e-Portfolio https://kalaitzakisant.github.io/ePortfolio/nism.html

Network and Information Security Management – Reflection

So, you like networks! Now what?

During the Network and Information Security Management module, we were introduced to the security concepts of computer networks and information security management, to the usage of various monitoring, testing, and logging tools and we learnt how to use vulnerability and assessment scanning tools against websites and web applications.

Throughout the first week in the NISM module, we were divided into groups as we would complete our assignments in teams. Additionally, we got access to Amazon Web Services (AWS) to set up our personal server and perform tests against it.

In Unit 1 I started reading about the basic principles of network and information security management and posted my **collaborative discussion** 1 regarding the security of medical mannequins. I found the penetration paper to be one of the most interesting papers I have ever read. I am not very familiar with medical mannequins, and I did not know they can be wirelessly connected to a computer.

In Unit 2 I collaborated with my team for the first time to prepare a **presentation** in STRIDE & DREAD tools. It was really nice to collaborate with people coming from different countries as I really value diversity.

In Unit 3 I performed my first **network tests** with basic commands such as ping, traceroute, nslookup, etc. While I had heard and read about these tools before, I had only used ping to check whether a server is responding. I found traceroute to be the most exciting one as it maps the route between your router until the destination.

In Unit 4 I prepared my second **collaborative discussion** where I collected and presented my network scan findings from the previous unit, and I read about the “fight” between ISO/OSI and TCP/IP.

In Unit 5 I studied the required reading for the network components and tools. As a long-time enthusiast of networks, I was already knowledgeable of them. However, during Unit 5 until Unit 6 I was collaborating with my team to complete our first assignment.

In Unit 6, I continued working with my team to complete our **design document.** In our System Proposal assignment, I prepared the introduction, the appendix graphs and I made a list with some network tools we can use. Additionally, after I received all documents from the rest team members, I worked on the final structure of the assignment, I corrected the typographic and grammatical errors, polished the final assignment, and submitted it to the portal.

Furthermore, I researched eight penetration tools and evaluated them in six criteria: ease of install, ease of use, flexibility, licensing, privacy, and reputation as part of the **third seminar**.

In Unit 7 I read about Kali Linux and its uses and prepared an e-Portfolio **component**. I had never heard about it before, however, once I read how it succeeded Backtrack 5, I understood some of its functionalities. I remember being amazed by Backtrack 5 when I was young and reading about it again was nostalgic.

In Unit 8 I was introduced to various applicable regulations including GDPR, HIPPA, PCI-DSS, and more. I read and prepared a **case study** regarding an unlawful CCTV personal data processing. While regulations can be disruptive for novel technologies, they can assure the safety of our data. However, all regulations need to be updated regularly to allow technology to evolve.

In Unit 9 I read about system logging and its analysis tools. Additionally, I was collaborating with my team to prepare our Executive Summary document. In general, Unit 9 allowed me to reconcile everything I learnt in the previous units and move on a little more prepared.

In Unit 10 I studied some immense data breaches. Furthermore, I selected a data breach that occurred in 2011 from SONY PlayStation Network and prepared a **study case** as I remember how devastating it was for SONY. Additionally, I was still collaborating with my team for our Executive Summary document.

In Unit 11 my team and I worked tirelessly to prepare our **final submission** well on time to review it. In our Executive Report, I prepared all EU GDPR and PCI-DSS sections (issues and recommendations), I worked with the conclusion section where I presented a summary of the data in our report and finally, I reviewed and corrected all typographic and grammatical errors, and I polished the assignment before we submitted it.

Furthermore, we worked on our assigned **debate presentation** regarding IPv4 and IPv6.

In Unit 12, I was working to get my e-portfolio ready for its final submission, but unfortunately, I miscalculated the effort and time required and got stressed to complete it on time.

I am completing the NISM module with knowledge in several scanning and penetration tools, Amazon Web Services, the PCI-DSS and HIPPA regulations, internet protocols and their history, Kali Linux, System logging and more.

However, I still have many things to learn, but I am eager to do so! Specifically, I will install Kali Linux on a virtual machine and start reading manuals, articles, and guides to become further acquainted. Additionally, I will attend some AWS courses and training to further work with it and explore all its services, mostly in collaboration with novel technologies such as Big Data and IoT.

Having reached the end of the Network and Information Security Management module, I could not stop thinking how interesting it was! I do believe that computer networks are one of the most important breakthroughs humans have done, and the future has yet to come.

Finally, I cannot help myself but feel proud for my team and myself for completing our assignments successfully with a great approach.