What:

In this module, I learnt about network security and vulnerabilities, including best practices to network security, modern scanning tools and attack techniques, vulnerability testing and assessment, security breaches, logging tools STRIDE and DREAD standards and much more. I also learned about various tools such as NMAP, Zed Attack Proxy, and Kali Linux software distribution that can be used for testing and scanning to perform an assessment and generate vulnerability assessment reports. This was eye-opening since I had never used such tools before. These tools were genuinely incredible. Furthermore, I learnt about the STRIDE and DREAD standards, which help identify potential threats and evaluate their severity, and the Cyber Kill Chain model, which outlines the different stages of a successful cyber-attack.

So What:

Throughout this module, I completed different activities which helped me learn about cyber security case studies, and I have researched different vulnerabilities and scanning tools. I have also participated in group discussions which helped me understand and learn about the other student's points of view. The activities were engaging and informative and helped me understand network security and vulnerabilities better.

Working on these activities helped me really understand how vulnerabilities are detected and how to mitigate and patch them. However, at times, I felt overwhelmed with the amount of information presented, and it was challenging to keep up with the pace of the course due to having two full-time jobs and doing this unit. However, I found that reading other student's posts and doing a ton of research helped me to understand the subject much better.

One of the key things that produced my learning in this module was the practical assignments that required us to apply our knowledge to real-world scenarios. Analysing a real website challenged me to think critically, identify potential threats, and develop solutions to mitigate them. I personally have never written an executive report before. Doing it for the first time was both challenging and exciting all at once. I really enjoyed producing it.

One of the things I didn't do as much is work and preper for my final thesis. Since the first day I joined Essex University, I've started learning and working towards producing a simple operating system on the ARM64 architecture. I wish I had more time to work on this more, but sadly, my progress wasn't as much as I would have liked. So far I have learned about the ARM64 architecture and how to create a simple bootloader which I have deployed successfully on my Raspberry PI device. Simply doing that took a lot of effort and research, but it was worth it. I absolutely love creating complex software like operating systems and game engines. I believe if I can create a simple OS for ARM64, many doors will open up in my career, which I am really excited about.

Now What:

Overall, this module has given me valuable knowledge and skills to apply in the real world. For example, I now understand the importance of conducting regular vulnerability assessments and creating documents explaining how to mitigate it and recommendations for network security. Additionally, I have learned about various tools and techniques that can be used to detect and prevent security breaches, such as logging tools and Kali Linux software distribution.

I have actually used these tools to test out our server at my full-time job to see if I can detect any vulnerabilities. I found a few I will be working towards fixing whenever I get the chance. Currently, our software is not public and is in the alpha stage so there is no rush.

In terms of evidence of my learning, I have produced a vulnerability assessment report that outlines potential threats and provides recommendations for mitigation. This report includes references to relevant literature and citations to support my findings. Additionally, I have developed skills in using NMAP, Zed Attack Proxy, and other testing tools, which I can apply in a practical setting.

Additionally, one of the most important takeaways from this module is the importance of maintaining constant network security audits because, as technology advances, new vulnerabilities and threats will emerge. Therefore, staying up-to-date with the latest tools and security threats faced by organisations worldwide is essential.

In conclusion, this module gave me a solid understanding of network security, vulnerabilities, scanning tools and framework for writing documents and reports. Furthermore, I have learned about multiple tools and techniques that can be used to detect and prevent security breaches. I have also developed the skill to conduct vulnerability assessments and audit reports. Moving forward, I plan to continue building on this knowledge and applying it in the real world to enhance my network security skills and prevent cyber attacks.