LAYERS OF DEFENSE COMPANY INFILTRATION

Lesson Description:

Students will learn about the layers of defense that a company may have to protect their data as well as physical security, accessibility, surveillance, password protection and the use of ciphers to code and decode. They will assume company roles and act out the various jobs to infiltrate the other company and hack their server.

Prerequisite Knowledge: Students are expected to know about the masonic cipher and basic mathematical number combinations.

Length of Completion: 90 minutes

Level of Instruction: Middle and High School Students

Applicable GenCyber Concepts: Layers of Defense and Think Like an Adversary

Resources that are Needed: PowerPoint slides, badges (blue and red), and post-it notes.

Accommodations Needed: There are no accommodations needed for this lesson.

LEARNING OUTCOMES

LESSON LEARNING OUTCOMES

- Understand how layers of defense are used in a company.
- Role-play thinking like an adversary considering physical security, accessibility, surveillance, and password protection.
- Use teamwork and critical thinking skills to solve ciphers and number combinations.

LESSON DETAILS

Interconnection: This lesson is an extension of the Defense in Depth unit, which includes various activities related to password management and data access rights, along with concepts about physical security. The main activity includes reviewing the "2.1 Onion Layers-Defense in Depth PowerPoint" and the "3.3 Usable – Cybersecurity Policy and Management."

Assessment: Students will be observed as they role-play, crack the masonic cipher and the other team's password.

Extension Activities: Review of the Masonic cipher.

Differentiated Learning Opportunities: This lesson includes various auditory and visual aids as well as a kinesthetic activity that will allow different learners to learn by role-playing.

LESSON

Lesson 1 Details: For lesson 1, please describe:

Warm Up: For the warm up, students were engaged in a discussion on the various layers of defense that exist to protect data, including cybersecurity policy and management regarding physical security concepts of access control and surveillance.

Lesson: The first part of the lesson includes an expository approach through a PowerPoint presentation about Defense in Depth ("2.1 Onion Layers – Defense in Depth") and Availability ("3.3 Usable – Cybersecurity Policy and Management"), to include issues of data access rights and cybersecurity policy related to physical security issues. Afterwards, a layers of defense activity is illustrated through the following activity:

Layers of Defense Red vs Blue Company

Preparation before class:

1. Plan on dividing the class into two groups (a red team and a blue team). Pair them up with a mix of beginner and advanced cybersecurity skills.
2. Create red and blue badges.

3. Have a paper with rules for creating a three-digit password that will be given to each team. These rules can be adjusted to make the challenge easy or difficult depending on the students. An example of these rules is below:

   <u>Red Company Password Rules:</u>

   a. Create a password that has three numbers.
   b. The numbers have to be between 1-9.
   c. The numbers need to be even.
   d. The numbers cannot be repeated.
   e. Numbers need to be in sequential order from low to high.

   2 4 6 8

   Combination possibilities: 246 248 268 468

   <u>Blue Company Password Rules:</u>

   a. Create a password that has three numbers.
   b. The numbers have to be between 1-9
   c. The numbers need to be odd.
   d. The numbers cannot be repeated.
   e. Numbers need to be in sequential order from high to low.

   1 5 7 9

   Combination possibilities: 975 971 951 751

4. Write on two post-it notes a masonic cipher that has the access code for the server (for example: CAT in masonic cipher) and each company's password rules.
5. Hide within the classroom the Red and Blue post-it notes in a common place that employees use to hide their passwords such as behind a monitor or under a keyboard.
6. Once a team decodes the masonic cipher, they will be allowed to approach the server and present the code (for example: CAT) to be able to have access and now provide what they think is the other team's password based on the company password rules from the post-it note.

Activity:

1. Students are divided into two groups to represent two companies (The Red Company and The Blue Company). Red and blue badges are passed out to the respective members of each company.
2. Half of the classroom belongs to The Red Company and the other half to The Blue Company.
3. Have each team create a password using the rules previously provided.
4. The goal of each company is to penetrate the layers of defense of the other company by entering the other company’s area bypassing the security guard, cracking the code on the hidden post-it note, and finally cracking the password that the team creates.
5. Each Company (Group) assigns the following roles to their members:
    a. Security guard (one)
    b. Hacker (one)
    c. Server(one)
    d. Workers (the rest of the students)
6. The Security guard’s job is to check to see if they have the correct identification color badge to be able to go inside the respective company. In other words, only members with red badges are allowed in The Red Company and only members with blue badges are allowed in The Blue Company.
7. The student that represents the hacker is the only one that is provided with two identification badges, a blue one and a red one in order to be able to go into the other company and bypass their security guard.
8. The goal of the hacker is to penetrate the other company using the other badge color and find the post-it note with the masonic cipher. Once this post-it note is found, the team decodes it and now has permission to talk to the other company’s server in order to figure out the other team’s password.
9. The student representing the server from their respective company sits aside and receives questions from a member of the other company that is trying to hack it. You can only ask the server a question and then you have to wait a minute to ask another one or you will get locked out for having too many wrong tries.
10. Each team will try a brute force attack and try to figure out the three-digit password by process of elimination using the rules found in the post-it note.

11. Once the correct password is provided to the server, the server has been hacked and that team/company wins the challenge.