James McKenzie's Project 1 Portfolio

James McKenzie

August 19 2019

Foreward

For Project 1, I have managed to find myself as a member of the OPs' divison. I have always been interested in OPs, Specifically in Systems Administration and Linux/BSD/Solaris Operating Systems

Strengths

Over my time of the BIT, and before, I have accumulated some knowledge and experience in several areas which i may be able to use to help the OPs teams. These things are

- A Strong knowledge of Linux/BSD operating systems, and experience with the GNU toolset
  As linux has been my go-to operating system for the past 6ish years, I am fairly comfortable with most basic and intermediate level tasks on it. However, I am still unsure regarding many networking aspects of linux due to lack of personal resources. Perhaps this would be a good thing to work on

- Knowledge of basic SysAdmin
  I have completed the 3rd year Systems Administration paper which I hope has prepared me with some of the practices that the OPs team will use during the semester

- A Strong knowledge in Programming (C, Bash, Python)
  I spend most of my free time coming up with seemingly useless Projects to write, or going through many exercise books and learning new languages. Perhaps this is the perfect time to learn some basic PERL scripting as it seems to be one of the industry standard scripting languages if you need something faster, and more powerful than python. Potentially it would be wise to brush up on both Bash and Python too, though i don't expect to use much C in my day to day project work

Weaknesses

However, even though I have some strengths that I can bring to the team, There are also some skills that I should work on.

- Security
  I am not overly confident with my knowledge of Security, as I have not taken that Paper, and I do not have much previous knowledge of experience, other than basic theoreticals. So this would probably be one of the more important things to get better with, If i want to keep improving my skills in IT

- Networking
  Networking is another concept that I am familiar enough with to get something working, but not well. I should see what i can learn to improve this aspect of my Ops knowledge, as i imagine that having a smooth network is of critical importance when working in OPs

- Lack of Windows experience
  Since i have never really used windows, Im not overly familiar with its shell or how to get it to do anything. If we are managing any windows servers, this might be a problem, but there is also time to learn, and i hope some of my Linux/BSD/GNU knowledge could be of use (Pesky Backslash)

1 Week 01

There is not much to discuss in Week 01, As it was mostly deciding the team that you were going to be apart of. I was hoping for either OPs or Mobile, Although, I'm not so sure about mobile, as I don't want to be using react native, as i never really liked React very much (or JS in general) but it is still an option. OPs looked good though

1.1 Lesson 1

After the discussion and introduction from Adon, we got to walk around and choose what groups looked interesting for us. Since I have always been a huge fan of managing Systems, OPs was an obvious contender for me. However, that did mean that I would have to give up my true love of Programming for a while, so i was also considering Mobile. Davids project looked too complicated for me, and since i haven't done machine learning, It probably wouldn't be a good idea for me to try it anyways. So at this point, it is really a toss up between OPs and Mobile, but at the moment, Mobile is looking more likely, due to the fact that there seems to be alot of interest in the OPs group, and not many spots. But OPs would be my first choice. Fingers crossed!

1.2 Lesson 2

Looks like I made it into OPs afterall. That's pretty great in all honesty. Im looking forward to learning all the Systems and how all the services we run work, and how I can interact with them. I am specifically interested in Docker and vSphere as virtualisation is something that I think I would really like once I get over the learning curve. I spent most of today setting up my work area. I am considering installing a linux VM (Preferably Arch, Alpine or Debian) on my machine so I can do most of my work in a Linux environment, although, I will likely be using my laptop for alot of work anyways. I'm glad that I am in the same team as Matthew Hall, and Stefan, as we all seem to have a wide, semi overlapping skillset. I am looking forward to the semester

1.3 Week Conclusion

Not much has really happened this week, other than finding out im in OPs, and having a discussion with the Porject 2 OPs students. For the most part, It was expectedthat the first week or two would be slow for us Project 1 students, as we currently don't have a grasp of what we manage, or how we manage it. But I expect things to start speeding up in the coming weeks

2 Week 02

2.1 Lesson 1

Today I set up my default linux environemt that I will be working with over the rest of the semester. I did this so that i could do all my other class work from my workstation, and also so that I could use all my preferred programs for basic Systems Administration. It also gives me a good reason to learn and use LaTeX for writing up my portfolio, as it is the standard advanced markup program in IT, and most of science in general. I decided on using Ubuntu, as its more likely that packages will run nicely on it. While arch linux would give me a bigger range of packages to choose from, I think that Ubuntu's wide userbase would be of more help, should I run into trouble with anything.

