Introduction:

Protecting any company, business, or personal data or computing equipment is extremely important. As a part of this exercise we have been hired as the Red Team to break into and edit a file on 7 Raspberry Pi’s, a Linux machine, and a Windows server by any means possible.

Events’ Narrative:

DAY 1 Monday December 3, 2018

Starting on Monday December 3, 2018, Jonathan R. and I decided to primarily work together to intrude into the CIS 421 network. We were searching for the file that we need to edit in order to “win” the exercise and be successful in intrusion. Following are the events and details of the day.

The first obstacle we faced was the fact that things were not plugged in correctly or turned on. So, we will remind ourselves from now on to check everything before we attempt to connect to or use any equipment. We also had previously decided that we would go to the source of the equipment we desire to get into, using the room and equipment in our favor. The first action we took was to disconnect the Raspberry Pi’s from the Internet, therefore, we could not be monitored remotely or accessed remotely. We did so by unplugging the ethernet from port 1 on the switch. However, this meant that we would need to connect to the Pi’s directly. This was not an issue once we were able to configure the setup using an HDMI cable that was already in the room along with a monitor.

Next we connected to a Pi directly. On this Pi (IP: 10.4.20.40) we found a file called monitor.bat, we believed that the file would or could hurt our efforts and deleted the file. We hen took a break from the Pi’s, due to connection errors (human error as well). So, we then searched through the windows server/computer. Searched for .txt files (even though it may not be one) and in the process found a trap called trap.txt. We decided to open the trap.txt file and it was truly a trap. However, when we disconnect the Internet we also disabled the trap. We then deleted the file.

Next I went to the Linux computer while Jon kept searching on the Windows computer. He ended up finding some network connections named CRACK ME UP and CS WINSRV. We were not able to do anymore with these though. On my end, the Linux computer had a username and password for the root user that we did not know. So, we put that on hold and went back to the Windows computer. We searched through the logs but did not find anything else suspicious or what seemed to be out of place. We did check some things that seemed odd to us, but we did not locate the file. We then took a break for dinner.

After dinner we returned and decided to further test the Raspberry Pi’s and see what we could access on them. We connected the Pi’s briefly back to the Internet to look and determine IP addresses using the Linux command line with the command hostname -I. We also learned how to connect to each Pi correctly (we could only get one to work up to this point, so we spent some time doing a hardware trial and error prior) to access the display and searched for what we could find as far as hidden files are concerned. On the Pi with the IP address of 10.4.20.41 we found a hint. The hint was a text file that contained the following:

CIS 421 2018

Genesis 7:12

Numbers 14:34

We thought they may have something to do with the login credentials for the root user of the Linux computer, but we were unsuccessful. We then looked up the verses and the both had the words forty in them multiple times. However, we did not discover anything more with this hint.

We swiftly moved onto other Pi’s to search them for clues as well. We connected to another Pi and shortly found another hint text file. This one contained the following:

