Weekly Planning Diary

**The Challenge**

“Create **a raspberry pi, npcap and wireshark** based **packet sniffing network monitor** that can be attached to **wired and wireless networks** and **passively monitor network communications**. Time permitting explore how anomalous transmissions can be detected using machine learning based modelling of normal network behaviour. This project also requires an analysis of the data protection and privacy implications of the technology.”

**Week 1**

By the end of this project I would like to be able to develop a device that can be connected into any network and provide network diagnostic information. I want the product to be easy to use and it’s information very readable to other people. I would like it to alarm whenever it detects a breach in the network, as well as provide ways of optimising the network. Ideally the device , as simple as connecting the device to a computer in order to begin. This **should benefit a lot of network administrators**, as it will provide a **quick way of analysing the network**, without putting in too much effort.

**Week 2**

I’ve only taken the first steps into the project however I still see the plan envisaged in Week 1. I do wish to add that the device created should **passively monitor the network**, so there is no need for human input (minus to start/stop the device and initial setup).My priority is to enable NPCap to run on my laptop aswell as running it on the raspberry pi. This will enable the collection of packets from the network and thus the ability to **passively monitor network communications.**

**Week 3**

In order to better plan, I have adopted a mentality of working from the product back to where I am at currently with the project.

When I imagine my device in operation I actually two distinct options. Either I could create a device which uses machine learning to detect anomalies in the network or I could create a device which would use multiple raspberry pis in order to fully analyse what is happening in the network. In either case I will have to find a way of wirelessly transferring the packet files from the raspberry pi(s) to my laptop. Once I solve that issue, I will be able to collect and analyse the packet information and feed that into an algorithm. Both of these options will be valuable to network administrators. However, the machine learning approach will provide a more proactive aid in cybersecurity, being able to detect if something is wrong. The other approach will provide a more detailed analysis of the network via the use of multiple raspberry pis, it will be able to analyse specific routes in the network and how optimised they are.

So my priority must be to figure out how **to send the packet files to my laptop**. Also this week I need to read around the two different options. It would be of benefit to **know what existing products** of this nature there are and their strengths & weaknesses.

**Week 4**

I have found a way to transmit files from the raspberry pi to my laptop (Flask) and after researching into existing products it seems that the **most valuable** course of action is to go with the **machine learning option**. This is because there are multiple products on the market which generically analyse the network, however there are none that explicitly state that they use machine learning. Further the machine learning option has only a handful of academic papers on it, so if I made a tutorial on the subject, it would be **extremely valuable** as it **would be a world first.**

Additional Tutorial (Packet Occurrence Barchart)

Another thing I could create to add value would be a video/web tutorial on how to create a Packet Occurrence Barchart in python. This would be valuable as a quick google search yields no results for something like it and I had to circumvent a python library(pyshark) in order to obtain the correct data type for creation of the barchart.

**Week 5**

I plan to run the machine learning algorithm in this week. At the time of writing I am going through the tedious process of cleaning the data.

Once this is done, I will take a step back and analyse my current situation. I will find good academic papers on the subject, to see if they can recommend a better machine learning algorithm.

On Wednesday the 19th of February, I gave birth to my first model. From this, it is now time to take a step back and analyse where I’m at in terms of the project and how far I’ve come

It is now six weeks since the beginning of the semester and 5 weeks since beginning the project. So far I’ve used/done many different technologies/feats which I have never done before, these include (but not limited to and in no particular order);

* Dual Booting a Laptop.
* Learning Linux Commands.
* Emulation.
* NPCap
* Setup of a raspberry pi
* C Code
* WebPage Creation
* Pandas Dataframes
* Flask Web server
* cURL
* Creating Packets
* Creating a Machine Learning Model

I am amazed at how much progress I have made in 5 weeks aswell as how much I have learnt. There is a danger now of losing site of what is important, that being the creation of something valuable. I have made a model, however since there is no validation data set, I cannot tell if I have made a good model. I believe that obtaining a suitable data to run the algorithm on is of upmost importance now, as with this I can prove that this model is valuable.

