NISM Module Overview & Reflections

Introduction

This programme module covers Network and Information Security Management at the University of Essex Online, and it lasts 12 weeks. As I progress through the units, I document all the achievements, invaluable insights, and unit summaries in the e-portfolio address below.

e-portfolio Address

https://gurkanhuray.github.io/home/

Module Reflections

As recommended in the University's e-portfolio guidelines, this document uses Rolfe et al.'s (2001) reflective model and consists of three sections called What? So what? Now what?.

What?

Our team was tasked to prepare a design proposal document, including assigning one of the business functions such as industry recruitment, e-health or e-commerce site to a made-up organisation called Pink e-health services' website. Afterwards, conducting a vulnerability scanning to produce a professional-grade executive report, including identified vulnerabilities, potential threats, suggested improvement measures to address risks, and further considerations based on GDPR and PCI-DSS requirements was the next and final part of the assignment. However, it was not an easy task, especially for those lacking hands-on experience in the field, and required noticeable prep-work to determine activities within the scope of the work appropriately.

So what?

The first steps were challenging; we thoroughly researched all available methods and academic references to establish fundamentals. (Goel & Mehtre, 2015) explains the entire lifecycle of the process in a well-structured way and describe the differences between automated and manual scanning. In addition, (Upadhyay & Prajapati, 2019) also explains how active and passive information gathering (AIG/PIG), including high-level evaluation of tools that could be utilised. In a way, that supported the idea I had in my mind and noticeably contributed to producing a professional-grade executive summary report and overcoming challenges that were persisting during the first steps. Therefore, the proposal of starting with active and passive information gathering was well received within the team and paved the road to success. However, after submitting the design proposal document (first part of the report), a weak connection between STRIDE-based threat classification and DREAD-based risk scoring was noticed. It is further confirmed with the latest constructive feedback received from the tutor. Therefore, the next challenging step was the incorporation of STRIDE and DREAD techniques in a proper manner, and I was personally involved in structuring a risk rating matrix, risk assessment and scoring method, prioritised risk classification scheme and limitations around the DREAD-based risk scoring approach. These contributions are well received within

the team and supported in addressing the constructive feedback received during the first part of the assignment.

Now what?

Ultimately, our team managed to overcome the aforementioned challenges and get a positive outcome. Some tasks had to be repeated due to miscommunication and language barriers. Still, the team preserved its integrity and continued to make a progress and succeeded in reaching the desired results. Working in a team promoted creativity. Additionally, it has maximised the shared knowledge within the team. There could have stale viewpoints if we were working as individuals; thus, the teamwork helped us avoid that potential concern.

References:

Goel, J.N. and Mehtre, B.M., 2015. Vulnerability assessment & penetration testing as a cyber defence technology. *Procedia Computer Science*, *57*, pp.710-715.

Upadhyay, D. and Prajapati, D.K.V., CYBER DEFENCE: A HYBRID APPROACH FOR INFORMATION GATHERING AND VULNERABILITY ASSESSMENT OF WEB APPLICATION.