https://github.com/s5miller88/e-portfolio
https://s5miller88.github.io/e-portfolio/Module%202.html

Reflective Piece:

Seminar Reflections:

Over the course of this module we conducted 5 seminar sessions. The intention of these sessions was to address and discuss aspects of course work and scenarios observed in industry that we may encounter in current or future professional roles. The topics covered were broad, ranging from foundational networking information such as the OSI model vs the TCP/IP stack to more practical discussion surrounding case study security breaches or regulatory violations as well as the results of scanning activities carried out for various deliverables.

These activities, while all distinct, taught us to plan and prepare with an objective to compare and discuss results and findings with classmates. These sessions were instrumental in team building as many of the activities involved some preparation to be carried out as a group. In this way we learned from each other through collaboration, for example learning from one team member, Arun the real-world process in carrying out compliance audits in preparation for Seminar 4, covering global data protection regulations (GDPR), health information privacy (HIPAA) and payment card industry (PCI) compliance. Additionally, I learned from teammate Umar, a network expert currently working for CISCO, a simpler way to look at the OSI model as a framework to apply the TCP/IP stack protocols.

Ultimately, these seminars were an effective way to not only work with peers in my own group, but also to see what conclusions other groups came to when answering the same questions. When conducting your own research on a topic, it is easy to form a bias towards your own conclusions, but these seminars were an effective way of breaking down some of these biases through exposure to other ideas drawn on by individuals with diverse backgrounds, professional and personal experiences. The topics covered also gave more insight into real world examples such as looking at various breaches that have occurred; more importantly looking at both what the victim's reaction was relative to what what we might have done differently under similar circumstances.

Artefacts created in preparation of these seminar sessions.

Unit_7_ePortfolio_Scan_Activity

Seminar_5-Adobe Breach

Discussion Reflection:

This module included three discussion topics to broadly cover three core components of this module. The first discussion centered on the *Medical Mannequin Case* where a group of undergraduate computer science students were able to compromise a medical training device. The second discussion focused on results obtained from scans carried out on our AWS website that was later instrumental in our Design and Executive Summary results and the third topic involved individual review of case studies involving various violations of GDPR compliance.

These topics were broad and incorporated both individual assessment as well as group work to complete. One learning outcome for myself through these exercises was to question the objective and outcome of some material covered. Discussion 1's paper was in my opinion fundamentally flawed, choosing to argue the vulnerability of medical devices by choosing a training device not held to the same regulatory standard as the target. Knowing what I know now on GDPR and HIPAA compliance, a medical training device such as the iStan mannequin would never be beholden to the strict security measures required by something that actually housed patient data. I feel if this paper sought to argue the vulnerability of IoT devices in healthcare, it needs to analyze a relevant device such as a demo insulin pump or bluetooth blood glucose monitor.

The second discussion was less a discussion as it was a report. All groups scanned and reported on the outcome of their scans on their respective AWS sites. One learning outcome from this was to research and as a group decide on what tools not only provided results, but also quality results. It taught us to find the data that fit the problem instead of attempting to use the problem to fit the data; this was especially true when given a limited word count and having to pick only the most relevant results to post and discuss.

The final discussion piece gave us the opportunity to pick and critically evaluate a case where GDPR compliance was violated. My case regarding employee health data without sufficient access control taught me the importance of both role based access control and effective logging policies.

There was limited engagement on these posts and students only reluctantly engaged in responses or even initial posts. I believe part of the reason for this was the considerable amount of work that can go into researching, writing and referencing these pieces with no graded incentive. Our first module incorporated a graded component to the discussions and it caused almost the opposite effect of people over posting to account for contribution marks.

Discussion_1-Summary

Discussion_2-Summary

Discussion_3-Summary

Design and Executive Summary Reflections:

The major difference between our design document and our executive summary was the difference in the types of information gathered throughout. Our design document focused heavily on information gathering and reconnaissance with an emphasis on tools such as *whois, dig, NMap*, etc. Many of these tools may have ended up being used in our final analysis during the executive summary, but were left out as the information they garnered wasn't sufficiently useful to be reported or was incorporated into a more thorough vulnerability scan. An example would be using SSLScan to check the presence of transport layer security (TLS) or secure socket layer (SSL) encryption on traffic. This tool failed to find anything making an inelegant conclusion that SSL was not present. In the executive summary we scrapped this in favor of the results of more comprehensive scans by Nessus, which found and rated the lack of any traffic encryption to be the highest severity vulnerability.

Another difference between these two documents was the "what" of what was found vs the "why" where the design document tended to emphasize a plan of finding "what" information might be available, with less emphasis on the relevance of what the information might be useful for in future exploits. This is excusable by the length and scope limitations of this document, while the executive summary had more room for explanation and implication. This is where the executive summary was able to tie in the relationship between the scan results and a more detailed account of industry regulation and best practice. Ultimately, this showed growth in understanding and execution throughout the module, where we were able to better put together a more polished, professional analysis of a website, using more comprehensive and advanced scans to check for vulnerabilities.

Design_Document

Executive_Summary