CIS 421 2018

Hydrogen

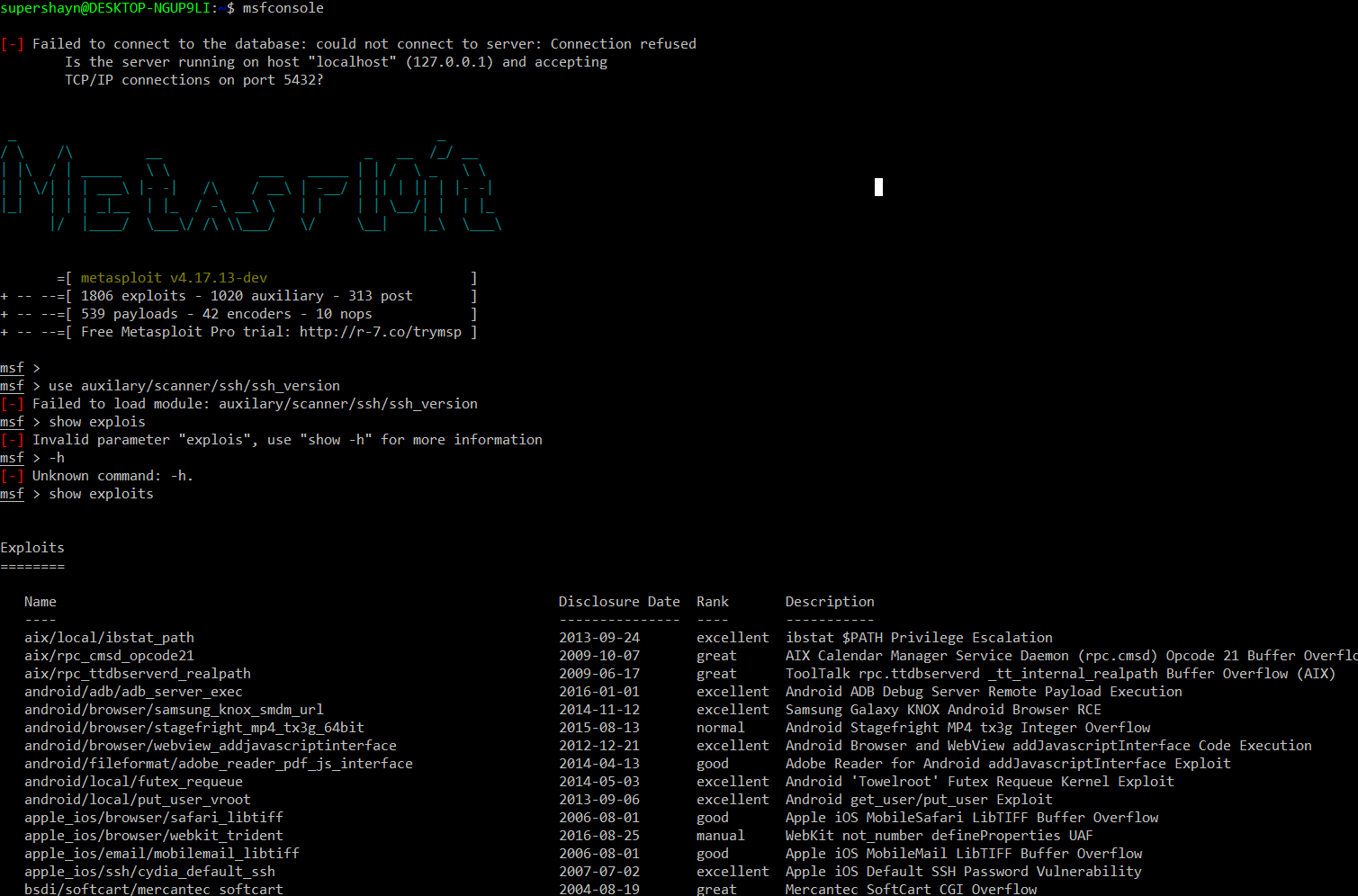
Helium

Lithium

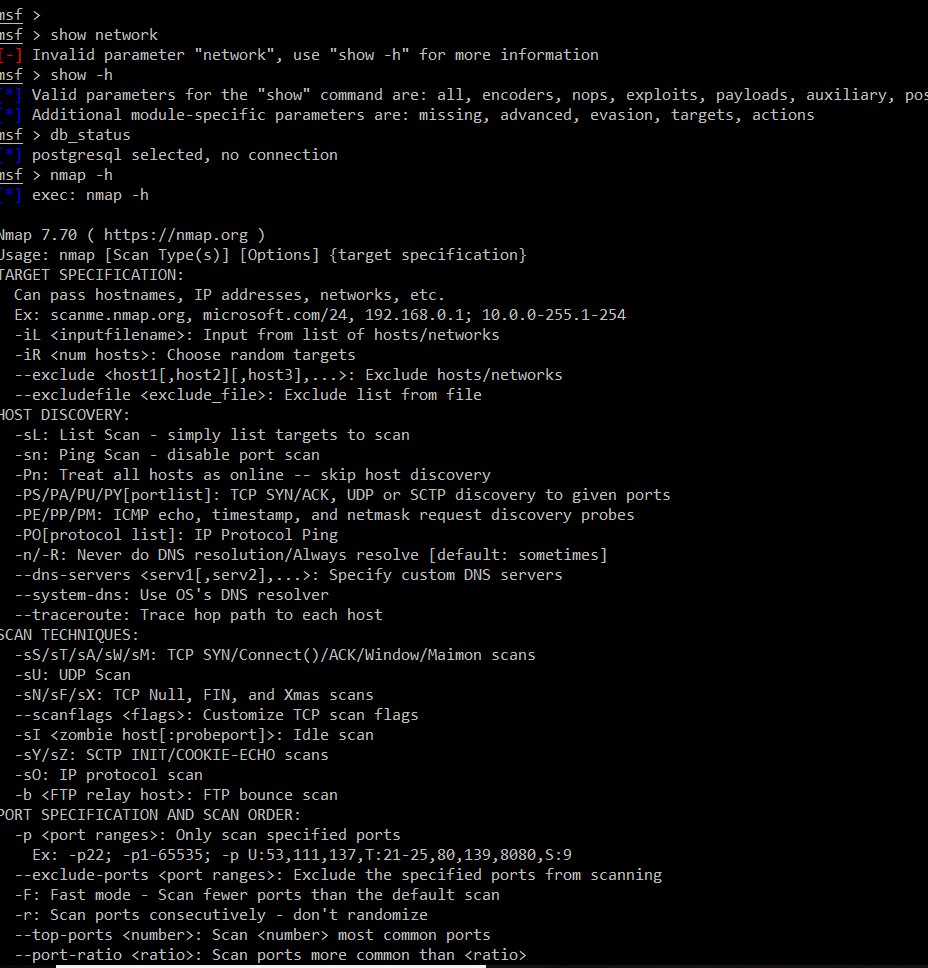
Carbon

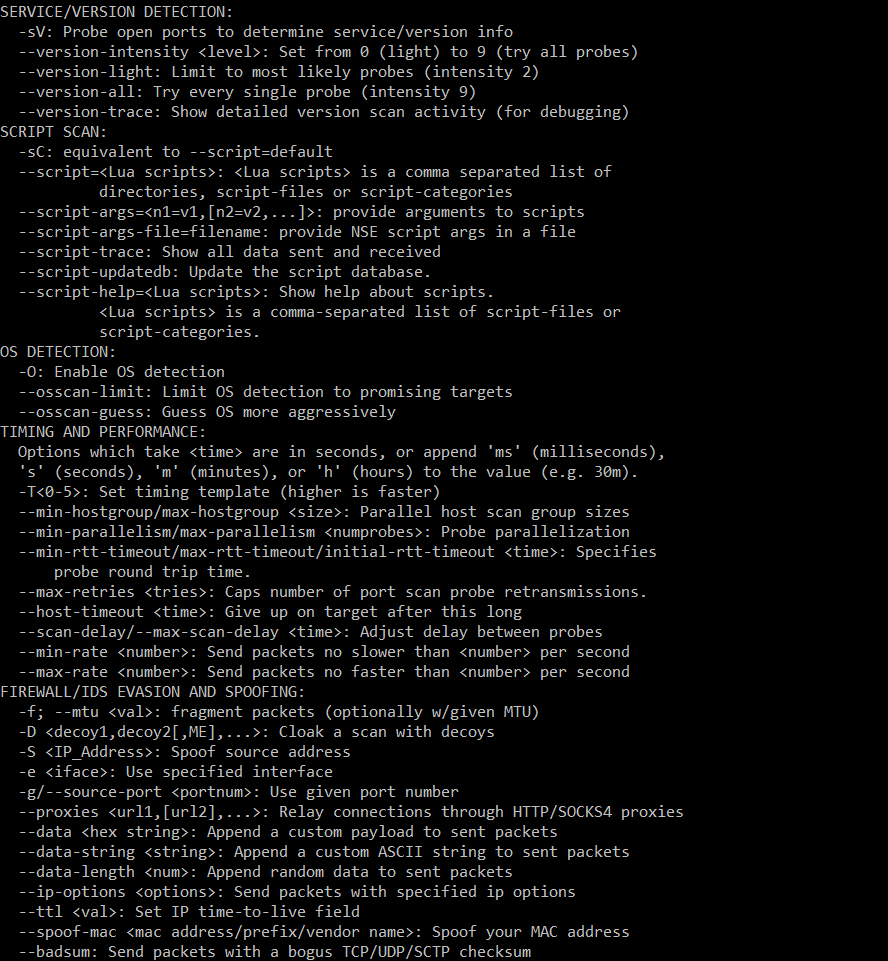
Oxygen

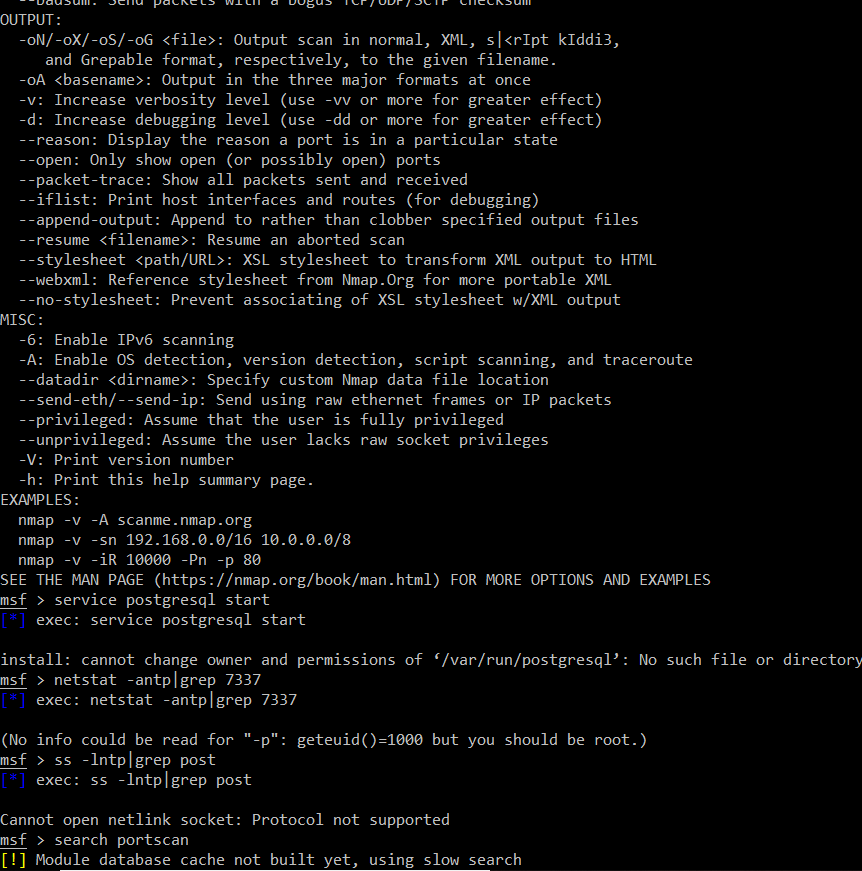
Uranium

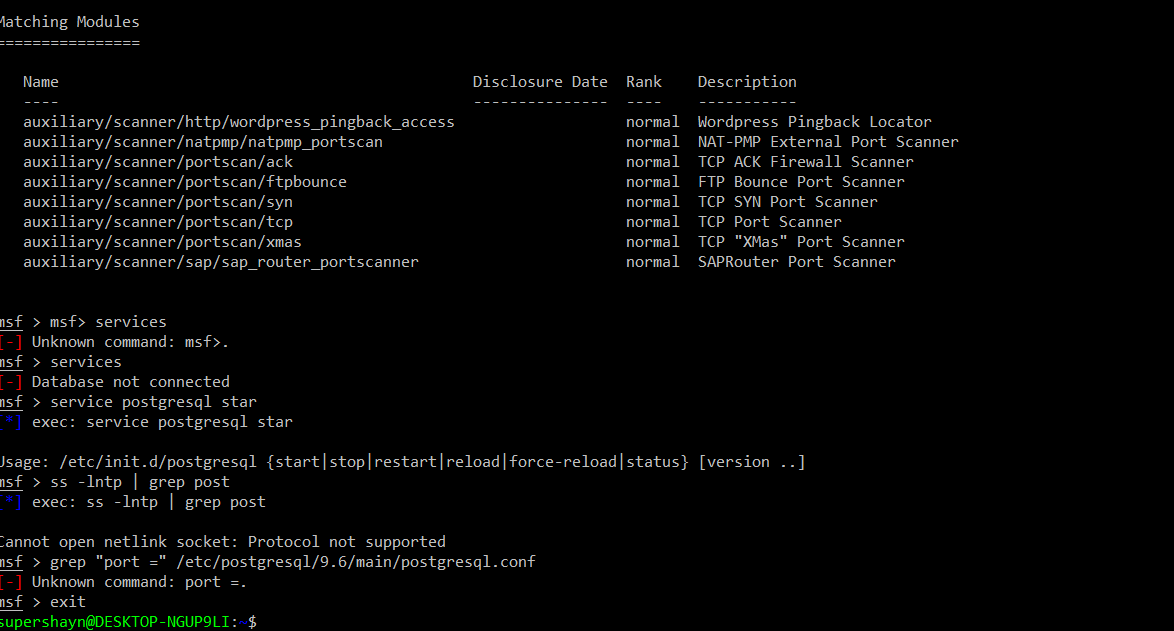
We could not figure out how this hint corresponded in any way either. No more hints were found. While on each Pi, I tried to access the MSF console for Metasploit (with and without Internet), I was unsuccessful in access Metasploit. We then connected my laptop directly to the switch using an ethernet cable. I then pulled up Metasploit using MSF console on the Kali Linux command line. I then tried to gain intel from using Metasploit and its features. I attempted to use Nmap to view and make note of open ports (etc.) however, Metasploit could not connect to the database and did not work. The images below show my attempts. 

