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 starts by a brief overview of the fundamental working principles of computer networks then introduces various types of attacks (malicious software, password guessing, man-in-the-middle, replay, session hijacking, and Denial of Service (DoS)), effective countermeasures (firewalls and intrusion prevention systems, encryption and the role it plays in securing information while in transit or in storage), attackers and their varying motivations. . Application of several cybersecurity First Principles will be incorporated, e.g., layering in design of secure network environments and least privilege to help minimize the possibilities of attacking various network components. While discussing attackers and their motivations, ethical concepts will be discussed to include the controversies associated with hacktivism.

Learner-centered classroom:

This module is designed to be taught in a highly interactive environment in which all attendees will be active participants in the learning process. To achieve that, one approach is to use a series of lab-based activities to enable students to "do it yourself" in order to enhance their comprehension of taught contents. Such lab activities include network reconnaissance, password cracking tools, and traffic analysis. In addition, we are using a number of simulating activities that highly promote participants' engagement and make them positive contributors to the learning process. Another approach is to use mobile technology to maximize participant involvement through the use of their own smart phones (BYOD) and/or the provided mobile devices. Services such as, Kahoot, tophat and Poll Everywhere will be used to achieve this.

Assessment:

This component of the module is designed to use a variety of formative assessment strategies in order to ensure that the students has acceptably achieved the Intended Learning Outcomes (ILOs) of the module. Examples of the proposed techniques are use of discussion, questioning, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form an interactive quiz administered via online tool such as Kahoot and given towards the end of this module. Such environment promote competitiveness and encourage students to be involved. After the students finish the quiz, all quiz questions will be reviewed and proper answers will be identified. This positively contribute to productive discussions in the classroom and increase the chances of students achieving higher degrees of learning.

Suitability to various groups:

In this module, the examples used and scenarios presented will have difficulty levels suitable for each of the groups. Topics covered will stress how these fundamentals of network security can be applicable to K-12 environments. Moreover, the contents presented and hands-on used will advance in the level of difficulty when being presented to the Middle school group compared to when being presented to the High school students.