ePortfolio URL

https://micjustus.github.io/essex-eport2/modules/m04-nism.html

---

Contents

End of Module 4 Reflection

Network Information Security Management

This module's content provided a good introduction to networking, vulnerability scanning and importance of data standards. Despite working in the IT field for twenty years, it was enjoyable to read the history of the internet and challenges faced by ISO and IETF to establish a dominant networking protocol (Russell, 2013). Unsurprisingly, IETF's implementation of TC/IP succeeded because of it was open and free—like the Sony Betamax and VHS war (Liebowitz and Margolis, 1995).

The module introduced IPv6 as a solution to IPv4 address limitations. However, if IPv6 is a great solution (which I believe it is), why then do most networks today still run on IPv4? I consider that Network Address Translation (NAT) and IPv4's easy-to-memorise address format are reasons behind its continued use. I found the book by Parziale et al. (2006) a valuable read that helped me better understand networking concerns, though I think chapter 2 (network interfaces) and chapter 3 (internetworking protocols, save for content about Dynamic Host Configuration Protocol) are irrelevant to this module because the content is too in-depth.

Transmitting data between networked devices—either via IPv4 or IPv6— and processing that data involves several data standards such as GDPR which served a core theme throughout this module at the exclusion of other standards such as ISO 27000, especially ISO 27017 aimed at cloud environments. HIPAA and PCI DSS standards were briefly addressed, but due to GDPR's prominence, I think it is good to focus on GDPR because many organisations require IT professionals who understand the importance of data privacy.

Overall, I found the content of this module relevant and well-suited as a high-level introduction to networking and information security.

Contributions and Teamwork

In our team setup, by agreed to allocate one member to manage meeting schedules and another to capture meeting notes using a self-organising approach (Magpili and Pazos, 2018). We established the scope of delivery and discussed our experiences from previous modules regarding tables, diagrams, academic references, and word counts applicable to our design proposal and final project.

We also engaged often and shared research findings with each other for further consideration. For example, I shared the following to raise awareness of recently identified security issues that made the news:

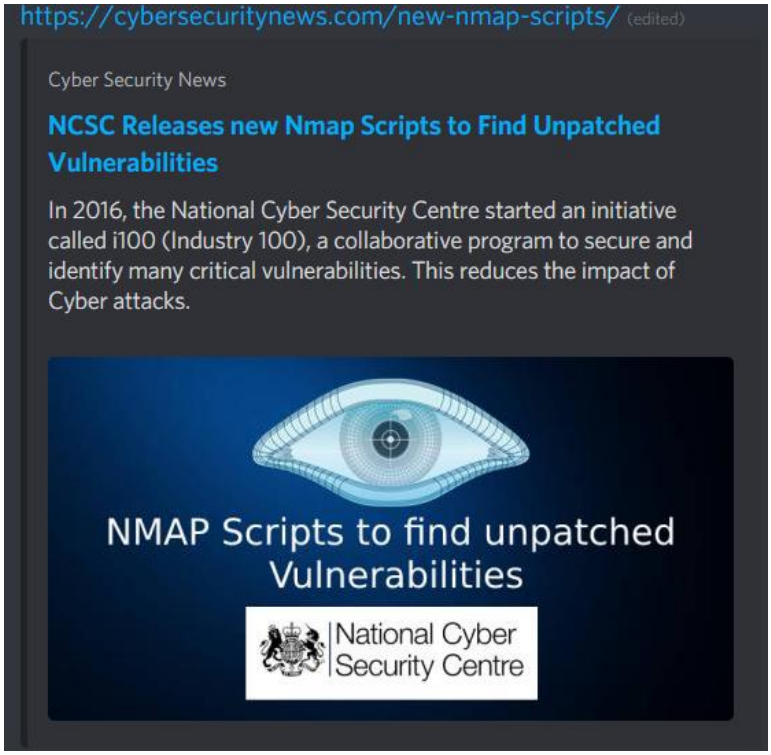
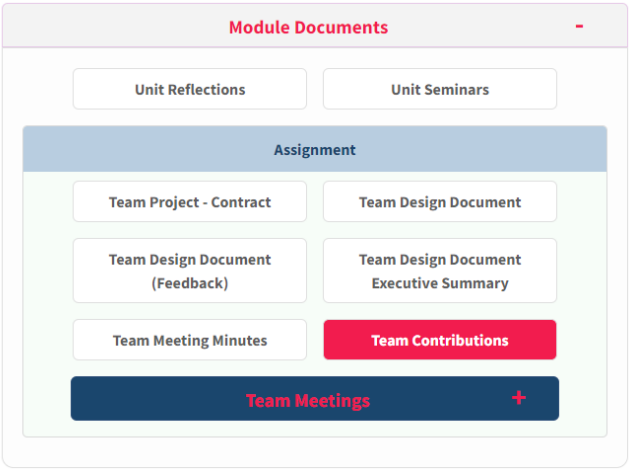


