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

Today, I spoke with Faisal regarding the Networking of the virtual machines. We decided that we should check the DHCP Server, as maybe it was giving different IP addresses when Cuckoo was running the VM directly. However, we ran into a few virtual box problems. The big one being we couldn't set up Automatic interfacing on the DHCP interface of the virtual machine. We also had a meeting where we all came together to discuss not only how the project is going, but what our plans are for the forseeable future.

6 Week 06

6.1 Lesson 1

Today I was still having a bunch of errors with Cuckoo. Namely, getting the machines to talk to eachother. I fixed the DHCP that i had partially set up last time, Just to make sure that the machines could ping, And The host could ping the guest when the machine was turned on, Which was better than we usually get. I tried to reInstall the agent on the Guest machine, but Virtual

Boxes Shared folder systems didn't want to work. I am not sure if that is an error of running Virtual Box inside a Virtual Environement or not, but Im sure i will eventually get that sorted. Once I manage to get the agent back working, which I will try to do before the next Project time, I am hopeful that it may fix the issues regarding the network erroring

6.2 Lesson 2

This session i spent some time trying to fix the networking issues, to no avail. I went up and grabbed a spare machine from the PC Maintanence Lab that Hamish had said i was allowed to use. I Spent the rest of the session trying to set up the bios, so that I could boot into a USB. This proven to be difficult as there was a BIOS Lock on the motherboard, but we managed to find the reset bridge and take off the BIOS Password

7 Week 07

7.1 Lesson 1

I spent this session installing Ubuntu SE onto the machine. This took a lot longer than anticipated, as the network cable I am connected with, is not in good condition, with only 4 of the 8 terminals connected. I set up a basic working environment, and installed X and i3 so i can try and Install Cuckoo with a new guide that faisal found for me. I hope this guide works properly, as it's quite long and complicated

7.2 Lesson 2

I started installing cuckoo following the guide that faisal sent me. I first had some issues with my locales, which wouldnt let KVM Boot. I made my way through the installation after I fixed that though, and we managed to write a document that had all the errors in the installation guide, that wouldn't run in shell, and I fixed them to the best of my ability. Most of the errors are things such as wrong GPG keys, Incorrect package names, and bad flags.

8 Week 08

8.1 Lesson 1

My installation broke today, as neither of my databases would connect to their port correctly. After spending some time, checking their configurations, and their status with system.d and journalctl, I decided it would be in my best interests to wipe the machine and try a different installation method. Faisal reccomended I look for a Ubuntu Resetting Program. I found one that was highly rated, and decided to install and run it. It proceeded to wipe my /usr directory before failing, as it nolonger had accessto the usr directiory. I am not sure if this is a bad joke of a program, but it appeared to brick my machine. I guess il try to install Ubuntu on it tomorrow

8.2 Lesson 2

Today, I went to install Ubuntu, but i couldn't boot into my live medium, as registers 8-15 were apparently not enabled, and thus, it wouldnt let me boot. After a bunch of fluffing around, reseating ram and bios flashing, we managed to boot into the live medium. I decided to try the new Cuckoo installation method that faisal had suggested. This one seemed alot longer than the last one, but it seemed that there were less inconsistencies than that one too. I got upto installing KVM. However virtmanaged was not running, so I called it a day and locked my PC

9 Week 09

9.1 Lesson 1

As i went to continue my install I found out that error I mentioned on thursday. I decided to google the error, which told me to restart my machine. After I restarted my machine, I noticed that my networking was broken. It said, Network Unmanaged in the systemtray, and i followed every guide i could find to try and fix the error, however, It wasn't fixable. I decided to try 1 last install of cuckoo before I give up on cuckoo entirely, and request a proper DevOPs project. Such projects I am considering, is installing Alpine Linux from Docker, Learn mopre about the Urbit Project, that a large number of Ops engineers are excited about, or just learning tools suc as Jenkins for CL/CI intergration

9.2 Lesson 2

This time, I am being as safe as I can. I am using an Ubuntu Desktop 18.04 instead of Ubuntu Server, so there is potentially less to go wrong. This resulted in the install taking much longer, as I no longer had a familiar environment to set things up in, and just general, the system was running slower. I ran into a few problems regarding permissions and packages, although a quick apt search means i can fix them. I got to the same point as last time, where I need to restart the system in order to continue, and I restart it, without causing any crashes to my network. I will call it a day here!

