**AIMALOHI ODIA**

**NETWORK SECURITY REFLECTIVE ESSAY**

**INTRODUCTION**

The network and information security Management module is aimed at educating one with current and emerging technologies in networks and information security. The knowledge and skills gained will aid in the design, development of a secure and trusted system. In addition, the course also gives an understanding of the fundamentals of computer networks, network protocols, network tools (such as ping, traceroute), penetration testing methodologies (OWASP), risk assessment and mitigation techniques (STRIDE). Furthermore, there were exploration of advanced and future security technologies such as security incident and event management (SIEM) and adaptive machine learning cyber security systems. This reflection explores some lessons learnt during the module and shows how these should be put into practice.

**NETWORK THREATS, VULNERABILITIES AND MITIGATION TECHNIQUES**

According to Modiri (1991), security involves the use of various security mechanisms like authentication and access control and encryption to create security solutions. This way, security principles such as Confidentiality, Integrity and Availability are more likely to be achieved.

The first collaborative discussion explored is (link above) on the compromise of a medical mannequin gave insight to potential vulnerabilities and threats devices connected to the internet are faced with. Moving forward, it is essential that one keeps in mind potential security vulnerabilities at work and in our personal lives. There are numerous mitigation techniques, each with its flaws. This course introduces several mitigation techniques, each with its own flaws and weaknesses. It is therefore essential that when it comes to cyber security, a combination of security solutions is more likely to form a good barricade against potential threats that a single solution. In addition, in the case study which is about hospital implies that hospital devices are now fully automated and computerised equipped with sensors susceptible to attacks.

**NETWORK SECURITY TOOLS AND TESTING**

Security Solutions can be technical or non-technical. Technical solutions involve: penetration testing, configuration management etc Security solutions must be improved and updated as often as possible to keep up with the constantly emerging threats.

Alotaibi et al (2017) opines that threats that target several layers concurrently by disguising malicious payloads brought about next generation firewalls. These aim to combine deep packet inspection with features present in intrusion prevention systems. Next generation firewalls will have features such as: encrypted traffic control, the ability to decrypt and inspect Secure Socket Layer/ Transport Layer Security (SSL/TLS) traffic to eliminate blind spots threats for better cyber protection etc.

In addition to technical solutions such as configuration management, encryption using HTTPS or SHTTP for client-server communication and penetration testing tools such as: kali Linux, Metasploit, Wireshark, Burb Suite, etc. Denis, et al (2016) suggests that it is important that more people become aware that we are not secure just having an antivirus anymore. As explored in the module, penetration testing tools have been getting a lot of attention and there are a lot of Open source tools than can be modified to suit individual needs depending on the vulnerability assessment needed to be performed. It is important to note that security solutions depend a lot on user needs, as tools are not perfect and security solutions are constantly evolving. However, humans are usually the weakest links, for example, an employee compromised by social engineering attacks or an IT personnel that has wrongly configured the firewall deployed. Thus, having multiple layers of network defence is essential, however, continuous training and enforcement of security policies is needed to attain an optimal level of security.

**SECURITY STANDARDS AND RISK ASSESSMENT**

According to Knuf Haufe et al (2016)**,** there is no all-encompassing method to determine the maturity level of Information Security Management processes. Some security standards widely used include: General Data Protection Regulation (GDPR), Payment Card Industry Data [Security](https://datafloq.com/read/?q=Security#utm=internal) Standard (PCI DSS) etc. there are key criteria applicable to nearly all organisations, these include: size, objectives, location etc. however, transnational data creates security issues in other jurisdictions which is daunting for security professionals.

Susanto et al (2011) suggests that parametersfor the fulfilment of information security according to 11EC include: information security policy, communications and operations management, access control, Information System Acquisition, Development and Maintenance, Organization of Information Security, Asset Management, Information Security Incident Management, Business Continuity Management, Human Resources Security, Physical and Environmental Security, compliance. This module has shown that, solely relying on technical methods for cyber protection at the workplace isn’t an effective strategy this both in the workplace and in our personal lives.

Security implementation methods should combine technical and non-technical solutions and must leave room for change and adaptability to meet the needs of a constantly evolving society.

**REFERENCES**

Modiri, N (1991) The ISO Reference Model Entities’ Available at: [https://doi.org/10.1109/65.93182.[Accessed](https://doi.org/10.1109/65.93182.%5bAccessed) 23rd July 2021]

Alotaibi, A. M. *et al.* (2017) Security issues in Protocols of TCP/IP Model at Layers Level. Available at: https://www.semanticscholar.org/paper/Security-issues-in-Protocols-of-TCP%2FIP-Model-at-Alotaibi-Alrashidi/b3015c94305f1815234843ad3c7bd5523edc8b0d [Accessed: 25 July 2021]

Pratishtha Saxena, et al (2018) ‘Network Security Attacks and Defence’. *Journal of Computer and Information Technology* 9, no. 5 . : Available at <https://doi.org/10.22147/jucit/090501>. [Accessed 23rd July 2021]

Denis, M et al ‘Penetration Testing: Concepts, Attack Methods, and Defense Strategies’. In *2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, 1–6. Farmingdale, NY, USA: IEEE, 2016. Available at: <https://doi.org/10.1109/LISAT.2016.7494156> . [Accessed 23rd July 2021]

Haufe, et al (2016) Security Management Standards: A Mapping’. *Procedia Computer Science* 100 (2016): 755–61. Available at <https://doi.org/10.1016/j.procs.2016.09.221>. [Accessed 19th July 2021]

Susanto, et al ‘Information Security Management System Standards: A Comparative Study of the Big Five’ 11, no. 05.