Lesson Plan

LESSON TITLE: **Module 6: Cybersecurity Challenges and Competition**

SUMMARY:

Topic Outline

- Developing competition rules
- Training Modules
- Building operating system images
- Virtualization
- Creating challenges and solutions
- Conducting an online competition
- Designing a scoring system
- Finding resources

GRADE BAND:

☐ K-2 ☒ 6-8

☐ 3-5 ☒ High School

Time Required:

60 minutes

Lesson Learning Objective/Outcomes: Upon completion of this lesson, students will be able to:

- To understand and appreciate the relevance of cybersecurity challenges and competitions.
- To learn how to create and conduct cybersecurity competitions.

Materials List:

Software tools: VirtualBox, Metasploit, QR Code reader, Kali Linux

How will you facilitate the learning?

- Describe the Warm-up Activity/Focused Activity/Closure and/or Reflection
- Describe the Teacher Instruction

We adopt the following best instructional practices and strategies to facilitate learning:

- Multimodal presentation of information
- Cooperative active learning
- Team building
- Periodic checking for understanding

This lesson includes:

☒ Mapping to Cyber Security First Principles

☒ Assessments

☒ Learning Objectives

Mapping to Cyber Security First Principles:

☐ Domain Separation

☒ Process Isolation

☐ Resource Encapsulation

☒ Modularity

☐ Least Privilege

☒ Abstraction

☒ Data Hiding

☐ Layering

☒ Simplicity

☐ Minimization

Assessment of Learning:

TYPE (Examples Listed Below)	NAME/DESCRIPTION
Quiz/Test Presentation Oral Questioning Observation Other Choose an item. Choose an item.	Online pop-quiz/survey using gosoapbox.com will be utilized to check understanding of key indicators. Key Indicators of Understanding • Familiarity with key concepts of creating challenge problems • Recognition of Cyber Security Principle involved • Being able to create a scoring system • Being able to implement a virtual system environment Hands-on exercises will be conducted to reinforce learning. Participants will be asked to present their observations on pertinent case studies.

Accommodations: (Examples may include closed captioning for hearing impaired students; accommodations for students with disabilities.)

We provide digital videos with closed captions of software tools and hands-on exercises.

Description of Extension Activity(ies):

Background Materials

Capture the Flag Competition

Capture the Flag (CTF) is a type of computer security competition wherein “flags” or “keys” are placed on computer systems in hidden, encrypted, or stored in some format that provides a challenge to the participant to access.

Key Resources for Capture the Flag Competitions

National Cyber League (http://nationalcyberleague.org/index.shtml). Provides an online virtual training facility for both faculty and students to develop and validate cybersecurity skills using team gaming concepts.

CyberPatriot (http://www.uscyberpatriot.org/home). CyberPatriot is the National Youth Cyber Education Program that has three distinct programs: the National Youth Cyber Defense Competition, AFA CyberCamps and the Elementary School Cyber Education Initiative. It was initiated by the Air Force Association (AFA) to inspire students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines.

New York University Cyber Security Awareness Week (NYU-CSAW) Capture the Flag (https://csaw.engineering.nyu.edu/ctf). Cyber Security Awareness Week is the largest student-run cyber security event in the country. One of its many competitions is the Capture the Flag (CTF) competition. The challenges are designed to enable contestants to integrate concepts, develop skills and learn to hack as they progress in the competition.

PicoCTF (https://picoctf.com/). picoCTF is a computer security game for middle and high school students. It consists of a series of challenges where participants must reverse engineer, break, hack, decrypt, or do whatever it takes to solve the challenge. The challenges are designed to be purposely hackable to provide the participants a hands-on learning experience wherein critical thinking and problem solving skills are actively applied.

Other online resources include the following:

- Smash the Stack. (http://smashthestack.org/) Challenging online exploitation exercises.
- Crackmes.de (http://crackmes.de/) Reverse engineering challenges,
- Netforce.nl (https://www.net-force.nl/) web exploitation and cryptography)
- Cybrary (https://www.cybrary.it/) Open source security training.

