In this module of my master's degree, I have learnt that network security is important in an organisation or a website. Over the six weeks of the module, I learnt some important aspects of network security such as the cyber kill chain model. Understanding the importance if the model made me understand the process of how a potential cyber-attack is executed. With this in mind, it ensured me that in order to protect a network, it is vital to understand the process of how a cyber criminal prepares the attack. Using this technique, to be able to mitigate the attack and reducing the risks, one should think of how the cyber-criminal plans and be vigilant with possible vulnerabilities the network possesses, therefore its vital to perform regular penetration tests on the network.

During the module covered, there were several activities that I was required to participate in. Some of the activities included participation in seminars and module activities that included scanning of the website chosen.

During the vulnerability assessment, I realised that I was unable to load the website I had selected. After several attempts on different web browsers and network, I was unable to load the website. As this was going to affect my vulnerability assessment and future activities, I decided that it would be better for me to change the website choice which would allow me to use the website for the rest of the module and contacted the lecturer of the module.

While I was attempting the scanning activity of my chosen website during unit 3, I had a few challenges in extracting the information required. As the weblink available on the activity brief was to a tutorial on how to use the traceroute command, I was only able to get some of the information. As traceroute only provides the number of total hops it takes to reach its final destination with the time it takes at each hop, I was

unable to extract information from the output such as the nameservers, mx records. While going through the recommended reading material form the module resources, I realised that the WHOIS command will be able to provide the relevant information required.

The second seminar of the module was regarding the top 15 data breaches within the 21st century. As part of the seminar, we were to each discuss one of the 15 data breaches and present during the seminar. I was able to present my findings on one of the data breaches. I had chosen to present about Adobe's data breach. The presentation went well however due to some technical challenges during the seminar once I presented, I had lost connectivity and reconnected. When I reconnected again, I missed the comments. As I had missed the comments and feedback, I later went back to the recording of the seminar, and I received positive feedback from the lecturer, and I was proud from the feedback. By presenting this in the seminar, I was able to share my thoughts and contribute to the seminar.

As part of the module activities during the course was to be able to scan the chosen website and extract possible vulnerabilities, open ports, etc. As this activity required scanning of the website, there are many tools and options on how to scan the website. At first, with the number of options available such as online tools and tools available via the Kali Linux operating system, I had quite a few options to choose from. Once I analysed the tools to scan the website, I chose to opt for installing Kali Linux on a virtual machine to perform the scanning of the website. I chose Kali Linux as the operating system is widely used for performing scans on networks or websites. The scanning tools available are preferred for such an activity. I had a few challenges while

scanning the network for open ports and vulnerabilities on the second attempt of the website. In order for me to overcome this difficulty I researched further on the vulnerability name in order for me to get further details on the vulnerability risks as I was unable to scan the domain again during the vulnerability assessment to gather the details.

The collaboration discussion topics were interesting however there was not much discussion and contribution from other colleagues in the module. I did however contribute positively towards the discussions and shared my thoughts on the respective topics. There was no motivation to include my summary of the discussion to the collaboration discussions. I felt that as this was not compulsory to contribute and no marks were being awarded towards the final grade of the module, other students did not take it seriously.

Overall, this module was a great learning experience for me as I did contribute to all possible activities assigned ensuring the best learning outcome is achieved. I particularly enjoyed the practical aspect of trying to scan the website as this gave me the opportunity to experience scanning a network in order to detect vulnerabilities and understand what it would be required to scan a network of an organisation. It would have been great for me to understand how to mitigate the vulnerabilities and reduce the number of open ports reducing the vulnerability risk.