There are a few options that I can pursue in order to obtain good datasets (in the form of pcap files). I can

1. Search online for datasets provided by institutions.
2. Ask academics at Queens for datasets
3. Obtain datasets from real attacks on honeypot computers.

The plan now is to obtain these datasets, and conduct the experiment, proving that the model works.

In an optimal setting, I would like to use the system in a real-world company with the help of penetration testers to see if the model worked or not. Perhaps even a real attack upon a system would be useful aswell. I say this because right now the program has only worked with static files, so it would be nice to see it working in real time. Alas, we do not live in search a perfect world.

**Week 6**

Datasets obtain the first task is to shift through them and decide which one would be best to use in order to test my model. Then following this, writing code that will test my model.

In terms of the future, I would like the graphical representation of my model to work correctly. This would be very useful as it would show what decisions the model is making “under the hood”.

Over the last week I collated a few dataset resources which may be of value to anyone attempting this project on the future. I shall make either a website or a repo for these datasets so others can have easy access to them.

My end game plan is to be able to sell a box(s) to a company which would handle all of their internal security issues. The device itself will have the ability to cut network access to affected computers and essentially quarantine them. The machine learning aspect of the device will decide which computer is affected and by what attack it is being affected by.  
  
The device it self will be a “plug and play” type of device where a user requires no technical knowledge to set it up. Ideally, for every error a step by step guide should be created so that customers themselves will be able to fix their internal networking issues. Failing that a customer could call a network of engineers who could help resolve the issue.

**Week 7**

At the end of the module I would like to achieve a dynamic network security device which uses machine learning to detect threats. I believe I can hit this goal, if I remove the final bug from my current system. I’m unsure that I will be able to create the physical device itself, nor allow it to break a network connection. I will have to test my model, so I will have to come up with a suitable testing strategy. I have already obtained enough datasets for the project. The required tests to be done on the model can be done within the time frame.

Who would benefit from my project?

As a network manager I want reassurance that my network is secure. Both internally and externally. Right now, there are plenty of cyber security products that deal with external threats, yet very little/no security products for internal threats. I would like a physical device for peace of mind. This device would detect attacked computers on the network and remove them from the network, so that the computes themselves are quarantined from the rest of the network. This device would then provide me with a detailed report of what had occurred, along with possible steps to fix the issue. It would also be kept up to date with all of the latest threats and would not conflict with the external network protection software. I would also like the device to alert me whenever the device disconnects a computer from the network, either by a siren or ,even better, ring or send a text to my phone. This way I can more easily uphold my responsibility of protection the network.

As a high-level member of a company, I would like to keep my company’s secrets, secret. I am already protected from external attacks, yet in order to safeguard against an untrustworthy employee, I would like this device protecting my most valuable digital assets. It is much easier to launch an attack upon these assets if the attacker already has access to the internal network. This device should alert me to an attempted attack and will be able to provide me with the address of where the attack came from. With this I can investigate the device.

I have created a function in python which parses packet data and returns useful information back to the user. This is my magnum opus of the coding for this challenge so far. This function has many uses outside of machine learning, such as plotting graphs of network data, visualising networks and mis configuration detection. I also have made another function which calculates packets per second for a given transmission.

In terms of prioritising what is of most benefit to people, I believe that packaging my current code into a library for people to use is of upmost importance. This means that even if I fail at implementing the model, I will still be able let others use my code in order to achieve that. Updating my github will also be a priority. This ensures that if I do not finish my project, those who come after me will have a head start. Essentially, leaving my work in a state that can benefit someone is of the greatest priority right now.

As my main audience is students interested in my project, the best community to find these people and share my work would be, in my opinion, on a subreddit, perhaps r/Python or r/MachineLearning.