**Diary Entry #1 – Week 2**

**Achieved this week:**

Unfortunately I was ill this week, the first week of project development, and hence was unable to make much progress in the practical side of the project. Some things I did achieve this week include:

* research about the system requirements of both Ubuntu and QEMU, to help decide whether I should dual-boot my laptop or my PC. This research and the knowledge that I am more productive on my laptop than my PC led me to the conclusion I should dual-boot my laptop.
* I also began researching some of the key areas of technology associated with the project. Areas I began looking at included:
  + Ubuntu
  + QEMU
  + QEMU with KVM
  + Honeypots
  + Zero-day attacks

Being totally unfamiliar with both Linux and any kind of system emulation, I began to feel intimidated as I read through the plethora of available online information. I found watching YouTube videos of people explaining the concepts to be much more helpful at this stage than simply reading information from a wall of text; and having gained the foundational knowledge from the videos I found that reading and taking in information from text-based sources became more profitable.

**NEXT WEEK**

Some things I would like to achieve next week include:

* Dual booting my laptop (Ubuntu / Windows 10)
* Install QEMU
* Explore and play about with the capabilities of QEMU

On top of these I will continue reading into the areas of technology associated with the project, as I do not yet feel equipped to discuss them in a tutorial-like capacity.

**Diary Entry #2 – Week 3**

**Achieved This Week:**

* Dual booting Ubuntu / Windows 10: this process took longer than expected due to a number of issues that I encountered. I documented my progress through them below.
* Quick course on Linux terminal.

**ISSUE #1: BitLocker Security** – Disabling secure boot meant I was prompted to enter a 48-digit BitLocker recovery code every time I wanted to use Windows.

**SOLVED**: A bit of experimentation led me to the conclusion that I was going to have to temporarily suspend BitLocker and decrypt the drive for the duration of the Ubuntu installation process. I would attempt to re-enable it later.

**ISSUE #2: Ubuntu installer not allowing partitioning** – At the stage of installation where I should have been able to create my partitions for Ubuntu, I was presented with a blank partition table. At first I believed that Ubuntu was failing to recognize Windows, or that Windows was somehow hiding the partition information from Ubuntu.

**SOLVED**:

* *Attempt 1*: Changed UEFI BIOS settings on laptop, following advice from Stack Overflow and Ask Ubuntu.
* *Attempt 2:* Performed Check Disk operation on hard drive and disabled hibernation function.
* *Attempt 3:* Tried to install an earlier version of Ubuntu with the intention of updating post-installation. When trying this, my laptop failed to even recognize my USB as a bootable disk which led to great frustration.

At this stage I became extremely frustrated and had to take a break. I was discouraged that I had encountered an issue so early on in the process that had stumped me. My annoyance reached such heights that I even considered installing Ubuntu as a sole OS for my laptop; however I decided I would return to the issue later with a clearer mind.

* *Successful attempt*: Researched terminal commands to check that Ubuntu was recognizing any of the hard drive partitions, and discovered that Ubuntu wasn’t detecting any of my drive partitions; not just Windows. This led me to an Ask Ubuntu post that advised I changed the SATA mode on my laptop from RAID to AHCI. After this the issue was resolved and I could install Ubuntu normally.

Upon successfully overcoming the issue I felt a wave of relief, as well as encouragement. Although slightly annoyed that the process had taken so long (around two days) I was glad that I could now progress further with the project.

Another note I made from this process was a feeling of discomfort I got when using the terminal to discover the drives, as I was simply copying what I read on the screen without understanding it.

**ISSUE #3: Wi-Fi** – Having successfully installed Ubuntu, it was failing to detect the Wi-Fi adapter on my laptop. Some research showed that it was likely because there were no drivers for the adapter present. One suggested solution from an Ask Ubuntu page was to simply reinstall the OS, as there is a check box to automatically install these drivers for you in the installation process (i.e., had I been paying more attention during the installation process, I could have checked it and avoided this issue altogether).

*Successful solution*: I swapped to the Windows side to discover the exact specification of my Wi-Fi adapter, and then googled how to install drivers for it on Ubuntu. I used Bluetooth tethering to my phone to access the internet on the Ubuntu side. Again I felt the aforementioned discomfort as I followed the terminal commands for the installation. I decided I should find a quick course on the basics of Linux terminal.