Figure 1 Vulnerability scripts

Figure 2 Log4J zero-day vulnerability

Additional contributions (links) can be viewed from **Team Contributions**

(additional contributions located under here



We held regular team meetings which helped sustain a common sense of commitment, to act as a professional and deliver on assigned tasks within the allotted time. Compared to previous modules, I think we were more focused in our team meetings and mindful of each member's personal time arrangements. Though we did engage with banter, we kept it short and ensured we moved onto the topic for discussion.

Overall, I enjoy working with team members who are engaged with the content and actively participate and look forward to doing so in future modules. Working with students such as members from our team gave me a positive learning experience, something worth fighting for.

Design Proposal versus Final Project

Working on the design proposal was a pleasure because a decent word count was provided, and we leveraged experience to guide the structure and content. In contrast, the final project was challenging and less engaging because of the difficulty matching *theoretical* vulnerabilities to *practical* penetration testing tools. I often asked myself if I was using the tools correctly. There was no clear link between vulnerabilities described by our chosen framework (OWASP Top Ten) and results of the scans because the website was already quite secure.

Unfortunately, this caused me to lose interest in this activity. Questioning why, I concluded that: (1) I *expected* to encounter actual vulnerabilities; (2) I had no experience using penetration tools in Kali Linux; (3) I had to sign up for a VPN service; (4) no "aha!" moments that triggered further investigation. The experience would have been much better if I could

identify actual vulnerabilities which the module introduced, such as data leakage. Another issue was the duplication of scan results from other members due to tools we chose to use.

Delivering the executive summary, I do not feel we cleanly mapped between design proposal and actual results. Although I am happy with the final project, I would advise a different approach to develop the proposal: first look at the tools to use and the vulnerabilities they can detect and then work the final project accordingly. Thankfully, we asked for guidance from the module tutor regarding data focus and in response, removed pages of irrelevant summary data.

Collaborative Discussions

The collaborative discussions had little engagement from fellow students. I observe that some discussions receive interactions while others do not. And I consider *why*. Unfortunately, a collaborative discussion topic like using ping or traceroute is of no value given there is only one outcome. How many ways can students say the different things about the same tools? Goshtasbpour et al. (2021) list 12 tips which I believe are generally met for collaborative discussion, but I think text-based discussions versus human interactions often leads to disappointing engagement levels.

In contrast to the abysmal collaborative discussion 2, presenting a selection of choices for discussion was refreshing: an “aha” moment. I opted for a data breach case study that highlighted how data was used (unethically) to model citizens' religious and gender preferences. Such a case study justifies the need for data privacy regulations as GDPR, without which, I think society—lacking knowledge and protection—is open unintended consequences of influence by institutions who seek greater control over people’s lives.

EPortfolio and Unit Reflections

I reworked the layout for this module's content based on feedback from the previous module's tutor such as opening the portfolio on different screen sizes and content focus and the format of other colleagues' portfolios.

