Introduction to Network Security Module

Module Learning Outcomes: (Please include explicit references to the submitted Grant Learning Outcomes – Appendix 3)

#1: Demonstrate substantial understanding of the cybersecurity first principles.
#3: Explain different types of attacks on computing systems.
#4: Experiment with different tools and techniques used to attack and/or defend systems.
#13: Remember the important role humans play in the digital world and understand how to minimize accidental and intentional human errors.

The Module addresses the following First Principles: (Please include explicit references to the First Principles - Appendix 1)

#1: Domain Separation
#4: Least Privilege
#5: Layering
#7: Information Hiding
#10: Minimization

Description:

This module will start by a brief review to the fundamental working principles of computer networks that were covered in the Networks/Smart Data module. Then, the participants will be introduced to various types of attackers and their varying motivation. The module will also discusses numerous malicious attacks including password guessing, man-in-the-middle, replay, session hijacking, and Denial of Service (DoS). In addition, various effective countermeasures will be expounded in details including the use of firewalls and intrusion prevention systems while relating such use to some the first principles such as layering and least privileges. Besides, the basic idea of encryption will be introduced