

系统安全平台第二次作业

第一题

1.端口扫描 (50分)

题目描述:

ssh test@靶机ip, 密码123登录靶机。

利用防火墙将ssh端口过滤掉后, ssh无法进入test用户, 但是在题目中又开放了返回shell的端口, 因此解题思路在于如何在外部找到test开放了哪些端口。这里需要用到nmap指令。

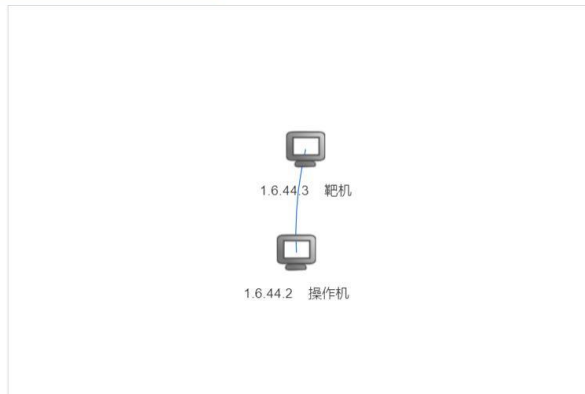
答案:

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, 27 秒



题目中说 ssh 端口被防火墙过滤掉, ssh 无法进入 test 用户, 于是先用 nmap 进行端口扫描。

使用命令: “yum install -y nmap” 下载 nmap, 同时也安装了 nc。

```
Terminal - root@34d72bfaa420:~
File Edit View Terminal Tabs Help

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

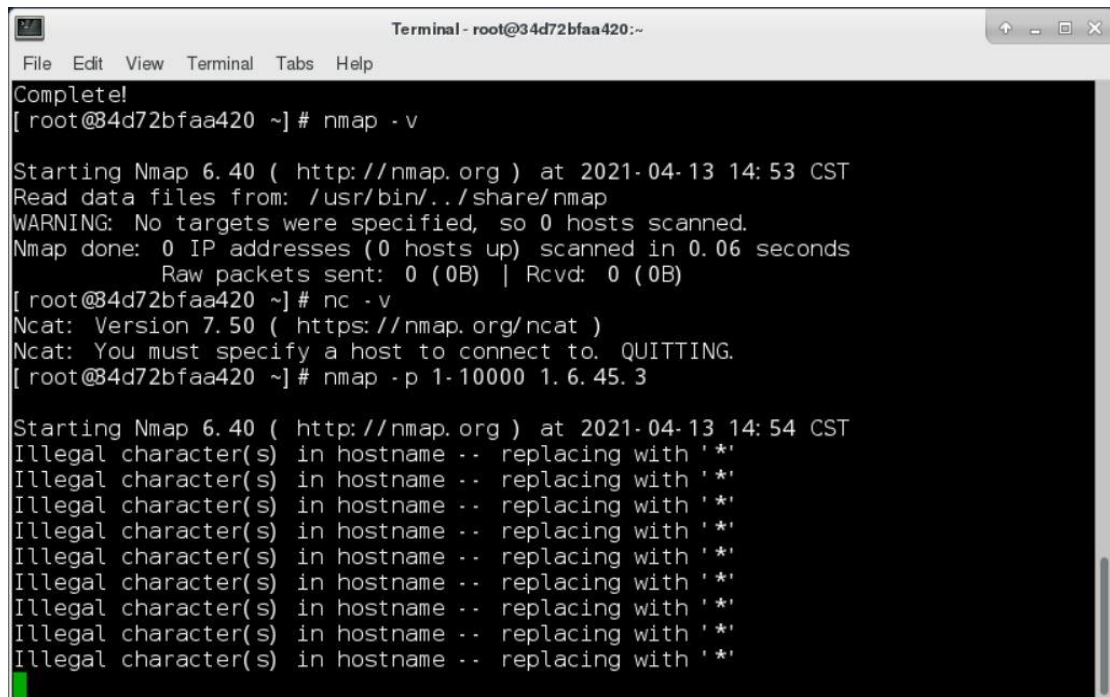
Dependency Installed:
libpcap.x86_64 14: 1.5.3-12.el7 nmap-ncat.x86_64 2: 6.40-19.el7

Complete!
[root@34d72bfaa420 ~] # nmap -v

Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-13 14:53 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@34d72bfaa420 ~] # nc -v
Ncat: Version 7.50 ( https://nmap.org/ncat )
Ncat: You must specify a host to connect to. QUITTING.
[root@34d72bfaa420 ~] #
```

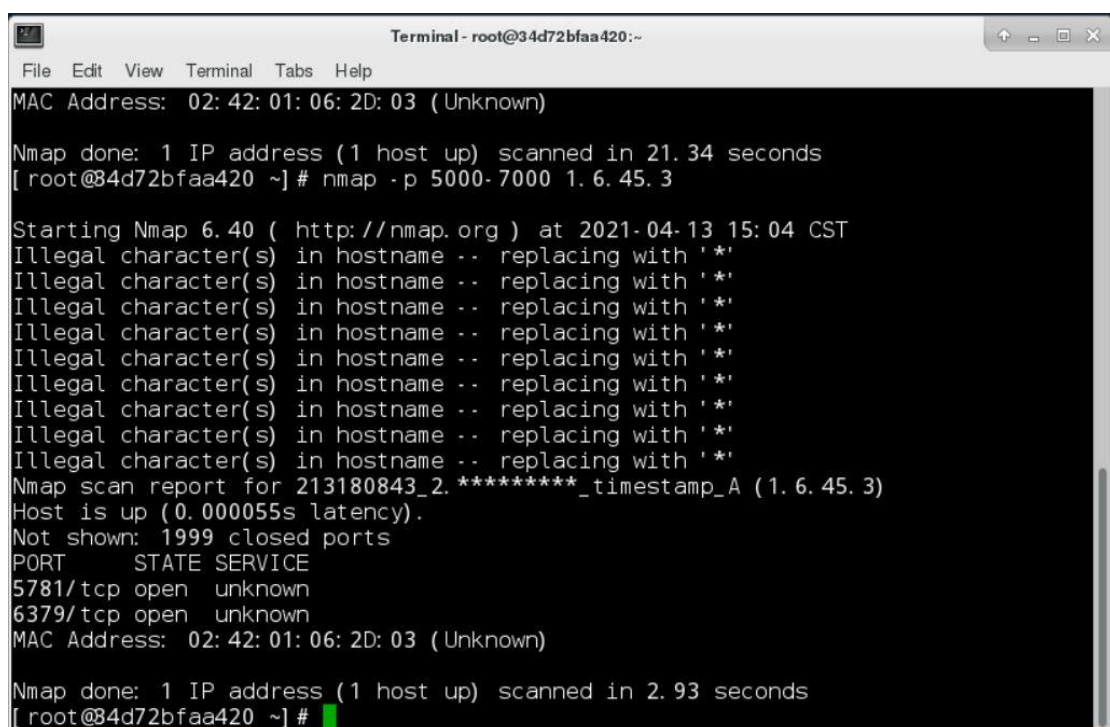
利用命令扫描 1-10000 端口

“nmap -p 1-10000 IP”这种方法比较慢，因为开放端口是 1-10000 之间的随机数，可以以 2000 个端口为一组进行扫描，这样速度比较快。

A terminal window titled 'Terminal - root@34d72bfaa420:~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the following commands and output:

```
Complete!  
[ root@34d72bfaa420 ~] # nmap -v  
  
Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-13 14:53 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@34d72bfaa420 ~] # nc -v  
Ncat: Version 7.50 ( https://nmap.org/ncat )  
Ncat: You must specify a host to connect to. QUITTING.  
[ root@34d72bfaa420 ~] # nmap -p 1-10000 1.6.45.3  
  
Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-13 14:54 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 '*'
```

经过分组查询后很快发现有两个打开的端口，我们知道 6379 是常用的 redis 端口，所以猜测 5781 是本题开放的随机端口。

A terminal window titled 'Terminal - root@34d72bfaa420:~' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the following commands and output:

```
MAC Address: 02:42:01:06:2D:03 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 21.34 seconds  
[ root@34d72bfaa420 ~] # nmap -p 5000-7000 1.6.45.3  
  
Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-13 15:04 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 (1.6.45.3)  
Host is up (0.000055s latency).  
Not shown: 1999 closed ports  
PORT      STATE SERVICE  
5781/tcp  open  unknown  
6379/tcp  open  unknown  
MAC Address: 02:42:01:06:2D:03 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds  
[ root@34d72bfaa420 ~] #
```

利用“nc IP Port”的命令格式连接，连接成功后没有左边的命令符提示，而是重起一行，可以输入 whoami 验证是否为 root，如果是 root，则说明连接成功。

```
Terminal - root@34d72bfaa420:~
File Edit View Terminal Tabs Help
[root@34d72bfaa420 ~]# nmap -p 5000-7000 1.6.45.3

Starting Nmap 6.40 ( http://nmap.org ) at 2021-04-13 15:04 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 '*'
Nmap scan report for 213180843_2.*****_timestamp_A (1.6.45.3)
Host is up (0.000055s latency).
Not shown: 1999 closed ports
PORT      STATE SERVICE
5781/tcp  open  unknown
6379/tcp  open  unknown
MAC Address: 02:42:01:06:2D:03 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 2.93 seconds
[root@34d72bfaa420 ~]# nc 1.6.45.3 5781
whoami
root
```

通过 `ls` 可查看目录，进入到 `cd test`, `cd root`, `vi flag.txt` 可看到 `flag`。

[illegible]

第二题

2.linux正则表达式 (50分)

题目描述:

ssh test@靶机ip, 密码123登录靶机。在靶机的/home/test目录下, 有一个很长的文本文件, flag被拆分成一个一个的数字安插在不同位置, 仔细阅读, 找出数字并且将他们合并起来

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, 35 秒



首先按照题目要求利用 ssh 登录到靶机

```
Terminal - root@dd34c3b04743:~
File Edit View Terminal Tabs Help
Warning: Permanently added '1.6.43.3' (ECDSA) to the list of known hosts.
test@1.6.43.3'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@2eaaad7529ac: ~$ ls
threekingdoms
test@2eaaad7529ac: ~$
```

看到 test 目录下有一个 threekingdoms 文件, 题目中说 flag 被拆分成单独的数字安插在文件中的不同位置, 于是我们利用命令:

“cat threekingdoms | grep ‘[0-9]’ ”

```
Terminal - root@dd34c3b04743:~
File Edit View Terminal Tabs Help
applicable law.

test@eaaad7529ac:~$ ls
threekingdoms
test@eaaad7529ac:~$ vi threekingdoms
test@eaaad7529ac:~$ cat threekingdoms | grep '[0-9]'
Give you good night6.
Unto our climatures7 and countrymen.--
Season your admiration6 for awhile
That beetles 6o'er his base into the sea,
大名?"那人道:"有书在此,少刻便知8。且取酒来。"李小二连忙开了酒,一面
可与我觅只船儿。"6酒保道: "这般大雪,天色又晚了,那里去寻船只?"林冲道:
曹操回府,荀彧等一班谋士入见曰:"天子认刘备为叔,恐无益于明公。"操曰:"彼既认为
皇叔,吾以天子之诏令之,彼愈不敢不服矣。况吾留彼在许都,名虽近君,实在吾掌握之内
,吾何惧哉?吾所虑者,太尉杨彪系袁术亲戚,倘与二袁为内应,为害不浅。当即除之。"
乃密使人谨告彪交通袁术,遂收彪下狱,命满宠按治之。时北海太守孔融在许都,因谏操曰
:"杨公四世清德,岂可因袁氏而罪之乎?"操曰:"此朝廷意也。"融曰:"使成王杀召公,
周公可得言不知耶?"操不得已,乃免彪官,放归田里。议郎赵彦愤操专横,上疏劾操不奉
帝旨、擅收大臣之罪。操大怒,即收赵彦杀之。于是百官无不惧。谋士程昱说操曰:"今
明公威名日盛,何不乘此时行王霸之事?"操曰:"朝廷股肱尚多,未可轻动。吾当请天子田
猎,以观动静。"于是拣选良马、名鹰、俊犬、弓矢俱备,先聚兵城外,操入请天子田猎。
帝曰:"田猎恐非正道。"操曰:"古之帝王,春搜夏苗,秋猕冬狩:四时出郊,以示武于天
下。今四海扰攘之时,正当借田猎以讲武。"帝不敢不从,随上逍遥马,带宝雕弓、金钹
箭,排銮驾出城。玄德与关、张各弯弓插箭,内穿掩心甲,手持兵器,引数十骑随驾出许昌
。曹操骑爪黄飞电马,引十万之众,与天子猎于许田。军士排开围场,周广二百余里。操与
天子并马而行,只争一马头。背后都是操之心腹将校。文武百官,远远侍从,谁敢近前。当
日献帝驰马到许田,刘玄德起居道傍。帝曰:"朕今欲看皇叔射猎。"玄德领命上马,忽草中
赶起一兔。玄德射之,一箭正中那兔。帝喝采。转过土坡,忽见荆棘中赶出一只大鹿。帝连
射三箭不中,顾谓操曰:"卿射之。"操就讨天子宝雕弓、金钹箭,扣满一射,正中鹿背,倒
于草中。群臣将校,见了金钹箭,只道天子射中,都踊跃向帝呼"万岁"。曹操纵马直出,遮
于天子之前以迎受之。众皆失色。玄德背后云长大怒,剔起卧蚕眉,睁开丹凤眼,提刀拍马
使出,要斩曹操。玄德见了7,慌忙摇手送目。关公见兄如此,便不敢动。玄德欠身向操称
```

可以输出所有包含数字的段落,最后统计一下出现的数字,组成 8 位
flag。