I found a quick free course on Udemy, and went back and reviewed the commands I used previously to better understand them. This made me feel more comfortable with using the terminal.

This week I also watched numerous more videos and read more articles on QEMU, KVM and virtualization in general. I am beginning to feel more comfortable with these topics, however the networking portion of the project is still a daunting prospect to me.

**NEXT WEEK**

For the remainder of this week and next week I intend to achieve the following tasks:

* Get QEMU running on Ubuntu
* Explore network emulation on QEMU
* Complete my tutorial on getting started with QEMU

**Diary Entry #3 – Week 4**

**Brain Dump**

This week I felt particularly motivated to get QEMU up-and-running, encouraged by success in the previous week. I decided to go to the library to see if I would work better there, and discovered that my productivity was much higher there than in my house. I was pleased that the installation of QEMU and starting of my first VMs went largely without hitch; however I felt that most of the tutorials lacked in one area or another, and found myself having to use a combination of them to get good results. Whilst my initial plan was simply to do a How-To guide on networking with QEMU, I decided I should include the installation process with a combination of all the information I gathered from different tutorials, as I think this will be helpful to others who were in my boat.

When I started doing some research into networking with QEMU, I became somewhat intimidated by the information available, as much of it seemed to conflict with itself (which I soon discovered was due to outdated or deprecated documentation still being available, even from QEMU’s own website!). It was during the process of trying to get networking working that I encountered a major problem. Any online documentation I found was EITHER for User-Mode Networking OR TAP device networking, and nigh on NONE of it stated outright that TAP bridging is incompatible with wireless host NICs (something I thought would be very important to mention). This lack of information meant I spent a few days digging in the completely wrong place to find a solution to my networking problem, and I became very frustrated. Due to the fact that I didn’t know about the wireless incompatibility, I thought for certain that I was doing everything right and it just wasn’t working, and I became quite discouraged. Furthermore, this area of the networking was a particularly niche area that I had only really delved into as I recognized the lack of good documentation and tutorials, and wanted to create one to help – it wasn’t necessarily particularly relevant to the project. This led me to include right from the offset of the networking part of my tutorial that there were three different sections to networking; hopefully this will save someone else the time it cost me.

However once I encountered some documentation that mentioned the fact that wireless NICs aren’t compatible with bridging, things started to look up. I spent another few days searching through how to use alternative methods, and again failed to find one source that included *all* the information I needed; I had to alter the steps in many processes to try and suit VMs rather than linking real-life hardware. I was somewhat glad of this discovery however, as once I got it working I knew that the How-To guide I created was going to be valuable as I could yet again combine the information I’d found into one coherent source.

**Things learnt / to learn**

This week was the greatest week of learning for me so far, as I was mostly learning by doing. As mentioned, most of my learning was driven by looking at guides online and by the time I had collected enough information to make my system work I felt like I had browsed half the entire internet. This learning process of taking tid-bits from each tutorial felt extremely tedious, however I decided to stick it out so that I could provide a useful combination tutorial at the end of it. One positive of reading through the plethora of different sources was that I gained a much deeper understanding of what was going on behind the scenes, as I saw the processes used in many different contexts. Although not necessary for the actual tutorial process, I tried to include this important contextual information in my how-to as I felt it was valuable to have (and I knew that readers who weren’t concerned with it would simply ignore it). I prioritized learning about the QEMU system and how virtual networking worked so that I could have a deeper understanding when writing my how-to guide. This also helped significantly with getting my own machine to work.

Some things I would still like to learn about is emulating different devices such as routers within the VLAN. I would like to explore creating honeypots and using the VLAN capabilities of QEMU in a cyber-security capacity, as this is an area I’m completely unfamiliar with.

**TASK PLAN**

(As a short-term note, I intend to spend a good deal of time next week exploring how this technology could be used, to make further entries in this section of the diary more comprehensive. Hopefully after attaining a better understanding of the technology’s potential, I will be able to create a much more concise and educated plan).

