| **Reflection - Formative and e-Portfolio Activities** | | | |
| --- | --- | --- | --- |
| **Component** | **What?** | **So What?** | **What Next?** |
| Collaborative discussion 1 (Units 1 – 3) | Based on the paper "Compromising a Medical Mannequin", students were asked to identify the significant threats and vulnerabilities discussed in the paper and necessary mitigation strategies.  Also, students were tasked with a group activity to prepare and present a summary using the DREAD tool. | The students' assessments primarily focused on critical vulnerabilities discussed in the paper - brute force attack and denial of service attack.  Even though some common themes related to remediation solutions were noted, like complex password policy for brute force attack, a range of solutions were discussed. Some of them were technical, and some of them were non-technical, like security awareness training.  The remediation activities ranged from using a firewall for Denial Of Service (DoS) attacks to security awareness training for social engineering attacks.  See Summary Post related to Collaborative Learning Discussion 1 below in Artefacts section.  The group activity helped to understand the real-world requirement to use the assessment tool – DREAD. In addition, the project management skills were also utilised to complete the task for the seminar. | Various remediation solutions and tools discussed during this collaborative learning can be learned profoundly and applied to numerous situations.  Tools like DREAD and STRIDE can be applied in the future to perform an assessment.  Last but not least, the project management technics can be applied going forward for future assessment. |
| Practical and Team activity (Unit 3) | This Practical and Team activity was primarily based on standard scanning tools such as ping, traceroute, dig and nslookup.  Students were requested to perform a basic scan using the website of the opposite team and respond to several questions related to the scans. | Initially, as the opposite team's site was not available, I was disappointed.  Then we became creative and used an alternate site for scanning.  We were able to pivot according to the situation and learned to be resilient.  I enjoyed using the tools in a controlled environment (non-production) without the fear of any negative impact on the environment. | The "emergency management" skills learned from the situation can be applied to disaster recovery conditions.    In addition, the usage of the standard scanning tools could be applied to understand the IT environment, and I would use this knowledge to collect basic information about the systems. |
| Collaborative discussion 2 (Units 4 – 6) | This Collaborative discussion 2 was focused on the results of scans.    Students were instructed to collect and correlate the information from various sources to support a comprehensive analysis. | We used several tools such as Pathping and Nmap to collect information and identify any vulnerability within the environment.  I felt empowered to investigate and identify potential tools for scanning.  As I worked with very passionate students, I was inspired to learn and test the tools. | I would use the tools and techniques learned from this activity to identify information about an IT environment, including vulnerabilities.  In addition, I would add these tools to my "tool kit" and learn more about each of them, including various combinations and switches that can use with these tools. |
| e-Portfolio activity (Unit 7) | The objective of the e-Portfolio Activity was to evaluate Kali Linux in various aspects, including its functionality and limitations based on articles and statements.    Among other things, students also requested to compare the Kali Linux with Nessus. | Based on the article "A Comparison Study of Open Source Penetration Testing Tools", assessing different tools side by side with Kali Linux for numerous attributes enabled us to learn and understand each of them better. I had a sense of accomplishment after this activity.  Close to the end, I found it challenging to pick the "winning tool". However, based on active discussions and reviews, we have concluded that each tool was different and instrumental for unique needs. | Learning from this activity can be used to apply the tools effectively during real-world scenarios.  Also, learning about the negative impact of the scanning tools within an IT environment should be considered during implementation. |
| Scanning exercise and Wiki (Unit 7) | This Scanning Exercise and Collaborative Learning Wiki were focused on the scans against the assigned website using the tools available in Kali Linux.  Based on the scan results, students were requested to respond to the questions related to the website details, such as what operating system is used, etc. | Based on the referenced material, identifying appropriate tools to scan the website was an exciting activity.  Interpreting the scan results to answer the questions was even a rewarding exercise. | Understand of the various tools available within Kali Linux would be applied to use those tools effectively.  In addition, knowledge gained from this activity can be enhanced by doing additional research. |
| Collaborative discussion 3 (Units 8 -10) | The Collaborative discussion 3was based on the case studies concerning GDPR related issues and breaches.  Students were requested to review a case study and discuss the case to answer various questions, including questions related to GDPR aspects. | The case study I have selected was an incident related to personal information discloser. As this is not about a technical issue, I was disappointed initially. However, as I learned about the GDPR implications based on innocent human error, I appreciated the case study.  As my case study was related to health records, I tried to connect to the current COVID situation, which the other students appreciated. | The learnings from this activity can be listed as below:   * Employee training within the organisation; * Policies and procedures aligned with regulatory requirements.   I would apply these learnings to the future to ensure compliance with the regulatory requirements. |

| **Reflection - Seminars** | | | |
| --- | --- | --- | --- |
| **Session Title** | **What?** | **So What?** | **What Next?** |
| Introductory session and group allocation for Team Project (Unit 1) | This seminar was the introduction seminar and was used to introduce the module.  Students were requested to work on the group contract. | I felt that the group contract enabled us to connect effectively and completed the tasks and activities efficiently. | The contract concept can be utilised in any project in the future. Therefore, I would use the modified version for my future projects. |
