Introduction to Information 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.
- #2: Explore the use of basics operating systems commands on different platforms.
- #5: Realize the importance of password and username management and apply effective approaches to increase their security.
- #11: Develop skills needed to defeat various mal- and social engineering attacks.

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

- #4: Least Privilege
- #5: Layering
- #7: Information Hiding

Description:

This module presents an easy-to-understand introduction to fundamentals of information security. Participants will learn about key information security concepts such as confidentiality, integrity, availability, and non-repudiation. Various components of a typical information system will be presented including software, hardware, data, people, etc. The module will highlight the importance of humans as a central component of any system and how human errors are typical causes of system compromises. The common saying that "humans are the weakest link of the security chain" will be expounded with several real-world examples. In such context, several security first principles will be fully explained. The concept of least privilege will be introduced as a technique that will help minimizing human errors or at least help containing the consequences of such errors. For example, assigning a regular user privileges to an employer (and not administrative access) will result in a much less catastrophic consequences of accidental deletion of a file or improper permission settings. Such errors will be contained by the limited access privileges given to the employer. Additionally, when discussing various components of an information system the concept of layering and defense-in-depth will yield themselves well. For example, the discussion will include an explanation of how various components can be viewed as various layers of security in which an attacker has to overcome this series of defensive layers in order to conduct a successful attack.

Moreover, different types of malicious software (malware) will be presented including viruses, worms, logic bombs, Trojan horses, and back doors. Various effective countermeasures will be expounded in details including the use of antimalware and antimalware while relating such use to some the first principles such as least privileges and layering. In addition, this module will discuss various security threats and attacks including software attacks, forces of nature and equipment malfunction. 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.

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 basics of Unix/Windows commands, name resolution service, network reconnaissance and enumeration tools, and password cracking tools. 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 tophat and Poll Everywhere are good candidates in such regards.

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, peer-assessment, and constructive quizzes. For example, a carefully chosen set of questions on the covered topics can form a quiz given at the end of this module. 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:

The contents of the module will be adapted to better fit the level of each of the proposed three groups. For the teachers group, topics covered will stress how these security concepts and techniques can be integrated into the K-12 curriculum in addition to covering advanced concepts such as advanced operating systems use. The contents will also 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.