Individual Reflection | Network Security

Executive Summary

Overall, the module was informative and interesting, leading to good opportunities to develop IT and Digital skills while developing foundational skills of research and problem-solving. The module also presented good opportunities to develop a fuller understanding of the ethical issues in the sector. Activities have been recorded in the e-portfolio.

There were, however, many barriers to overcome when completing the module, stemming from a lack of prior knowledge or professional experience in the IT sector. While the module may have been well sequenced for those who work in, or have experience of, the IT sector, the technical challenges required additional time and persistence to complete. Time management was also a barrier as it would have been better to complete more to the practical activities that appear later in the module to bring the theory to life.

Unit 1 | History of Network Security, Vulnerabilities and Approaches

This unit provided a good introduction to network security. There was, however, a steep learning curve in terms of learning lots of new technical language. This was compounded by not working in, or having a professional background, in information technology (IT) or any prior knowledge of network management beyond the very basic introduction from the 'Launching into Computer Science' module. The signposting to texts within the reading list was also challenging as some articles were more helpful than others both in terms of accessibility and relevance.

Due to the wealth of content being presented in an unfamiliar context, it was challenging to complete all of the optional tasks by the informal deadlines. For example, completing the reflections on the security implications of the digital economy could only be completed to a reasonable standard after further reading, research and familiarisation with the topic.

This was a fast-paced start to a complex module, placing and significant demands on subject knowledge, research skills and time-management.

Unit 2 | Advanced Persistent Threats: Applying the Cyber Kill Chain Model to a Case Study

There technical element of the course assumed a level of practical understanding of the technical aspects of penetration testing. While some understanding can be gained from reading case studies and research, knowledge acquisition is deepened by doing. It was challenging to attempt to fully absorb the literature review without the chance to complete, or simulate, scanning activities and other methods of penetration testing (which happened later in the module)

Unit 3 | Vulnerability Assessments

The vulnerability assessment brought together the technical aspects of the research. The feedback from the assessment was accurate and highlighted the higher scores (Distinction) relating to the more conceptual side of the topics and issues, but less well (Merit) regarding the application of knowledge. This had led to some frustration as the application of knowledge (ie practice penetration testing) is covered later in the module.

UNIT 4 | BREACH ANALYSIS AND MITIGATION

The unit provided an opportunity to practice the penetration testing techniques. While ultimately enjoyable, this provided a great deal of frustration but did enhance and develop problem solving skills. By completing the scanning activities, a there was a significant gain in IT and Digital skills. For example, before the penetration testing could start, a Linux environment needed to be installed. The concept of setting up the required virtual Lunix environment using Oracle VirtulaBox was something completely new and quite challenging, particularly as the information in the reading lists led to some dead-ends. These must have been deliberately placed in the reading list to provide enough of a trail to complete the task, but also to emphasise the need for independent research.

Having no prior knowledge or experience of Lunix or networking was a barrier to completing the penetration testing. However, working through the scans made the literature come to life. It was sometimes, quite challenging to interpret the results without a deep practical experience of networking.

UNIT 5 | LOGGING, FORENSICS AND FUTURE TRENDS

Reviewing the assessment reporting template was helpful in terms of understanding industry standards for reporting the results of penetration testing. It was also interesting to begin to grapple with the industry standards such as IEEE, CVSS alongside government requirements such as GDPR. This highlighted the issues with global threats and state legislation. This was neatly highlighted as the report template came from the US, but the frameworks from the ICO or NCSS are overseen by the UK government. This left an unanswered question, perhaps for independent exploration, regarding how governments can, or should, hold technology companies to account. This is a topical issue today in terms of the tension between individual privacy and national security as highlighted by the position for encryption taken by both Apple and Meta in the UK.

UNIT 6 | THE FUTURE OF THE INTERNET AND GENERATIVE AI

The use of generative AI is interesting challenge for network security. Again, this highlights ethical issues for consideration, as well as the technical challenges presented by AI. For example, an issue with AI is ‘hallucination’ which is yet to be fully understood but results in false or misleading information. Perhaps a more pressing concern would be the ethical standards and regulation of AI. The impacts of AI are, and will be, global while effective legislation and controls would require international cooperation.