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 and the role it plays in securing the information while in transit or in storage.

Moreover, the module will overview various categories of hackers and their motivations. In doing so, ethical concepts will be discussed including some of the controversies associated with various issues such as hacktivism. A considerable portion of this module is dedicated to a set of carefully chosen active learning simulations and hands-on activities in order to reinforce students' understanding of the covered topics and create a better engaging environment as described below One example of the interactive simulation used in this module is one that addresses how a real-world networking system such as email can be secured.

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. For the teachers group, topics covered will stress how these fundamentals of secure programming can be integrated into the K-12 curriculum in addition to focusing on developing a sample lesson plan for one of the discussed topic. Moreover, the contents presented and programming source code 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.

How the Teachers and Students groups will be interacting:

This module will not have explicit interaction among the three groups. But, input from the teachers will be sought on how to better deliver the module contents to the other two students groups. Teachers and student groups will have plenty of chances to work and interact with each other in most of the first day's sessions, during the two working lunches facilitated by two invited guest speakers and during the merged cyberbullies sessions on Wednesday. We will also provide a very engaging, culminating, and competition-based activity that will involve all three groups in the last day of the camp. Such culminating activity will emphasize the 10 cybersecurity first principles.