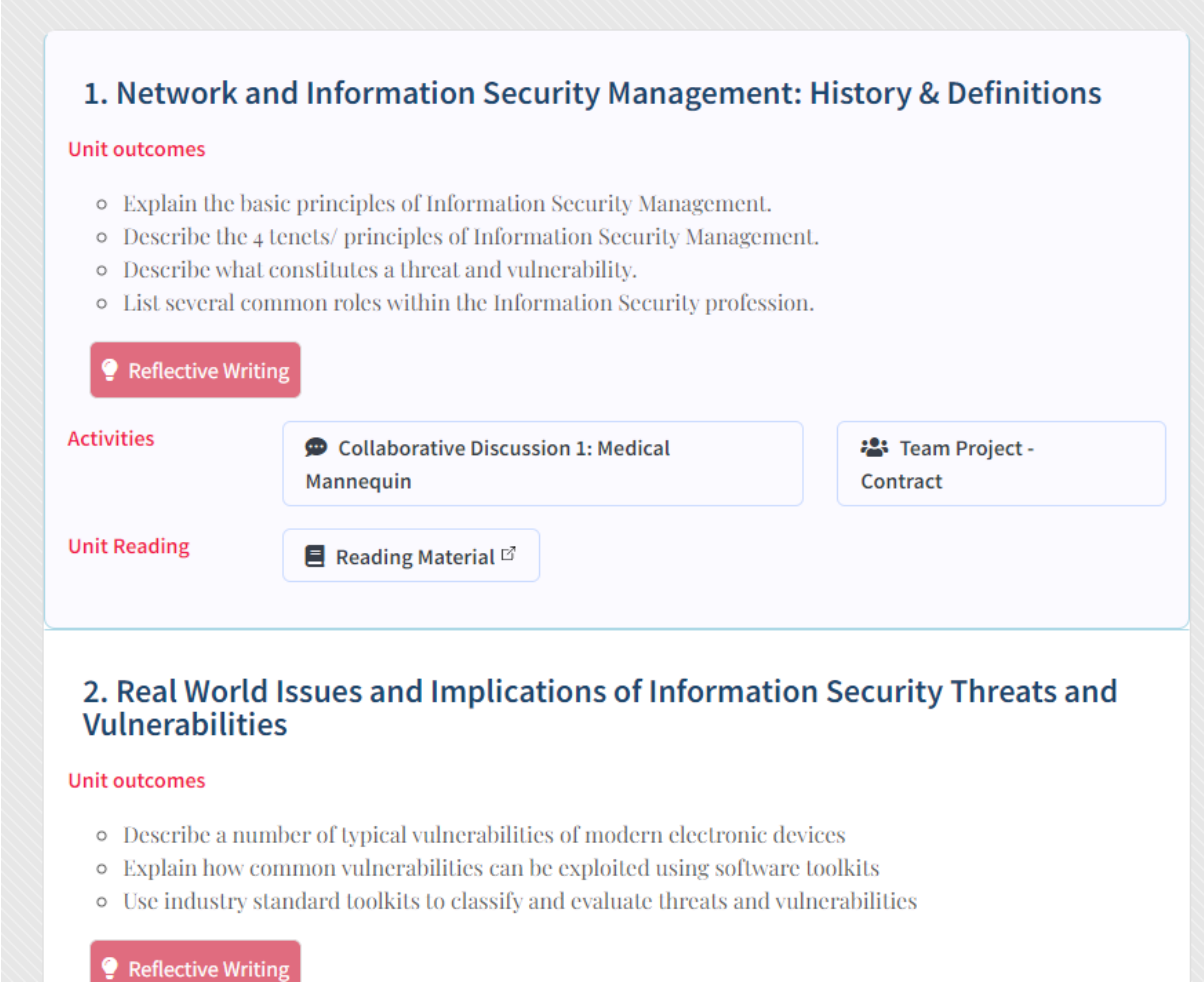


Figure 3 New module layout

I settled on the above approach because it is (1) simple to navigate, (2) clearly identifies artefacts of each unit and (3) enables quick navigation to each unit on smaller screens. I enjoyed developing the portfolio that continues to expand my experience of CSS and JavaScript, skills in demand for today's online world. Despite that I find no personal value from the e-portfolio, I extract great value from the *practical* aspects of building and maintain it because the *skills* enable me to deliver better software.

References

Goshtasbpour, F., Swinnerton, B.J. & Pickering, J.D. (2021). Twelve tips for engaging learners in online discussions. *Medical Teacher*:1-5.

Liebowitz, S.J. & Margolis, S.E. (1995). Path dependence, lock-in, and history. *Journal of Law, Economics, & Organization*:205-226.

Magpili, N.C. & Pazos, P. (2018). Self-managing team performance: A systematic review of multilevel input factors. Small Group Research, 49(1):3-33.

Parziale, L., Britt, D., Davis, C., Forrester, J., Lui, W., Matthews, C. & Rosselot, N. (2006) TCP/IP Tutorial And Technical Overview. 8th ed. New York: IBM. Chapters 1-5

Russell, A.L. (2013). OSI: The internet that wasn't. IEEE Spectrum, 30.

Thomas, D. & Hunt, A. (2008). *The Pragmatic Programmer: from journeyman to master*. Massachusetts: Addison-Wesley.