(many more exploits listed here, I have not included pictures of the whole list)









Then we moved back to the Linux computer. Jonathan looked up a way to change the root user's credentials and we set off in doing so. We used information from [www.marketecheasier.com/reset-root-password-linux/](http://www.marketecheasier.com/reset-root-password-linux/). Once the password was changed we were able to get into the Linux computer.

Once we were into the Linux computer we began searching around. I used the ls, ls -a, cd, and cd .. to navigate, locate, and search through the directories. Once we came upon some files we were suspicious of we use the nano command to read the files. We even added and edited our own file for testing purposes.

END OF DAY 1: TOTAL TIME: 6 hours

DAY 2 Tuesday December 4, 2018

We were delayed in out start time due to an Egypt mission trip meeting being within the space. Once into the room, we did not disconnect the Internet, simply because we wanted to see if we could see any one monitoring us. We discovered nothing. We then went back to the Linux computer. Using the new root password, we set up yesterday. We went back and saw if we could find any hidden files on the system. We ended up using ranger to navigate through the command line more efficiently. We attempted to use the grep command to search with keywords however, our results were unfruitful. We then went to the Windows computer and briefly looked again to see if we could find anything new or if anything had been moved onto that computer. We also made no progress and did not find anything new or helpful. We did go back and look at the hints we found and tried to make sense of them because we may have found all of them. Tyler went back and looked at the Monitor.bat file we had found and deleted yesterday (we were prompted that it was a hint). It contained:

Eat 10 vegetables a day to keep the doctor away, or is it 24, period.

This still did not help us piece the clues together, so we moved on. I then tried to use Metasploit on the Pi through the VNC viewer with the IP address of 10.4.20.34. I managed to get the framework running and attempted some basic commands. Then I tried to use meterpreter because I thought that it might bear more fruit than some of the other Metasploit features and commands. However, I did not succeed in doing anything. After that frustrating experience I went back to the Pi’s (while I was attempting meterpreter and the Pi’s, Jonathan was still searching on the Linux system computer and Tyler was using Metasploit). I viewed files on the Pi’s to see if anything was new or if there was anything I missed yesterday. Nothing presented itself.

\*Also, we believe Professor Sabal installed a camera onto a Raspberry Pi. We did wave and have the camera faced towards us and yes there would be legal implication and we would be caught and sent to jail. However, since we were given access to the room, we decided to point the camera away from us and play a stream of SpongeBob in front of the camera. In a real situation there would be different precautionary measures taken to ensure we were not caught.

Tomorrow I want to try and use Metasploit again. I want to use some new commands I also found on offensive-security.com. <https://www.offensive-security.com/metasploit-unleashed/msfconsole-commands/#search-command>.

END OF DAY 2 TOTAL TIME: 3 hours

DAY 3: Wednesday December 6,2018

I did not work on the project on this day. Jonathan and Tyler made little to no progress. They did believe that the elements file was important, however, this later proved to be a red herring and false hint.

END OF DAY 3 TOTAL TIME: 0 hours

DAY 4: Thursday December 7, 2018

I came to the classroom thinking than we were meeting for class but that was not the case. So instead I began searching through what was Pi 40 due to a hint Professor Sabal had given us. I simply used the command line to search through directories and files (ls-a, nano, etc.).

In the evening I arrived at the room around 9:00 pm to work with Tyler and Jon. We were still focused on the elements directory. So, we spent the entire night trying to gain access into the files we thought contained the file we needed to edit. To list all of the local users we used cut -d: -f1 /etc/passwd. We attempted to add a user using sudo adduser new\_username. This did not help us gain access.

We then tried and succeeded at changing user passwords after doing some research on <https://www.linode.com/docs/tools-reference/linux-users-and-groups/>. We then still tried to gain access to the file we thought we needed to in the elements directory. We did end up gaining access through the root user however, there was nothing there. We decided to stop for the night round 12:30 am.

