The module introduced me to a variety of subjects, including the history of networks and their vulnerabilities, an introduction to the Cyber Kill Chain concept, and a case study on the advanced persistent threats (APT) responsible for the SolarWinds supply chain incident. In addition, the module addressed industry-relevant concepts such as vulnerability assessment, penetration testing, baselines, and strategies. It also went into the defensive side of analysis of breaches and possible mitigations, as well as a lively debate on the necessity of logging, monitoring, and forensics, ending in a puzzle where we speculated on the future of the Internet.

For the activities covered in the module, the following were my primary responsibilities:

1. I was required to undertake a baseline review and design a strategy for evaluating a website for security flaws.
2. The last step was to do a vulnerability and risk assessment on the website and give a short report of my findings.

During the baseline evaluation, I reviewed the recommended reading material inside the study portal and used several external types of extended reading in the form of blogs and online tutorials. I gained a deeper understanding of how web-applications are scoped for a project and of different evaluation methodologies and frameworks, such as NIST and OWASP Top 10. This information assisted me in evaluating my baseline strategy, which was mainly based on it. Throughout the preparation of this paper, I was able to examine the many limits of guidelines and how they do not illuminate the other legal and managerial restrictions of an application. This is when I learnt the significance of management systems and audit in the form of ISO27001, as well as the legal viewpoint in the shape of privacy regulations and the GDPR. With this information in hand, I was able to construct a proposal that met all of the highlighted criteria and checked every box on the checklist.

In the executive summary report, I relied on my limited experience as a penetration tester and used a number of industry-appropriate approaches to conduct vulnerability assessment and penetration testing. On the chosen website, I was able to identify a number of security flaws and GDPR-related legal violations. During the course of the evaluation, I was able to identify over 10 vulnerabilities. Due to some of the scans, the website prohibited my network activity, therefore I had to use an alternative network proxy and route to circumvent this.

I was able to finish each assignment independently with the aid of recommended readings, accessible lecture casts, tutor-led seminars, and online extended reading. No activity was too complicated or lacked required components. On the discussion forum, I was unable to share my expertise and insights with my colleagues. Due to my office's excessive workload during collaborative weeks, I failed in this regard. However, I did read everyone's input, and it was a delight to read such fresh and succinct ideas expressed by my peers.

I was enthusiastic about doing the tasks of drafting a paper, conducting a baseline assessment, executing penetration tests, and scanning for vulnerabilities. It was enlightening to learn about different tools, such as nmap, Nessus, dirbuster, OWASP ZAP, and Kali Linux, an operating system geared for penetration testing. These exercises were enjoyable and difficult, and I was able to acquire many new strategies and methods. This information enabled me to use it at work and made me feel happy with my efforts.

Because it was less about "what the application was doing" and more about "what I could make it do”, with this I was able to explore new frontiers and think outside the box as a result of these activities. In addition, it compelled me to consider many viewpoints and approaches and helped me create a more critical way of thinking and approach.

As proof of my growing abilities and knowledge, I am now acquainted with a whole new operating system and its numerous tools, which accomplish a variety of tasks using both automatic and manual processes. I am certain that I can use these insights to safeguard a range of websites and systems.

Throughout the course of this module, I have attempted to use proper citations and references that demonstrate a wide reading as well as additional work placed into the practicality of the needed activities and submissions. I have made it a priority to generate academically concise work with the needed level of integrity by paraphrasing, referencing, and attributing sources of information when relevant. I have also incorporated each and every reference that is accurate and pertinent to my created work.

**References**

* GDPR.eu. (n.d.). Chapter 3 (Art. 12-23) Archives. Available from: https://gdpr.eu/tag/chapter-3/. [Accessed 23 Jul. 2022].
* OWASP (2021). OWASP Top Ten. Owasp.org. Available from: https://owasp.org/www-project-top-ten/. [Accessed 23 Jul. 2022].
* NIST (2019). Cybersecurity Framework. NIST. Available from: https://www.nist.gov/cyberframework [Accessed 23 Jul. 2022].
* ISO - International Organization for Standardization (2019). ISO/IEC 27001:2013. ISO. Available from: https://www.iso.org/standard/54534.html [Accessed 23 Jul. 2022].
* PWC (2018). Inside the mind of a hacker. THE BLOG. Available from: https://blog.pwc.lu/the-mind-of-a-hacker/ [Accessed 23 Jul. 2022].
* TEDx Talks (2012). Top hacker shows us how it’s done | Pablos Holman | TEDxMidwest. YouTube. Available from: https://www.youtube.com/watch?v=hqKafI7Amd8 [Accessed 23 Jul. 2022].