Network Security June 2022 B

Unit – 6

Individual Reflective Piece

by

Gokul Kurunthasalam

Table of Contents

Introduction:

I have listed down my understanding unit-wise in this assignment. I have categorized my observations and summarized them as follows:

Unit 1: History of Network Security, Vulnerabilities and Approaches

Knowledge and Understanding:

This Unit provided a concise explanation of the significance of CIA, Vulnerability Management, and Incidents. The history of network security and vulnerabilities has been discussed extensively. In addition, covered several security best practices and the Cyber Kill Chain model provided by Lockheed Martin (Hutchins et al, 2011).

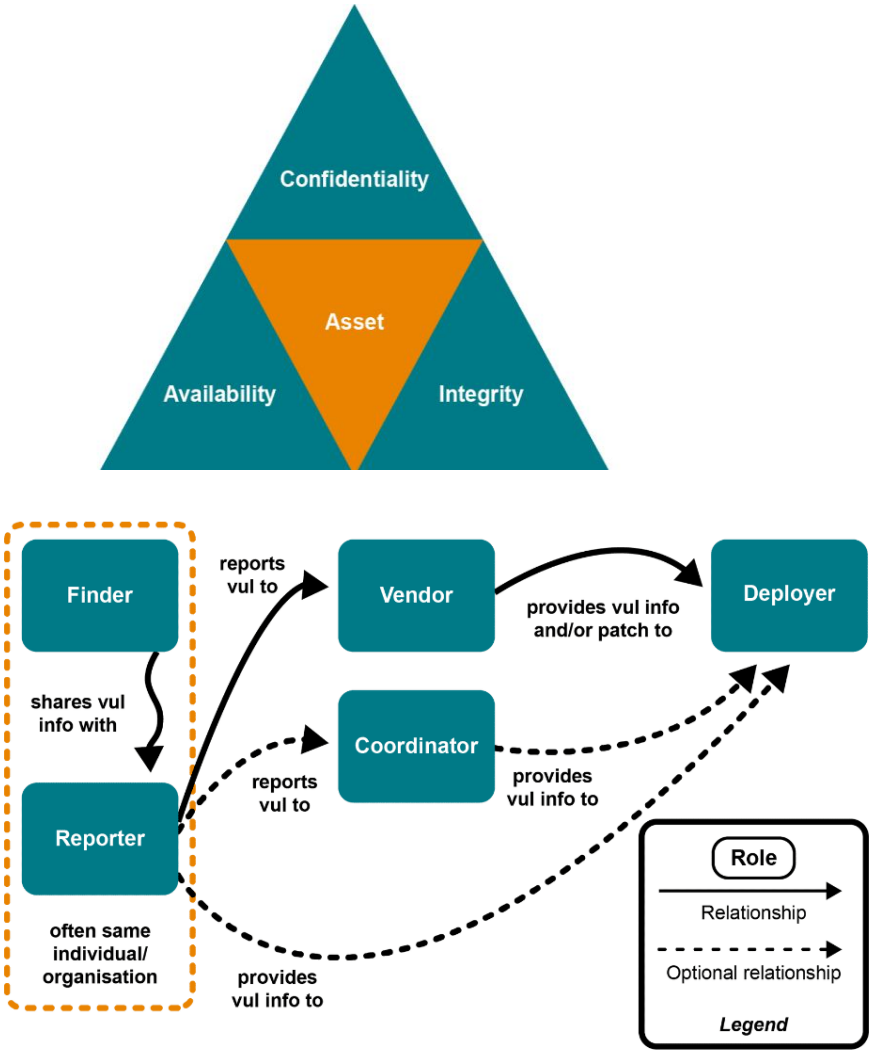

Fig 2: Diagram from Moore & Householder 2019

Activities and Evidence:

- Websites choose an activity - the following website has been selected: https://tigertek.org.uk
- Collaborative Discussion 1: Digitalization – What are the security implications of the digital economy? Banerji (2019) and Spremic and Simunic (2018)
- The initial post for the questions in the Unit-1 discussion forum has been made.

Learnings:

- The Cyber Kill Chain model developed by Lockheed Martin, which is crucial for the current security issues, is explained in this unit.
- The capacity to recognize and analyze security threats and vulnerabilities in network systems and to choose the best methodology, tools, and techniques to address them.

Unit 2: Advanced Persistent Threats: Applying the Cyber Kill Chain Model to a Case Study

Knowledge and Understanding:

This unit explained penetration testing, including black box and white box testing, as well as the history of the idea of the advanced persistent threat (APT). To determine whether the well-known Cyber Kill Chain model is still applicable, research and study on the solar winds exploit (Temple-Raston, 2021) have been conducted.