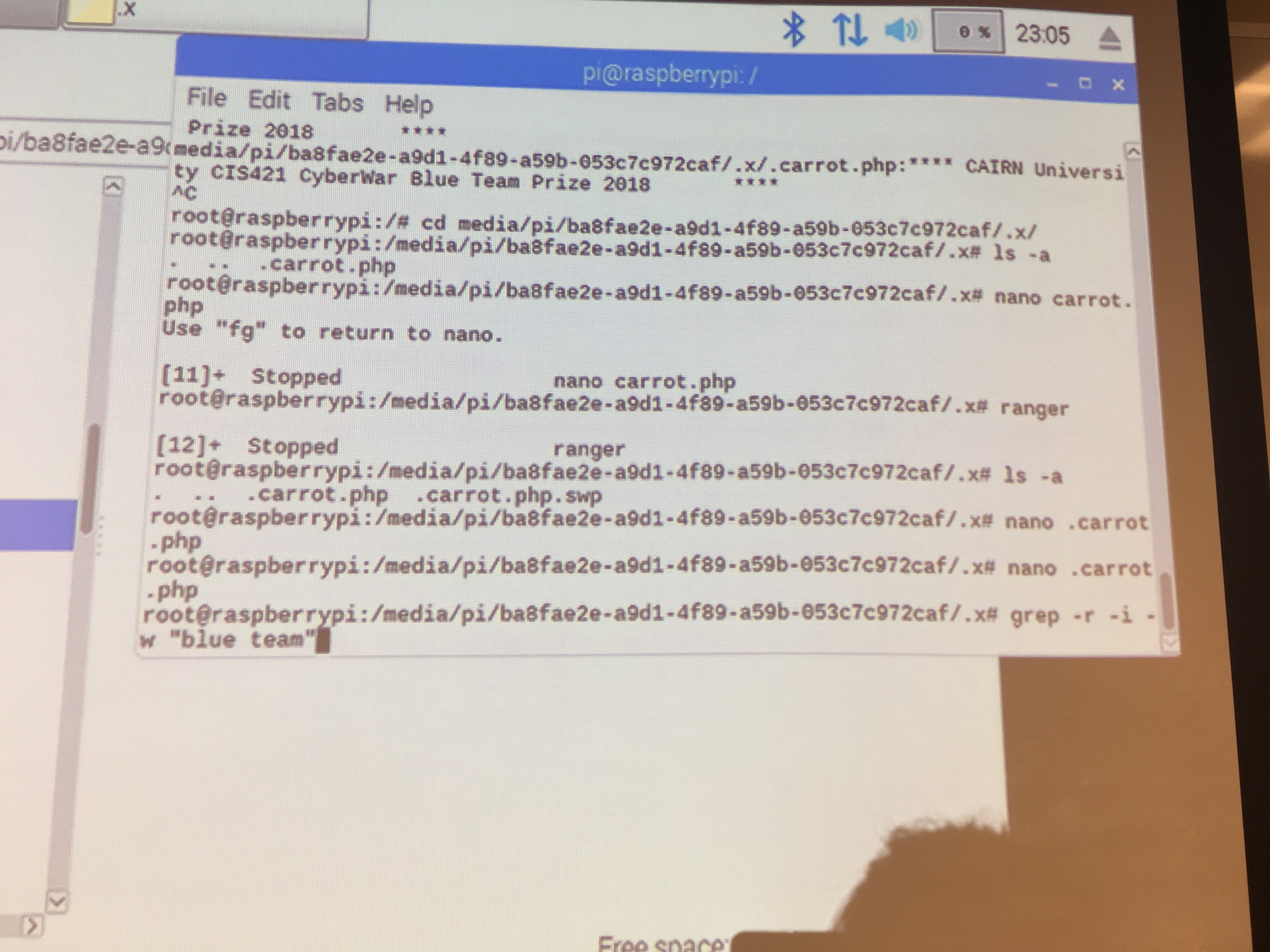
END DAY 4 TOTAL TIME: 3 hours 30 minutes