* One thing I have been thinking about is designing an intuitive front-end GUI for the QEMU system; particularly one tailored to creating VLANs and for users interested in the cyber-security side of things. I have only been making using of QEMU in its terminal form, and have thought that having a front-end would make the whole process a lot more wieldy. I am aware of existing front-ends for this, and will do some research into the pros and cons of each of these to try and discover where improvements could be made as this would make it useful to others.
* I also thought about including the Argos system in this front-end, however this is an area I will have to explore as stand-alone first.
* I would like to create a device, perhaps on a Raspberry Pi, that was capable of carrying out attacks on my virtual networks and pointing out weaknesses. In parallel, a tool like Argos for detecting these attacks and spotting where the weaknesses are from the attacked machine is something I could look at.
* I enjoyed the process of making the how-to guide, and will likely begin making others along the way if I encounter something where documentation is lacking again.
* I would also like to make some tutorial/explanation videos, as this is a media I find very helpful when trying to learn about new things and there are few videos online regarding QEMU and networking that I found to be of good standard.

**Diary Entry #5 – Week 6**

**Brain Dump**

**Monday:**

Have mostly recovered from illness, so motivation levels are good. However I have a project due for another module at the end of this week, and am expecting my attention to be diverted mainly towards it.

Began exploring the real-world use-cases of VMs connected to VLANs. Took a look at the Argos tool, and did some research into Honeypots and other forms of network security. Found the concept of a honeypot very interesting, and came across the concept of high-interaction honeypots that make use of multiple virtual machines. Also came across the concept of deception technology, that I will look into later.

**Wednesday:**

Attempted to get the Argos tool running on my machine, but encountered an issue with setting up the VLAN. Unfortunately it is not working how I expected it to, and will need to spend some time getting that part up-and-running before attempting to go any further.

Tried following some tutorials and walkthroughs online, but to no avail as of yet. I also realized that I will need to edit my tutorial, as this area is covered within it and it may not work for others as they expect either.

Was unable to get it working today.

**Thursday:**

Tried again for a little while to get the virtual network running as expected in preparation for using Argos, and again was unable to get it working. I began to get quite frustrated again, as it seems as though I am doing everything right but it simply won’t work. I had a feeling it was to do with the assigning of IP addresses, so I did some more research into that area however I will need to do some more in order to better understand it.

Doing work for my other project took up the bulk of my working day today.

**Things learnt / to learn**

This week I feel like I have dipped my toe into a vast area of networking. My discovery of the concepts of High-Interaction Honeypots and Deception technology has excited me to delve more into these areas. I now feel better equipped about the scope of where the project could go, as these areas appear to go quite deep and complex. I have also learned a great deal more about virtual networking and IP addresses, as well as some more about virtual machines.

I still don’t know exactly how I will implement any new features for the project, however this will hopefully come with some more research and conversations with Dr Bustard.

**TASK PLAN**

This week I feel like a gained a great deal more knowledge on where the task could possibly go. The Argos website mentions a new generation of honeypots to automatically identify and deal with zero-day worms and other attacks. The area of honeypots in general is something that interests me, however I have not done enough research or practical testing to be able to determine exactly what I could work on to make advancement in this area. I intend to discuss this at the next meeting, as I am feeling a little lost on how to make practical progress on the project (even after overcoming my current technical blip).

**Diary Entry #6 – Week 7**

**Brain Dump**

**Tuesday:**

Today I attempted to get the private isolated network running (in order to make progress towards the project goal). I attemtped using a network bridge and TAP devices in order to connect the devices together, without connecting them to the actual network. Whilst I managed to get the devices successfully connected to the bridge, they failed to communicate with one another across the virtual network. I tried looking through and following the tutorials of many websites, but to no avail.

**Wednesday:**

Today I made another attempt to get the private isolated network functioning. Unfortunately however, after following a certain online tutorial the OS on my laptop began to fail to recognise the presence of a network card on my laptop. This was an issue that I had encountered at the beginning of the project process, and so I was able to go back to my documentation and fix the issue with few problems, however to have such a strange problem at this stage was quite discouraging. Tomorrow I will continue to attempt to get the isolated network to work.

**Thursday:**

Today I am very relieved to say that I managed to get the private isolated networking functioning properly. I tried a few more last-ditched attempts at self-configuring the network through the terminal, however discovered that some GUI tools would provide the correct networking configuration tools for you. I installed software known as Virt-Manager, which allows the handling of VMs with a GUI front-end. Using Virt-Mangager and following a few YouTube tutorials, I was able to get the private isolated network running. I intend to look into the source code of Virt-Manager in order to understand the inner-workings of what goes on with its network wizard, so that at a later date I could perhaps attempt to make it work manually again.