| STRIDE and DREAD tools (Unit 2) | This seminar was based on a paper about Threat Modelling, specifically Microsoft STRIDE & DREAD tools.  Students were requested to apply a 3 level DREAD rating to the "Compromising a Medical Mannequin" case. | Threat Modelling is a critical process to identify the security threats within a network environment, and therefore I was interested to learn about this.  I found it challenging to apply three levels of DREAD due to the limited options.  However, by discussing with the group, I overcame the challenge. | Threat modelling technics can be applied to any risk assessment requirements.  I would probably use more levels than 3 levels to identify the risk levels precisely. |
| TCP/IP v ISO/OSI (Unit 4) | The seminar's objective is to empower the students to think hypothetically about the Internet – would the Internet be any better if it was based on IOS/OSI 7 -layer instead of TCP/IP.  Additional factors include availability, influence and impact of server and desktop tools and environments and origin also requested to consider. | As both of them are very familiar to me, specifically IOS/OSI 7 -layer from the academic background and TCP/IP from various implementations, I was very excited to work on this exercise.  This exercise provided autonomy to the students to design their "own" Internet using ISO/OSI 7 -layer. We learned more about TCP/IP and IOS/OSI 7 -layer and application. | I learned the relationship between IOS/OSI 7 -layer and TCP/IP effectively. I will use this knowledge to design and implement effective network solutions. |
| Evaluation exercise (Unit 6) | The penetration testing tools discussed in a blog from Network World were the basis for this seminar.  Students were requested to evaluate the eight tools - Metasploit, Nessus, Burp Suite, Nmap, OWASP Zap, SQLMap, Kali, Jawfish against the established criteria such as flexibility, reputation, etc. | Using the security assessment tools effectively is critical to complete the penetration test successfully. Therefore I was motivated to learn and understand each of them.  Initially, I found it challenging to evaluate against numerous criteria. However, as I learned about the tools and their attributes, I was motivated to learn more to complete the evaluation accurately. | I learned various attributes about the penetration testing tools. As each of them is better for different assessment needs, I would "mix and match the" tools according to the penetration testing objectives and requirements. |
| Security Standards (Unit 8) | This seminar was based on Security Standards, Guide to the General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS) and Health Insurance Portability and Accountability Act (HIPAA).  Students were requested to identify the applicable standards to the website, evaluate the website and provide recommendations to comply with the standards. | Organisations must comply with applicable Security Standards to avoid regulatory penalties, legal and reputational issues. Therefore, the entities are recommended to integrate the relevant standards within their policies, standards and procedures.  In the beginning, the materials covered within the Standards made me feel overwhelmed. However, I reviewed and learned various materials related to the Security Standards our group selected for review. Finally, I was able to contribute to the seminar deliverable significantly, associated explicitly with PCI DSS. | Knowledge gathered from this activity can be applied to regulatory are compliance-related projects in the future.  The key takeaways from this activity were the following:  Compliance is everybody is the responsibility; and  Elements from people, processes and technology should be considered for compliance. |
| Data Breach case study (Unit 10) | This seminar was developed on various case studies conducted on security data breaches. Students were requested to select a case study and discuss the various aspects of the breach, such as what happened, types of affected data, etc. | As these case studies focused on significant incidents within large organisations and had substantial media coverage, I was highly motivated and interested in learning about the details related to the case study selected - the Equifax data breach. We did this activity as an individual engagement.  Even though the requirement was to perform an assessment related to a case study, I was inspired to learn from other case studies, which helped deliver a more comprehensive presentation for the seminar. | These case studies and root cause analysis helped me understand the importance of the processes and security awareness training, and technological limitations.  I would use these concepts to develop security programs and remediate gaps identified within the organisation's IT environment. |
| Debate Vote (Unit 12) | This seminar was developed based on future Internet technologies.  Students were requested to present their views about four leading technologies. | As these technologies were related to the future of the Internet, I was inspired to research these technologies.  Due to the limitation of the information, I felt that the activity was limited in some aspects. However, the technology assigned to our group, content-centric networking, was very relatable to our day-to-day activity streaming movies and videos. Therefore we were motivated to research and analysis about the topic. | I would use my learning to develop my knowledge about the technologies which can be used to improve the Internet.  In addition, where possible, I would involve and contribute to the development of the future Internet. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Reflection - Assignments** | | | |
| **Summative Component** | **What?** | **So What?** | **What Next?** |
| Development Team Project: Design Document (Unit 6) | These projects were developed based on a design document and executive summary.  Students were requested to develop a design document for the website. And finally, based on the design details, students were asked to create an executive summary. | These two engagements were the highlight of the module and enabled us to learn several security tools.    As these activities were similar to real-world situations, students were motivated to learn and research more than required. | I would apply the skills and experiences learned from these exercises. |
| Development Team Project - Executive Summary (Unit 11) |
| Individual Module e-Portfolio (Unit 12) | This was an e-Portfolio module, and students are required to reflect on the module. | Initially, this exercise seemed like a duplication of work. However, as I start to work on this, I was inspired, as I collected all the learning in a consolidated manner.  This also enabled me to think about each activity and related learning.  In addition, during this process, I also identified future applications and real-world examples. | I would apply the learning in the future and build my e-Portfolio. This will be an effective representation of my learning and development. |