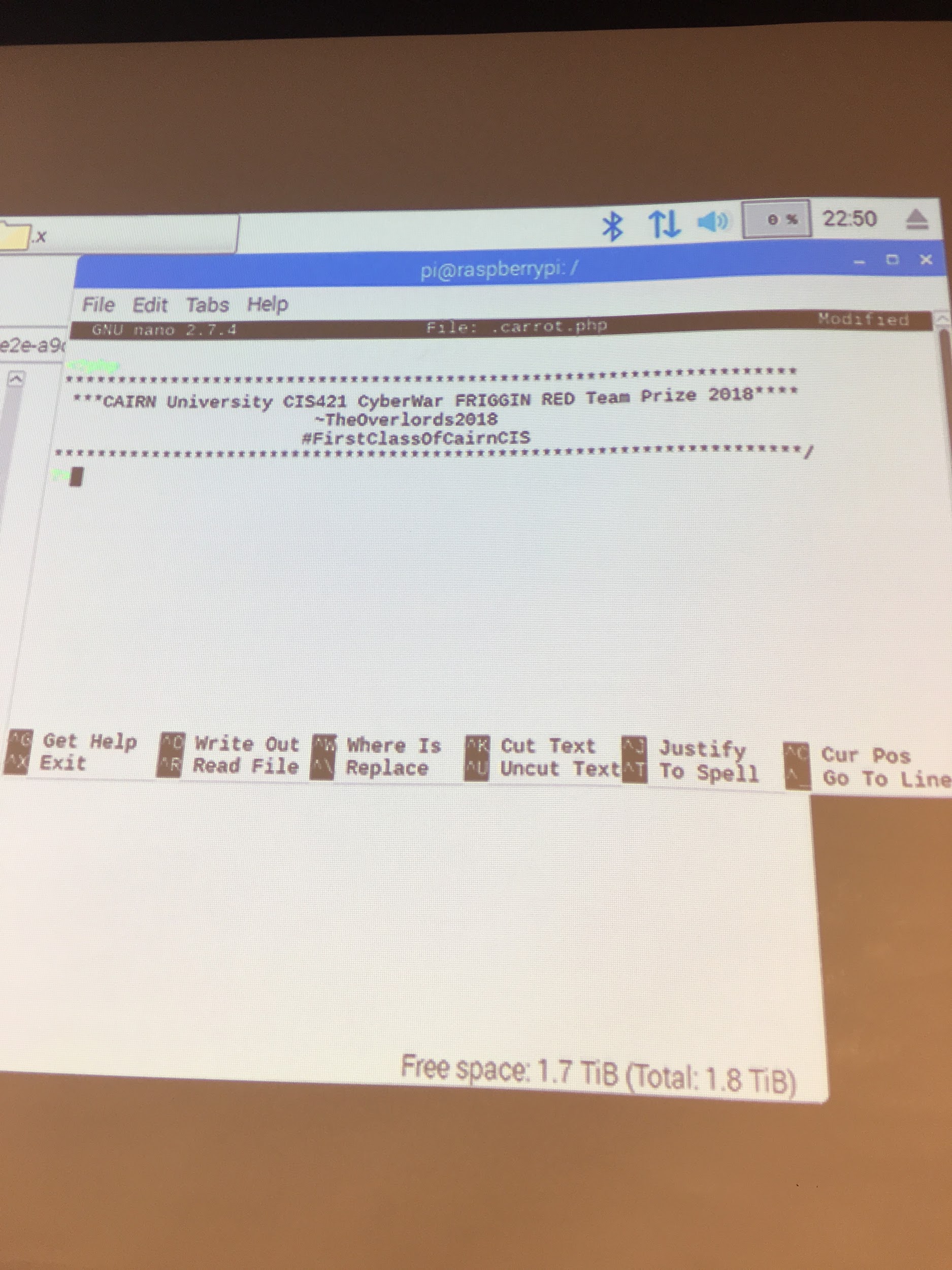
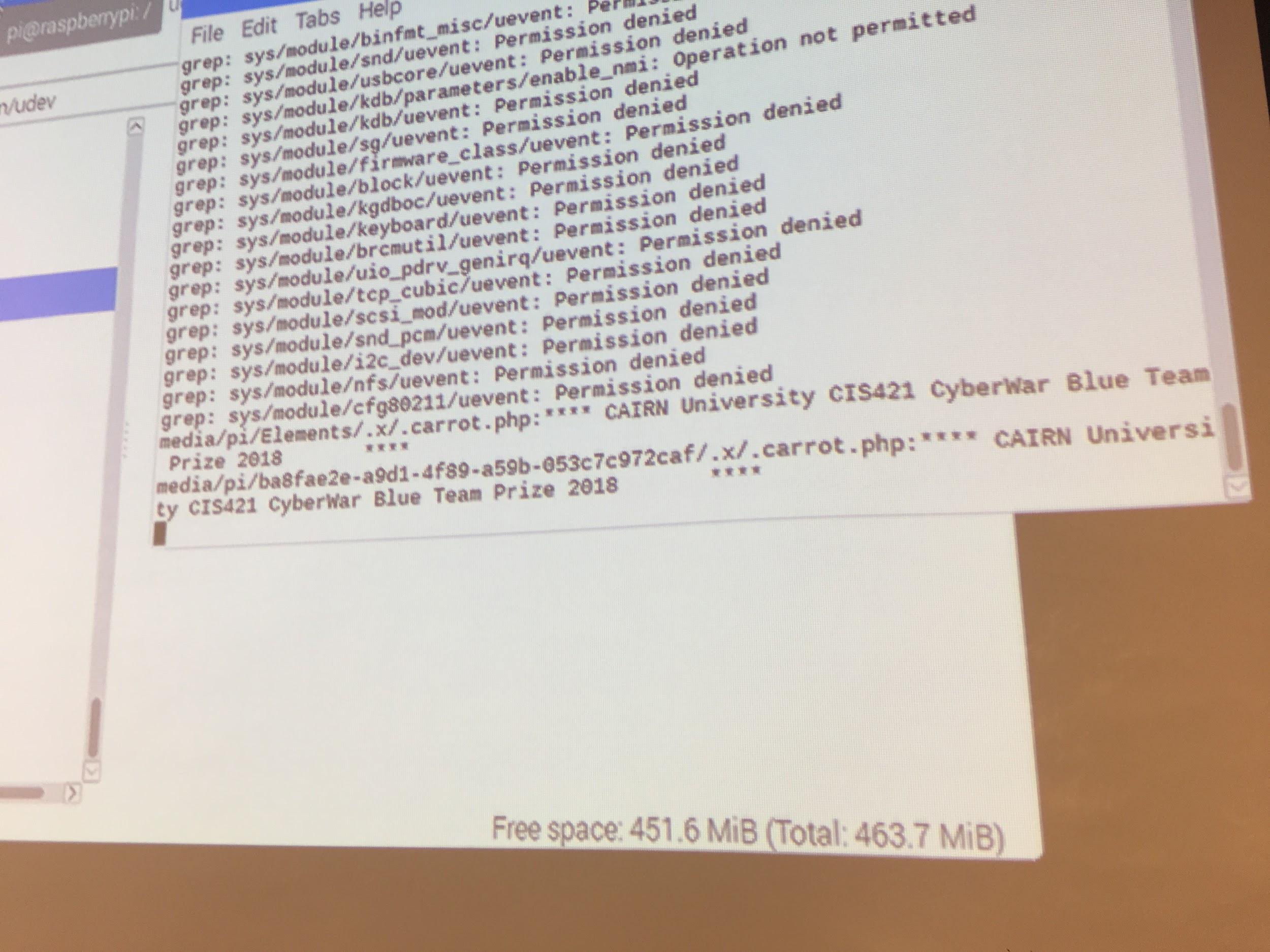
DAY 5: Friday December 5, 2018