Virtualization

Virtualization has become an integral part of most businesses and is becoming more pervasive in several sectors of society. It has cut down on costs and increased revenue dramatically. The virtue of virtualization rests on its ability to cut down cost and to provide an effective means of managing IT resources. The purpose of our study on virtualization is two-fold: first is to find an effective way to deliver online pedagogical materials and exercise, and second is to compare the merits of various virtualization systems using a common platform.

The concept of virtualization began with the mainframe computers of the 1960's (Rosenblum, 2004). At that time, the prohibitive cost of hardware forced companies to institute timesharing systems, which allow multiple users to make use of a single computer system Crosby & Brown, 2007). To accomplish this, a piece of software called the virtual machine monitor layer (e.g., VMware) sits directly on top of the hardware and provides an abstraction for the operating system (Rosenblum, 2004). This abstraction allows the operating system to treat the virtual machine as if it were the hardware itself. A fortunate by-product of this early approach was that user processes were protected from one another, since each was run in a different instance of the virtual machine (often called a sandbox) (Ray & Schultz, 2009).

Associated Problem-based Laboratory Exercises:

I. Hands-on exercise on creating Virtual Machines (VMs)

You are required to create two VMs on the Oracle VM Virtual Box system on your desktop. The two VMs will be configured with Linux Mint Cinnamon and Windows XP, respectively. The virtual disk image (vdi) for each operating system is provided for you on the Desktop folder named VMFiles.

II. Hands-on exercise on Capture the Flag (CTF) using Penetration Testing

You are required to hack into a Windows XP machine which you earlier installed as one of the VMs. You will use Metasploit with Armitage, a penetration testing software tool, installed in the Kali Linux systems (another VM that is pre-installed in your Virtual Box). Your assignment is to capture the flag in a text file in the Windows XP VM. You know that you are successful if you see a pattern of letters that start with the word FLAG.

III. Hands-on exercise on Capture the Flag (CTF) using Social Networks

The Federal Bureau of Investigation (FBI) has received new information from Ben Louis. Ben Louis was the

Steganography and Communications expert for John T. Error. Louis has informed them that John T. Error had the group doing two jobs. During his incarceration, he was placed in minimum security. Before he could tell the FBI everything, he was broken out of jail. Word is, he is going to still do the job with his own team. The FBI would like your help again in finding him.

Your task is to track Ben Louis through social media using a technique called Open Source Intelligence (OSINT). What is the newest scheme that Ben is planning? Find the specific dates and places that are critical to Ben's plan.

Please note that some websites allow you to hide different things in the HTML code.

Here is his twitter account: @bentalkstoomuc2.

Here is a plan that may work.

1. Start off with the twitter account.
2. Find Wordpress website in the profile page.
3. Read the blog posts to find a Github account. Everything is hidden in two separate blogs.
4. Github account is hidden from plain sight. The password is in a commented code.
5. Github site tells you to go to Onedrive in a readme file.
6. Use the password to sign in Onedrive. Once logged in as Ben, search for the document.

IV. Hands-on exercise on Capture the Flag (CTF) with QR Code Scavenger Hunt applying knowledge of the 10 Cyber Security Principles

Rules:

1. You need to screen shot every clue (QR code contains key value that you will use at http://www.gosoapbox.com as event ID). Write down the key value.
2. Bring your GenCyber cards with you. Refer to those cards if needed.
3. Work together as a team but don't tell the other groups what you have found.
4. Team placement will be based on the length of time to completely collect all the key values provided by the QR codes.

Activity:

1. Start item: Minimization - The goal of minimization is to simplify the number of ways the software can be exploited. Instead of giving you another riddle, I'm just going to simplify this and tell you to go look for Michael
2. Keep on going. You will be solving a riddle pertaining to one of the 10 Cyber Security Principles as you move along. Your access code (event ID) is in the QR code.

Acknowledgements: