Qianyi Feng

CIS 410

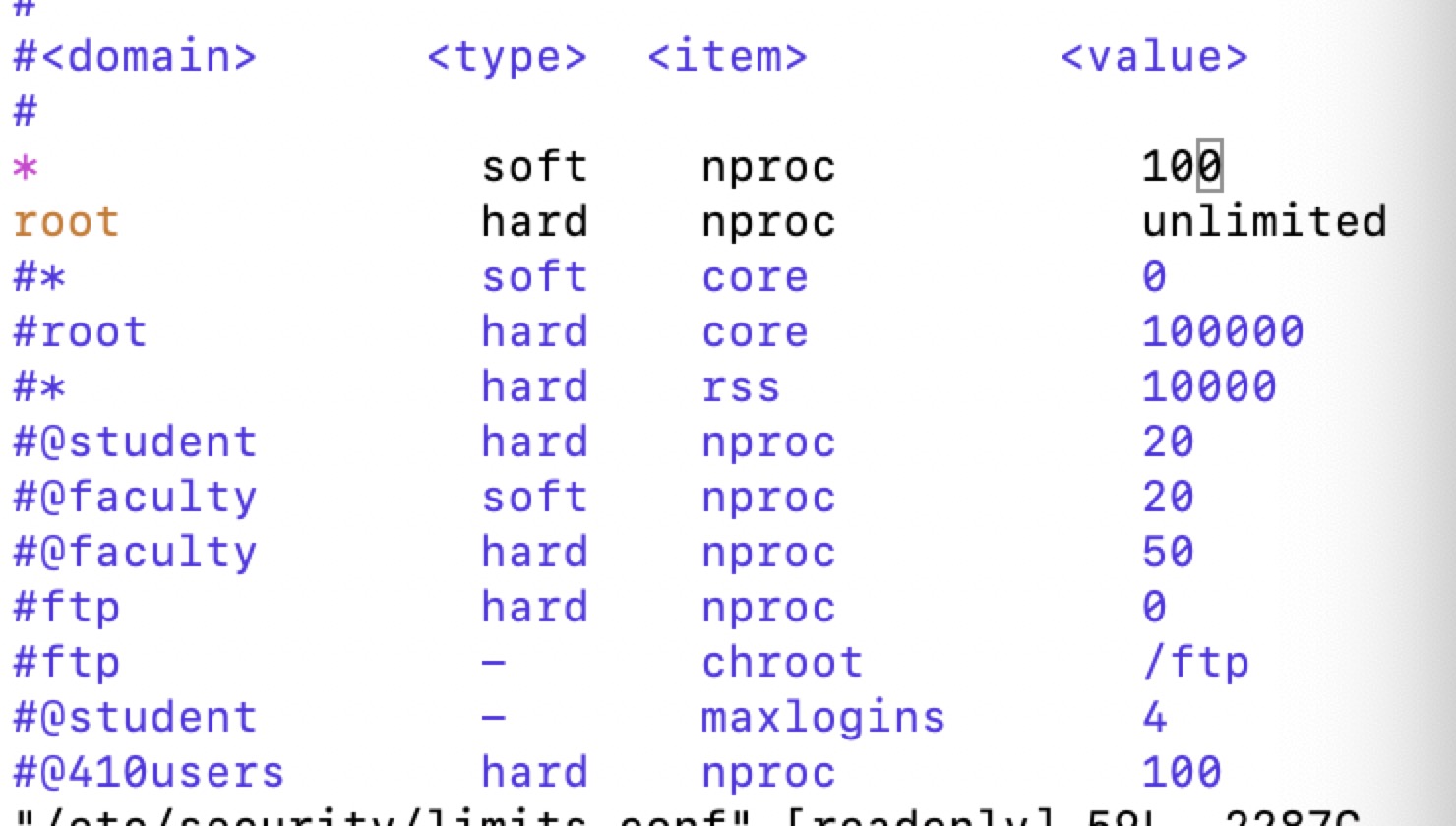
Assignment 5 report

**Exercise 1: Detecting/Launching Fork Bomb Attacks on VMs**

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

Script on ix: runvm.sh

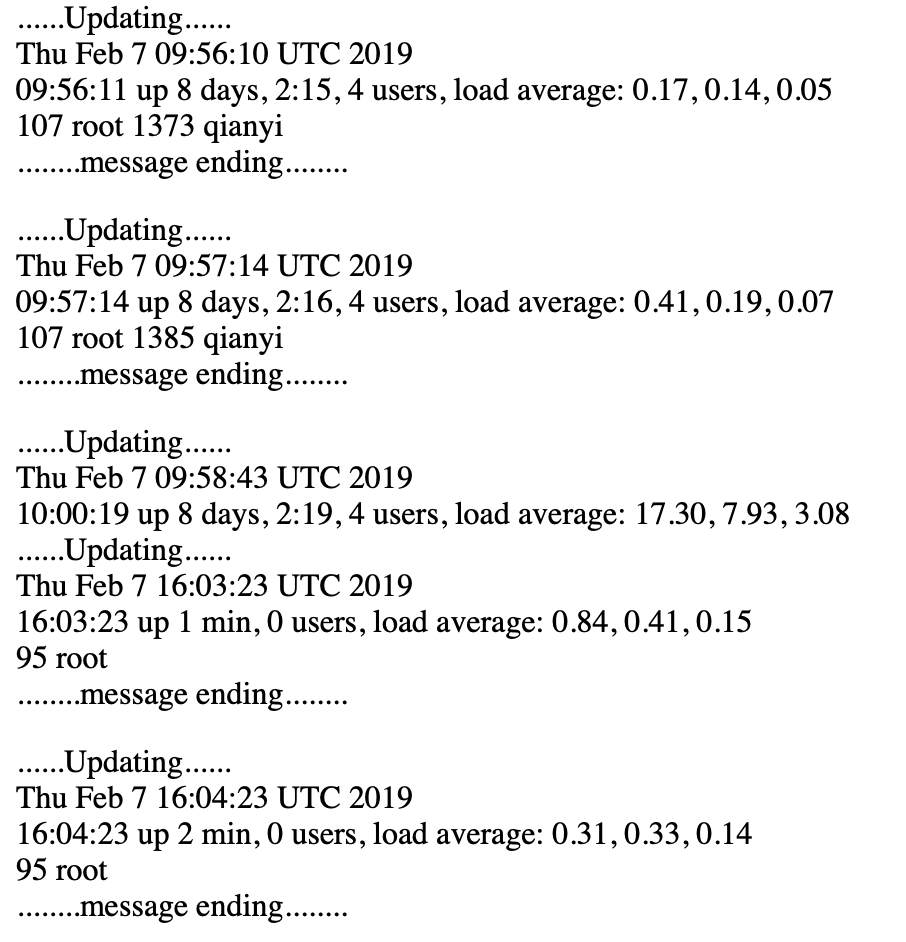
Script on my VM: mon1.sh

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

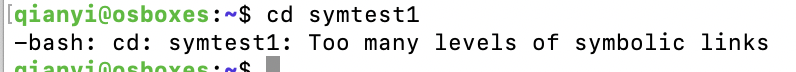
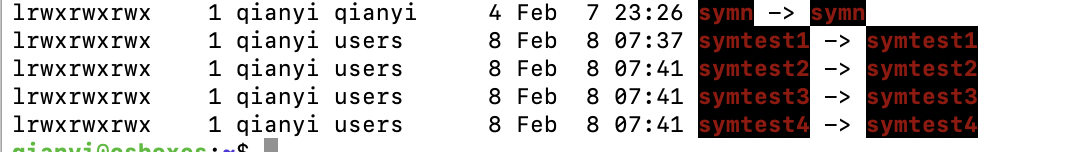
http://ix.cs.uoregon.edu/~qfeng/snail-wk5.html:

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.

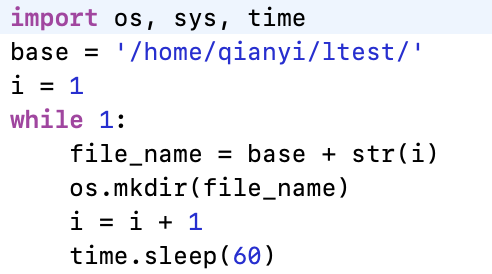
**Exercise 2: Defending/Launching Various Attacks on VMs**

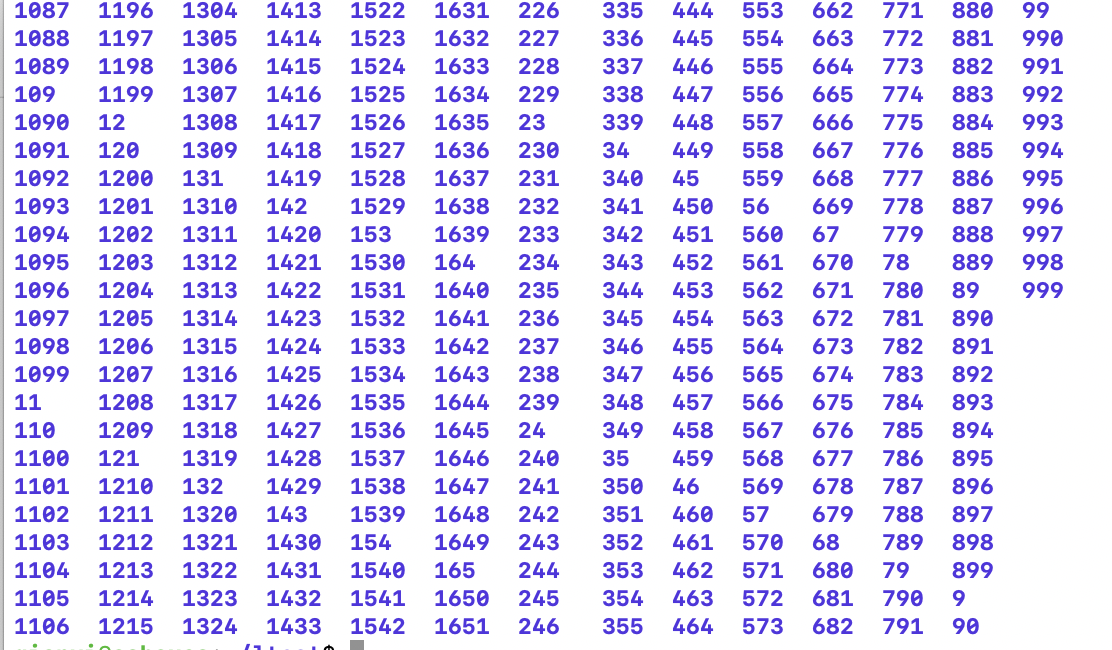
**2.1. Launching other Attacks on Selected VMs:**

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: 

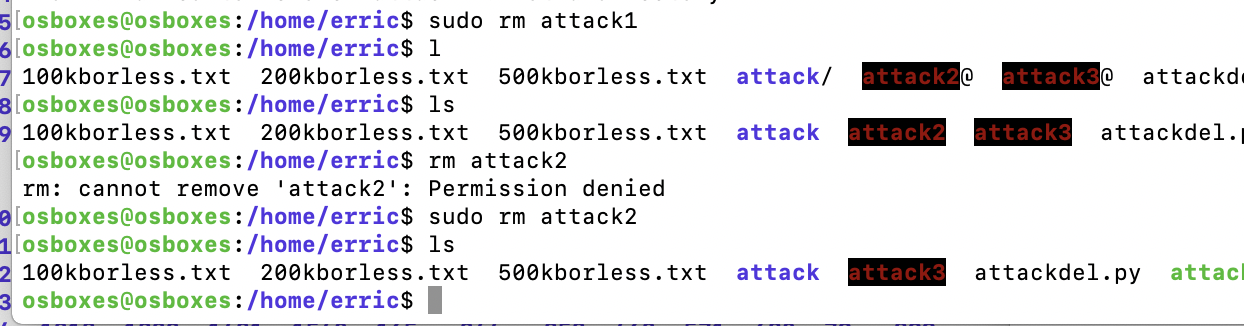
For the second one, I have no idea to delete open files in batch, therefore I deleted them manually. Firstly I used lsof command to find open files, and then use rm command to remove them. However, I have no permission to delete other people’s file, and I was not sure which files of mine could be deleted 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:

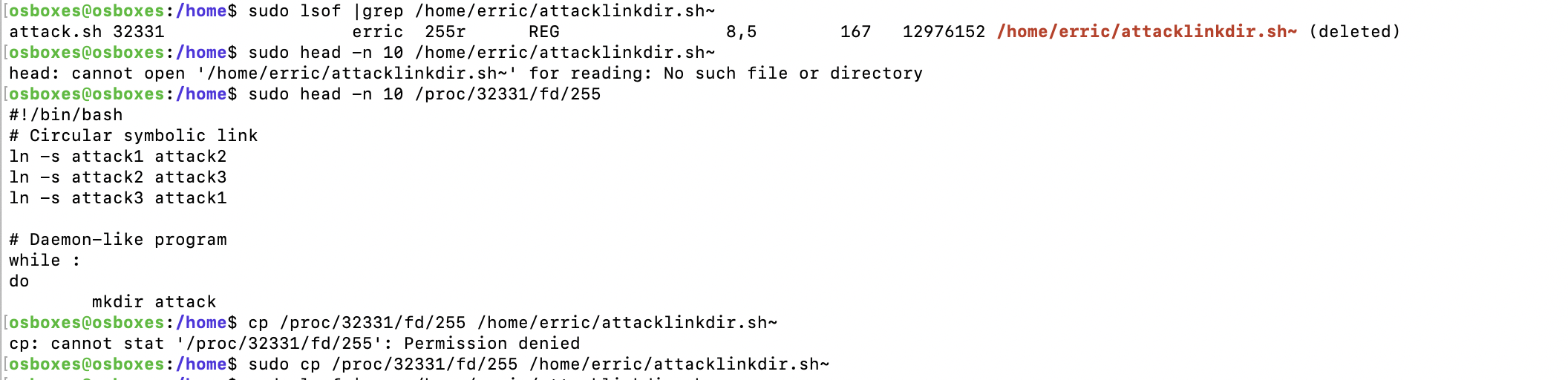


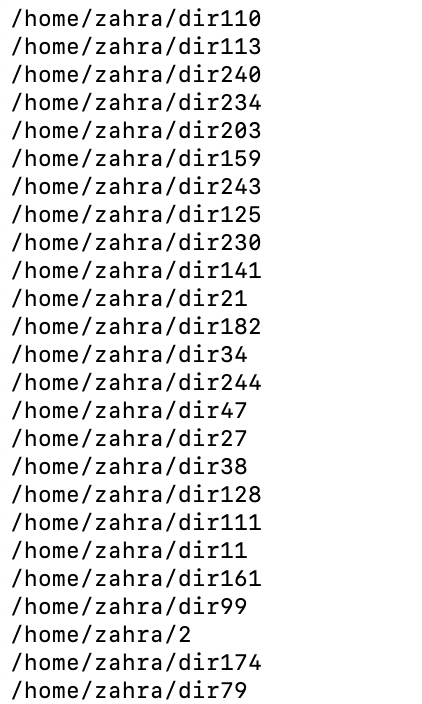
**2.2. Detecting Attacks on your VM:**

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:

I then removed it manually:

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:



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.

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