: ~$ ls
prompt test.txt
test@b9f2b6a03c8c: ~$ vi test.txt
test@b9f2b6a03c8c: ~$ find / -perm -u=s -type f
/bin/mount
/bin/ping
/bin/ping6
/bin/su
/bin/umount
/etc/en
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
```


复制路径可直接运行，结果是“10 小了!”，可知是猜一个两位数，于是使用二分法在 test.txt 中修改数值

```
Terminal - root@1cdb3183eb3f:~  
File Edit View Terminal Tabs Help  
find: '/proc/88/fd': Permission denied  
find: '/proc/88/map_files': Permission denied  
find: '/proc/88/fdinfo': Permission denied  
find: '/proc/88/ns': Permission denied  
find: '/proc/92/task/92/fd/5': No such file or directory  
find: '/proc/92/task/92/fdinfo/5': No such file or directory  
find: '/proc/92/fd/5': No such file or directory  
find: '/proc/92/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@b9f2b6a03c8c: ~$ cd /etc/en  
-bash: cd: /etc/en: Not a directory  
test@b9f2b6a03c8c: ~$ /etc/en  
10小了! test@b9f2b6a03c8c: ~$
```

```
Terminal - root@1cdb3183eb3f:~  
File Edit View Terminal Tabs Help  
find: '/proc/88/fdinfo': Permission denied  
find: '/proc/88/ns': Permission denied  
find: '/proc/92/task/92/fd/5': No such file or directory  
find: '/proc/92/task/92/fdinfo/5': No such file or directory  
find: '/proc/92/fd/5': No such file or directory  
find: '/proc/92/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@b9f2b6a03c8c: ~$ cd /etc/en  
-bash: cd: /etc/en: Not a directory  
test@b9f2b6a03c8c: ~$ /etc/en  
test@b9f2b6a03c8c: ~$ vi test.txt  
test@b9f2b6a03c8c: ~$ -type f  
55大了! test@b9f2b6a03c8c: ~$
```

最终得出 33 是 flag

```
Terminal - root@1cdb3183eb3f:~  
File Edit View Terminal Tabs Help  
find: `/proc/92/task/92/fd/5': No such file or directory  
find: `/proc/92/task/92/fdinfo/5': No such file or directory  
find: `/proc/92/fd/5': No such file or directory  
find: `/proc/92/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@b9f2b6a03c8c: ~$ cd /etc/en  
-bash: cd: /etc/en: Not a directory  
test@b9f2b6a03c8c: ~$ /etc/en  
test@b9f2b6a03c8c: ~$ vi test.txt -type f  
test@b9f2b6a03c8c: ~$ /etc/en  
55大了! test@b9f2b6a03c8c: ~$ vi test.txt  
test@b9f2b6a03c8c: ~$ /etc/en  
33就是 flag! test@b9f2b6a03c8c: ~$
```