I came and met Jonathan in the room at 9:30 pm, to assist in finding the file. We had then learned from Professor Sabal that we were in the wrong Pi and that the elements file was a false hint. Lesson learned, do not trust the enemies hints. We found the right Pi (40) and began our search. We had done some research on grep functions. We used the following sources to achieve our final result.

<https://stackoverflow.com/questions/10375689/how-can-i-grep-hidden-files>

<https://stackoverflow.com/questions/16956810/how-do-i-find-all-files-containing-specific-text-on-linux>





WE WON!

We edited the file using the nano command. We then decided that we would completely disconnect Pi 40 so that none of our work could be undone. Then we celebrated.

END OF DAY 5 TOTAL TIME 3 hours

Conclusion:

Being a part of a Red Team exercise was educating but also presented many challenges. We did used the physical access we were given to our advantage however, in a real-world situation we would be arrested and charged with breaking and entering along with theft of personal information. Along with being charged with property and equipment damages. Overall if there was not physical access then the system would have been much safer from us. Also, we only had one experience where Professor Sabal blocked us, and he was also present in the room. If the file was encrypted or password protected I believe that that would have provided better protection from us. Overall, this assignment was frustrating, but I feel accomplished that we found and edited the file.

Work Cited

\*Non-Online sources

Kennedy, David. *Metasploit the Penetration Tester's Guide*. No Starch Press, 2011.