Please find the module ePortfolio under
https://essex.sevale.de/modules/network-security/eportfolio/

The Network Security module introduced a diverse set of activities, including seminar presentations, practical exercises on website fingerprinting with the use of command line tools, security and compliance audit of a website. To better reflect on my learning experience, I will use Gibbs' model, which provides detailed guidance for that (Gibbs, 1988; University of Sheffield, 2024).

As a result, I gained hands-on experience with network analysis tools like `traceroute`, `dig`, and `whois`, and worked with the penetration testing tool Zed Attack Proxy (ZAP). The assignments not only introduced me to identifying and testing vulnerabilities like cross-site scripting (XSS), SQL and CRLF injection, and other, but also deepened my understanding of standards relevant to modern businesses like General Data Protection Regulation (GDPR) or Payment Card Industry Data Security Standard (PCI DSS).

The module forums and discussions highlighted the operational side of cybersecurity, how analysts are overworked and do not have the capability to process the massive quantities of alerts they face, which negatively impacts both the individuals and the enterprises (Vectra AI, Inc., 2023).

Feelings

As the module first started, I felt anxious and was concerned about the six-week format: it meant that the module will be more intense. However, I was pleased to notice that this also encouraged engagement and made me more focused. Working with ZAP was a completely new area for me and overwhelming at first. However, as I gradually explored

the tool and grew to understand its testing and reporting capabilities better, I felt more comfortable with the tool and the assignments.

Similarly, in the beginning, I hesitated about making a presentation during a seminar, but I ultimately enjoyed the process of preparing slides and sharing my findings with the tutor and my peers. I especially appreciated the communication it encouraged, even though we did not have a chance to debate on the topics properly.

Evaluation

I appreciate how the seminars fostered engagement and allowed to research topics in more depth, and the assignments were built on top of each other, guiding me through the module. The practical nature of the assignments like using ZAP allowed me to better understand some concepts like XSS, which I struggled to visualise earlier. Besides, I feel that my time management was better in this module than before: even though I had some personal commitments to tend to, I had plenty of time to prepare seminar presentations and module submissions.

At the same time, it seems that some interactive components did not work well like the forums or seminar discussions. Some aspects of the assignments remained confusing, like the evaluation of compliance against complex regulations or standards.

Analysis

My initial confusion with ZAP stemmed from how new the area was for me. Previous modules required developing software, which I'm quite familiar with. And while they might have introduced new concepts, the underlying structure is always the same. With security testing, the tool did not have any familiar elements, and I had to gradually

investigate how it works and repeat scanning multiple times until I grew familiar with the process.

The vulnerability assessment tasks highlighted how different resources like Open Worldwide Application Security Project (OWASP) and Common Weakness Enumeration (CWE) are from standards and regulations like GDPR and PCI DSS. While the former provide clear definitions, step-by-step guidance, and clear examples, the latter fail to provide compliance checklists, which in my opinion, can impact the proper adoption of the standards, as this complexity should interfere with developers' and analysts' understanding of the standards. My main conclusion is that a lawyer specialising in information and communications technology (ICT) regulation is essential for compliance evaluation.

Conclusion

In this module, I gained practical experience with security tools like ZAP and had a chance to look at other familiar tools like `traceroute` from a new perspective. The integration of ZAP with CWE and OWASP resources, as well as their good organisation, allowed me to grow more familiar with them and navigate them with more confidence. While compliance assessment remained difficult, I still gained more awareness about the regulations relevant in the UK and the EU.

An outcome that I did not expect is discovering my interest in the human side of the ICT, the analyst wellbeing and how to improve it. This side of the discussion arose coincidentally, and I feel that the module could also focus more not only on the technical side of cybersecurity but include the organisational challenges as well. After all, behind

any processes there are people, and it is important to understand how they work and what challenges they face.

Action plan

I find the knowledge and experience gained in the module quite valuable, and I believe I will continue to use ZAP in practice, including my current position, where it could help detect server vulnerabilities. Similarly, CWE and OWASP resources provide useful guidance on developing secure software that I plan on referring to in the future.

I intend to continue exploring the organisational aspects of ICT in further modules, as it is vital for professionals to be not only well-versed technically, but also be satisfied in their roles.

References

Gibbs, G. (1988) “Learning by doing: A guide to teaching and learning methods,” *Further Education Unit* [Preprint].

University of Sheffield (2024) *How to reflect in an academic context*. Available at: https://sheffield.ac.uk/study-skills/university/independent/reflect (Accessed: September 7, 2025).

Vectra AI, Inc. (2023) *2023 State of Threat Detection*. Available at: https://www.vectra.ai/resources/2023-state-of-threat-detection (Accessed: August 12, 2025).