2.2 Lesson 2

Today I spent some time reading through the documentation of GitLab, so we could do the planned update. I had Henry Cooper help me through it. I read and understood all the documentation before i did any updates, That way, I knew immediately when I strayed from the documetation, and I knew of any possible traps i could fall into. There was a few issues with the documentation, but they were very minor, specifically, it says 2nd line when it means the first line. I plan to fix this up at a later date, as i should really start getting my teeth stuck into my Project

3 Week 03

3.1 Lesson 1

Today Faisal introduced me to a program called Cuckoo. Its a Dynamic Malware analyser which simulated a User using a machine that you can infect with malware. There is a large amount of documentation, and it seems to be much easier to setup on Ubuntu than Arch or Windows. Over the next couple of weeks, I will try to get cuckoo to install successfully, although, It does seem like a pretty difficult task, and I am not sure how long it will actually take, but I hope to have alot of fun with it, none the less

3.2 Lesson 2

I tried to actually install cuckoo today, However, I hit several roadblocks. I had a big issue where Virtual Box and cuckoo were in conflict over what versions could be used. This resulted in several hours of googling how to use apts version manager (which i still don't understand) to try and get them to play nicely. I also ran into some issues with configuring mongoDB to run with Cuckoo. I am still unsure how I will end up getting cuckoo to work. At the moment, getting Cuckoo to launch would be a good start. I did however manage to fix alot of problems by fixing my pip configuration. I have never used pip before, as ive never really needed to, but after configuring it and using it, I understand that it can be a very powerful package manager. Perhaps I should try to get better with it, and practice using it on my other machines?

4 Week 04

4.1 Lesson 1

After a few hours of fiddling with different package managers, considering trying to compile cuckoo by source, and installing pointless rust libraries, i finally hit a break through where cuckoo decided to be found in PATH. Seeing the cuckoo screen come up was a great relief. However, there were still many errors to fix. Specifically, networking errors. I spent a few hours trawling the documentation to find a few commands to fix the networking errors, after which, I was greeted with some missing library errors, So ofcourse, I then proceeded to install all those libraries until we are left with an error about a missing Cuckoo VM. I think i am making good progress now, and I will set up the VM next time, and hopefully we can get some malware testing going some time next week

4.2 Lesson 2

Now that the cuckoo error is just about the missing Cuckoo1 VM, I guess that's what I will work on next. Ive gone with the morally grey approach of downloading an Official Windows 7 iso and just not activating it. This way, If

it breaks, I won't need to get another lisence (Theoretically Atleast) However, I couldn't get virtual box to boot a 64 Bit version of Windows 7. From my experience, this is usually because Virtualization isn't enabled in the BIOS of the host. However, since virtual box doesn't have a bios(At least to my knowledge) I had to settle with a 32 Bit version of windows, which I guess will get the job done.

5 Week 05

5.1 Lesson 1

Today we had a meeting with Faisal, Where we went into further detail regarding our Projects for the semester. I feel like I am atleast keeping up with the pack in regards to my understanding of my topic. Even though I have yet to get cuckoo working. I managed to sort out the web interface on Cuckoo today, which is nice, although, I am still having issues with networking the VM with the Cuckoo host. Even though both the Host, and VM Config are the same IP Address. I will spend the next couple of days before Lesson 2 trying to sort this out, However, if I am still stuck with it by Thursday, I'll see what Faisal thinks about it! I also wrote a very basic shell script to make sure that the Virtual Box network is up before I run cuckoo. Once I get more familiar with cuckoo, I would like to incorporate the running of Cuckoo into this script. Mainly as it would be nice to just run a single command to get cuckoo up and running! I can however, use the web interface well enough, and i have done a fair bit of poking around, trying to find any extra features

5.2 Lesson 2