https://qtr9.github.io/E-portfolio/NetworkSEC.html

Final Reflection of the NISM Module 1000 words:

After studying the NISM (Network Information and Security Management) module, my understanding of networking, monitoring and logging tools, information security principles, and vulnerability and scanning tools has increased. At the beginning of the project, students were divided into three groups for various collaborative lectures and vulnerability identification tasks. I am a member of group 03, where it consists of 5 students totally.

Collaborative sessions enable me to comprehend and comprehend my colleague s' viewpoints. In the conversation everyone brought forward different ideas and opinions I enjoy how it helps me develop my skills and makes it simple for me to comprehend the distinction between risk and vulnerability. Moreover, OSI layers, TCP IP, DREAD and STRIDE model that where utilized in many unit's exercises.

Campbell (2016) defines danger as "a weakness in an investment or management that may be attacked by one or more threats", A vulnerability, on the other hand is “a flaw in an asset or management that might be exploited on or more attackers. My understanding of the security issues facing medical devices has also evolved, given that I have had little knowledge of technological improvements in the industry in the past. I learned how to do the DREAD analysis properly, which is a new concept. As you can see from the joint effort, I need to do a lot of research on this topic to fill in the gaps in my knowledge.

Regulations like the General Data Protection Regulation (GDPR), information Commissioners office (ICD), payment Card Industry Data Security Standard (PCI-DSS) should been thought about carefully. It necessitated my reading and comprehending a number of study papers. (I.T Governance Ltd, 2021) focusing on hazards and vulnerabilities associated with e-commerce platforms. Obtaining data for the project is not as simple as some may believe it proved to be a challenging issue for me.

In this learning mode, the scanning activities introduce me to the many scanning instruments that businesses utilize. In terms of collective effort, each member participates in team dialogue. These findings are analyzed and then adjusted in group discussions. I'm happy with this conclusion because it confirms and validates my understanding of the issue, as it does for the rest of the group (*Examples of Classroom Assessment Techniques*, 2016).

The project asked the team to utilize various scanning techniques to find vulnerabilities and make recommendations and mitigations to protect problematic websites. As a cybersecurity expert, one method to protect *E-commerce* (*electronic commerce*) sites and servers is conducting frequent scans and penetration tests using various scanning tools along with a regular patching framework. Scanning tools aim to obtain additional information about a host or target (I.T. Governance Ltd, 2021).

These organizations have given people a great deal of experience in locating and assessing system weaknesses and providing helpful advice. Additionally, these responsibilities have allowed me to do a more in-depth study of regulators and related regulations (GDRP, ICO, and PCI-DSS) and become proficient in penetration testing exercises with Kali Linux.

The primary purpose of this module is the basic knowledge of computer systems and security. Understand the principles of information security risk management. Learn about the different monitoring and logging tools, their uses and benefits. Learn how to build and use system vulnerability, assessment tools, and applicable programming methods. The ability to understand future network designs and information assets. Ability to critique and analyze own personal growth. The ability to present essential arguments to different audiences about specific actions or outcomes.

After completing this module, I will be able to: Identify and assess security threats and hazards in I.T. network systems and select appropriate methods, tools, and strategies to manage and address these issues. Create solutions that help control and monitor risk and security problems through the design and critical evaluation of computer programs and systems. To help systematically examine security vulnerabilities and issues, gather and synthesize information from numerous resources, including online security warnings and warning sites. Describe the legal, social, ethical and professional challenges facing information security professionals.

From my point of view, this course introduced me to the fundamental concepts of computer networking and the skills required to manage information security. This module provides an overview of cybersecurity foundations and concepts for information security governance. Its foundation would be mapping information security management activity to multiple security models. In this learning mode, I examine the security management and protection issues, such as company resources, risk, monitoring, and business continuity strategies. This module also covered Nessus, sniff, Syslog, ELK, and typical network and information security patient monitoring tools. These topics are given to me pleasantly and dynamically, using group and individual tasks.

After completing all modules, I can get some things done in my work Since I work in information security. I can tackle all the issues related to the vulnerability. I have a great passion for the (GIS) Group information security field, so I have selected this course. In the present era, every organization wants to protect critical information from attackers, and for that purpose, these organizations adopted cybersecurity-related techniques. In this module, I have learned many things related to network security, network management, the network controlling, etc. I have also collected excellent knowledge and working experience as a team member in the group project.

I chose the information security field as my career, and there are many career-oriented opportunities where we can serve the organization. This learning models was well organized, and it provided knowledge from essential to advanced levels. Overall, I just received a fantastic work in a company related to information security, which has been beneficial to me a lot with my study in the university at the same time.

References:

Campbell, T. (2016) Practical Information Management System. 1st ed. APRESS Examples of Classroom Assessment Techniques. (2016, June 22). MGH Institute of Health Professions. https://www.mghihp.edu/faculty-staff-faculty-compass-teaching-teaching-strategies/examples-classroom-assessment-techniques [Accessed 28 May 2022].

I.T Governance Ltd (2021) Vulnerability scanning: what it is and how it works. Available from: https://www.itgovernance.co.uk/vulnerability-scanning [Accessed 28 May 2022].

Miqdadi, F.Z., Almomani, A.F., Masharqa, S., & Elmousel, N.M. (2014) 'The Relationship between Time Management and the Academic Performance of Students from the Petroleum Institute in Abu Dhabi, the UAE', ASEE 2014 Zone I Conference. University of Bridgeport, Bridgeport, CT, USA, 3-5 April. 1-5.