10 Week 10

10.1 Lesson 1

This session involved me installing some network traffic emulation program. However, this took a very long time, and once it was done, it started to use around 200 percent of my CPU time, so it probably wasn't work keeping around, but in order to not break anything, I decided to keep it as is. It probably isnt worth risking some more Apt clashes to get a bit of a better performance

10.2 Lesson 2

I got cuckoo installed again, but i keep hitting my head against the wall on the same problem; that the Host and guest cannot network with eachother. This has been an issue for me across both KVM and Oracle Virtual Box, so I am not quite sure what the issues are. My first point of call is checking that my guest is set up correctly, however, I know this is the case as i followed the instructions directly from the cuckoo wiki. So unless the documentaion is completely wrong, It shouldn't be that which is the issue. However, I could be wrong. My main concern is that the polytech network, and the fact that we are using a non standard (for my experience anyway) subnet. But i do not know enough about networking to say that to be sure.

Holidays

I spent the majority of my holidays working through some of my website functionality, where I am using mpd+icecast+ncmpcpp as an internet radio server. My goals for this was to be similar to lainon.life, which is one of my goto places for new music. I also had to work around hosting this locally at my flat, while also not interrupting my other flatmates hosted services. It took a bit, but i managed to get it all working. I also spent some time refamiliarizing myself with tree data structures for ADS, as well as my sorting algorithms. I would have liked to learn some stuff regarding OPS however, there just arent the online resources to get a OPs setup working on a student budget.

11 Week 11

11.1 Lesson 1

Coming back from the break, I was instructed to give up on my project of getting cuckoo working, as it would likely continue to be fruitless at this time, considering the large amount of time i was putting into it, mixed with the crushing lack of success it was bringing me. I instead was told to do some research on AnyRun and FlareVM, so I will get around to doing that on thursday, but i gave them a quick look, and they look like sensible alternatives to cuckoo

11.2 Lesson 2

I had a look at both FlareVM and AnyRun today. AnyRun seems to be an online version of cuckoo, except they hash and store the results of given input, so that the tests dont always need to be run, Shortening the amount of time it takes for the Malware Analysis turnaround to happen. FlareVM on the otherhand is a little bit of an enigma. It seems like its a virtual machine where you give it malware, and then watch it run from inside that machine itself. Obviously, Im sure its a great idea, although i just don't understand it at the moment.

12 Week 12

12.1 Lesson 1

I spent today writing some very basic programs to send into anyrun to analyze. However, my effort ended up not being that useful, as the anyrun virtual machines are not installed with a python interpreter, so it didn't run, and therefore, wasn't detected as malware. I also threw some other known malware at it, such as some forkbombs, and wanacry, which it caught nicely and quickly, I guess because it has been tested before. I also found out that anyrun has an API, so you could write your own pipelines to automate sending files to anyrun to be scanned. This is the ideal option to add malware security to an email server, as you can then automatically send the attatchments and check them before the recipient recieves them. My only concern is that this wont work in an end to end encrypted system, as you wouldn't be able to de-encrypt the file, (There is some irony here) and while im sure you could turn 1 end to end pathway into 2, that would violate the users trust of the e2e encrytion system.

12.2 Lesson 2

13 Hiatus and End of Semester

I ended up having a 2 week break from Polytech as i needed to play a few shows to fill in for some old friends. Over this time, I did alot of programming in my spare time.

After I came back, I spent a long time working on my poster for the showcase about malware analysis. I also reguarly would talk to my peers about my project to make sure I could explain the basic concepts and get across some of the nuance regarding Dynamic Malware Analysis, so I would be well versed for when showcase happened, because in a way, The Showcase would be really where i have to perform, and show people Dynamic Malware Analysis. I spent some time trying to come up with a few different diagrams, to show how you can make a pipeline to add Dynamic Malware Analysis for, although, trying to make one simple enough to be understood, and complex enough to be interesting prooved hard, but I eventually came up with a design i liked

I also took this time to write the report i was asked about. This served two purposes. The first being it would act as something to hand in to show that I understood what I have been working on this semester regarding Dynamic Malware Analsis, and the other was that it would help me prove to myself, that I understand the concept well enough to talk about it come showcase. I did have to touch up on some research, and double check some things, although it would be far better for me to be wrong now, than to be wrong on the final day at showcase. After my poster was made, I had a thorough discussion with Faisal, where he asked me a fair amount of curveball questions. He then told be he was happy with how i was discussing Dynamic Malware Analysis, except i needed to put some more passion into it to make it more exciting to listen to. So I am doing that now to try and improve the delivery of my presentation at showcase

14 Showcase

Showcase was a very interesting experience. While the OPS group wasn't one of the most popular groups, we did have a few people come around to ask us what we were doing. I had a good talk with people from all different experience levels with malware and programming. I got some interesting questions such as "Why isn't this technology used everywhere automatically" and "Why isnt antivirus good enough?" I had prepared for these questions thankfully through my grilling by Faisal, who i felt really helped me to get through the night. Most people told me that they walked away knowing significantly more, about not only Malware Analysis, but also about how malware works in general, which I think, goes hand in hand with Malware Analysis