Having got the private isolated network functioning and tested, I have begun updating my How-To guide with the appropriate steps to follow, so that others may have an easier time of completing this process than I did.

**Things learnt / to learn**

This week I learned a lot more about how networking works with VMs. However there are a lot of areas that I need to learn more about; I am going to look into the source code of the Virt-Manager tool in order to try and better understand how it creates the isolated private network. Hopefully then I will be able to manually configure a private network myself. I also need to learn more about how KVM in general handles the networking of VMs, so that I can better provide information to others in my How-To guide. I also need to learn more about the emulation of different kinds of network devices and protocols, as currently the only devices being emulated in the network are PCs - whereas in attempting to emulate a full-scale network there are many different kinds of devices and servers running that would be very useful to emulate.

**TASK PLAN**

The end-goal of this project is to have a piece of software or software-hardware configuration that can emulate the entirety of a prospective business or organisation's network. The tool would be designed for network admins, and should allow for all kinds of devices and servers to be emulated; a complete carbon-copy of the organisation's network so to speak. This could include built-in security testing features, such as penetration testing to allow the network admin to test the network without causing any real damage. This will involve the emulation of a VLAN, or private isolated network that is disconnected from the real-life network. This system should also provide system monitoring, to detect incoming attacks aswell as creating them. Any issues I encounter along the way will be documented, and I will provide walkthrough guides for the issues where they don't already exist so that others may have an easier time of creating the project.

Recent steps towards this goal include the successful creation of a VLAN, and short-term goals include getting the Argos tool working, which will allow for the network monitoring part of the system to be integrated.

**Diary Entry #7 – Week 8**

**Brain Dump**

**Monday:**

Wrote initial script for blog post, and began working on new sections for my how-to guide. The new section will be about isolated networking with QEMU, as mentioned in last week’s diary entry I found it very difficult to find useful tutorials and walkthroughs in this area – I feel that a more clear and complete How-To guide will be useful to other people who wish to undertake this task in the future.

**Wednesday:**

Completed the blog post write-up. I have written the blog post with the intended audience of someone like myself who is completely new to the whole area of virtualization (and even Linux). The post is written to be light and easy-to-read, in an attempt to contrast the dull and official nature of reading ordinary walkthroughs and documentation. The post is also not written to be a stand-alone walkthrough – readers will be directed towards my How-To guide(s) to get the technical information that is being discussed in the post; this helps improve the posts readability as it is therefore not filled with technical jargon. The main purpose of the post is to help someone who may wish to advance my project to get caught up on how I reached the stage I am at, and I will continue to update it as the weeks progress.

**Thursday:**

Converted the blog post from its’ word format to a singular HTML document for the purposes of submission. I followed the previously provided walkthrough on how to make an HTML file to complete this process.

**Things learnt / to learn**

This week my learning section is barren, as I spent my time working on my blog post for this Friday’s submission.

Next week however I intend to delve into the source-code of Virt-Manager in order to understand the inner workings of its network wizard, in the hope that I might be able to manually configure a private isolated network. This will help me to provide a more in-depth and valuable How-To guide to other future users.

**TASK PLAN**

It is clear now that the initial end-goal of the project is not going to be achievable within the time-frame of the module (although I will likely continue working on the project after the expiry of this module). After doing some thinking and looking around, the most valuable output I can hope to have with the given time left is to construct a few more How-To guides in the areas of the project that I have been frequently finding under-documented. These areas include wireless bridge networking and isolated virtual networking. I will provide in-depth How-To guides in these areas, in the hope that if someone was to come and continue to work on my project they would be able to glide over all the issues I have encountered so far and go straight to making new ground.

The How-To guides will be written with a similar target audience to that of my blog post – people like myself who are complete beginners to virtualization. I chose this target audience as I feel that the current walkthroughs and documentation are far from ideal for this group, as within many of the articles some previous knowledge is assumed. This meant that I had to bring together the information from many sources in order to get something to work – a process I hope to relieve further developers of with my How-To guides.

I will continue to work on the technical side of the project where I feel it will help me write more in-depth guides; and time-permitting may work on towards the initial end-goal of the project mentioned in previous diary entries.