Activities and Evidence:

- Attended seminar on "The Solar Winds Breach Case Study"

- Continued group discussion-1 and performed Vulnerability Analysis – Literature Review Activity
- Peer review for discussion forum postings by Beatrice Mutegi and Amit Pahuja was complete.

Learnings:

- Network system security threats and vulnerabilities have been identified and studied. Appropriate management and/or resolution procedures, tools, and strategies have been determined.
- The SolarWinds security incident case investigation was understood.

Unit 3: Vulnerability Assessments

Knowledge and Understanding:

This lesson covered a variety of methods for performing vulnerability assessments, including Cyber Essentials, scanning policies, identifying necessary scans, and selecting appropriate tools. Vulnerability assessments can be represented as a continuum from mostly paper-based, internal reviews (as exemplified by the cyber essentials process (NCSC, 2021)) to a blueprint for a full attack (as discussed as part of the cyber kill chain (Hutchins et al, 2011)).

Activities and Evidence:

- Submitted an assignment on the basic analysis and scan of https://tigertek.org.uk, along with the results.
- Prepared the responses to the questions from the ***"Scanning Activity"*** for the next seminar.

Learnings:

Recognized how to use the most basic tools on hand to scan websites.

Unit 4: Breach Analysis and Mitigation

Knowledge and Understanding:

The legal ramifications of security breaches are covered by Schwartz and Janger (2007). The articles listed below go over how to use Kali Linux (and its related tools) and offer some suggestions for doing so.

Activities and Evidence:

- Completed initial post in Collaborative Discussion 2: The Pros and cons of logging – The impact of log4j
- Scanning and Collaborative Wiki Activity using ***Kali Linux tools - OpenVAS, Nmap and Burp Site***
- Installed Kali Linux on a virtual machine workstation, and you can find the results of a scan using those tools below.

Learnings:

Understanding of and proficiency with "Kali Linux and tools" for website scanning.

Unit 5: Logging, Forensics and Future Trends

Knowledge and Understanding:

The topics of digital forensics, log analysis, forensic tools, secure protocols, and virtual networking are covered in this lecture.

Activities and Evidence:

- Continuing Collaborative Discussion 2: The Pros and cons of logging – The impact of log4j

- Case Study: Reviewing an Assessment Reporting Template

Learnings:

Deep understanding of tools and analysis for penetration testing

Unit 6: The Great Debate: The Future of the Internet

Knowledge and Understanding:

A number of potential approaches are discussed in the themes related to technological advancements in an effort to establish a next-generation internet that addresses the faults of the current internet. Reading the IEEE papers on Software Defined Networking Architecture by Rawat, D., and Reddy, S. (2017).

Activities and Evidence:

- Seminar on "The Debate - The Future of the Internet"
- Completed assignment on Vulnerability Audit and Assessment - Results and Executive Summary
- Individual Reflective piece

Learnings:

Understanding the potential answers put out to address some of the technological, security, societal, legal, and privacy issues brought on by modern internet technologies

Conclusion:

I'm pleased to have learned a lot about a solid foundation in network security. I have done my best to comprehend the topics by engaging in all the activities suggested in the module, starting with fundamental ideas and moving on to security incidents,

secure application design, website scanning, vulnerability tools management, and security products. After completing this module, I have a thorough understanding of network security. I should also remark that all seminar sessions were outstanding and helped me delve even further into the ideas of networks.

References:

Spremić, M. & Šimunic, A. (2018). Cyber Security Challenges in Digital Economy. Proceedings of the World Congress on Engineering 2018 (1).

Hutchins, E. et al (2011) Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.

J. Straub, "*Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT&CK and STRIDE Frameworks as Blackboard Architecture Networks*," 2020 IEEE International Conference on Smart Cloud (SmartCloud), 2020, pp. 148-153, doi: 10.1109/SmartCloud49737.2020.00035.

NCSC (2022) Penetration Testing - *Advice on how to get the most from penetration testing.*

Schwartz, P. & Janger, E. (2007) Notification of Data Security Breaches. Michigan Law Review.

SolarWinds Windows Logging Basics - The Ultimate Guide To Logging.

https://www.kali.org/ [Accessed during Unit 5 and 6 weeks]

Hertzog, R. et al (2017) Kali Linux Revealed (KLR/PEN-103) - Mastering the Penetest Distribution.

Rawat, D. & Reddy, S. (2017) *Software Defined Networking Architecture, Security and Energy Efficiency:* A Survey. IEEE Communications Surveys and Tutorials 19(1): 325-346.