



THINK LIKE AN ADVERSARY ESCAPE ROOM

Lesson Description:

Students will learn about reconnaissance and social engineering by viewing a PowerPoint and using online tools to look up DNS records, public information and decode ciphers (Masonic and Caesar). These skills will be put to use during the "Think Like an Adversary Escape Room" activity, where students complete three challenges and try to escape the room by figuring out the numbers to open the 3-digit combination lock.

Prerequisite Knowledge: Students are expected to know what an escape room challenge is and have a basic understanding of reconnaissance and social engineering.

Length of Completion: 90 minutes

Level of Instruction: Middle and High School Students

Applicable GenCyber Concepts: Think Like an Adversary and Confidentiality

Resources that are Needed: PowerPoint slides. Access to the following websites:

Caesar Cipher Decryption <https://md5decrypt.net/en/Caesar/>

DNS Look Up <https://mxttoolbox.com/DnsLookup.aspx>

Property Search https://www.miamidade.gov/pa/property_search.asp

A 3-digit combination lock and a treasure lock box.

Accommodations Needed: There are no accommodations needed for this lesson, other than time extension.

LEARNING OUTCOMES

LESSON LEARNING OUTCOMES

- Apply skills learned regarding reconnaissance, decoding ciphers, and performing a DNS lookup to solve various challenges and escape the room.
- Use teamwork and critical thinking skills.

LESSON DETAILS

Interconnection: This lesson is an extension of the Think Like an Adversary unit, which includes various activities related to social engineering. The main activity includes reviewing the “5.3 Think Like an Adversary- Understanding Hacking” PowerPoint.

Assessment: Students will be observed as they use the various skills learned and complete the various challenges to escape the room.

Extension Activities: Review of the Masonic and Caesar cipher online tools.

Differentiated Learning Opportunities: Groups were created with an even mix of novice and experienced students in order to make the escape room challenges fair and challenging for the students.

LESSON

Lesson 1 Details: For lesson 1, please describe:

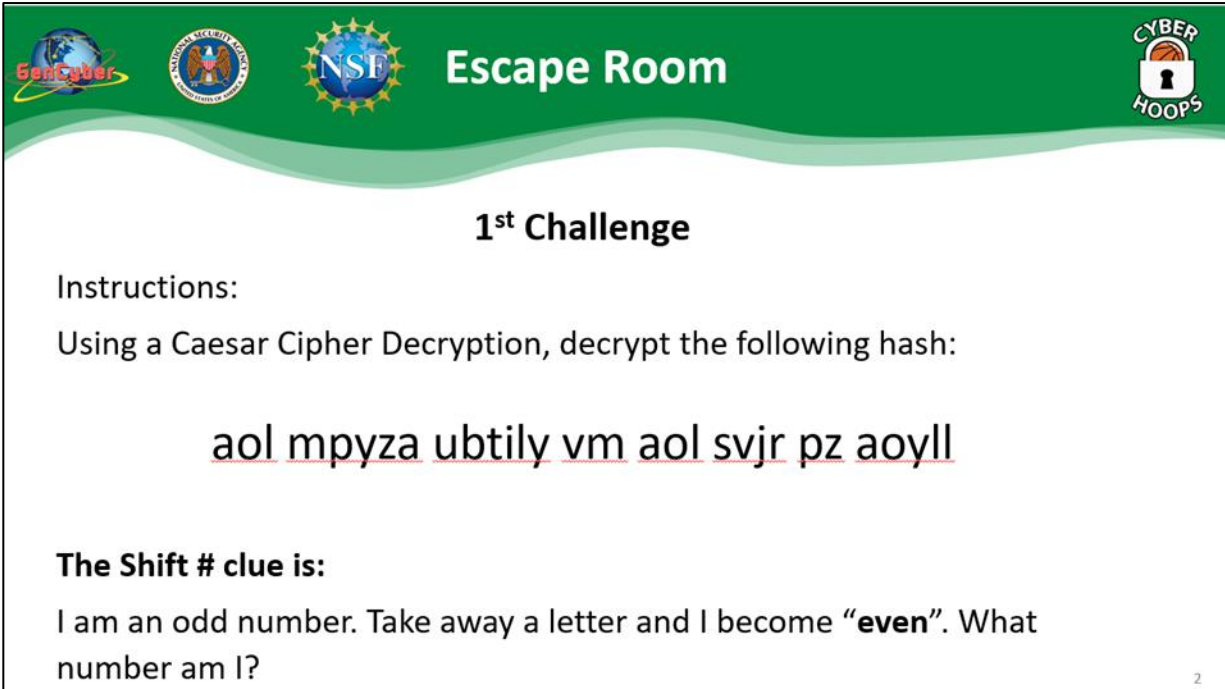
Warm Up: For the warm up, students were engaged in a discussion on how hackers use reconnaissance and social engineering. They were also asked about their previous experiences with escape rooms and an example was provided.

Lesson: Prior to the lesson, the instructor hid within the classroom a small treasure box with a three-digit lock. Also, a masonic cipher with the location of the treasure box was written with invisible ink on a sheet of paper and placed on a table with UV keychain flashlights nearby for students to use and view the cipher. Students were divided into groups of 5 students.

The first part of the lesson included an expository approach through a PowerPoint presentation about Thinking like an Adversary and Social Engineering (“5.3 Think Like an Adversary- Understanding Hacking”), which also included a series of hands-on activities related to skills needed for solving the escape room.

The escape room activity was more of an inquiry approach since the instructor provided challenges for students to follow on their own and figure out the three numbers of the lock and escape the room. These challenges were provided to each group through a set of three envelopes. Each envelope contained a challenge that needed to be solved before getting the next envelope. Once a group figured out the three numbers, they were instructed to figure out the masonic cipher hidden in the blank sheet of paper using the UV flashlights with the location of the treasure box. The first team to locate the treasure box and open the lock using the three-digit code wins the escape room challenge. All teams are given the opportunity to complete the challenge with extra time.

Below is the text found within each of the envelopes.



The image shows a challenge card with a green header. The header contains logos for GenCyber, the National Security Agency (NSA), the National Science Foundation (NSF), and CyberHoops. The main text of the card is as follows:




1st Challenge

Instructions:
Using a Caesar Cipher Decryption, decrypt the following hash:


aol mpyza ubtily vm aol svjr pz aoyll

The Shift # clue is:
I am an odd number. Take away a letter and I become “**even**”. What number am I?

2



Escape Room






2nd Challenge

Instructions:


1. Find the IP Address of the following url: enrichedfoods.org
2. The last digit of the IP Address is the second number of the lock.

Hint: You will need to use an online tool to locate the url's IP Address.
(a DNS Lookup tool)

3



Escape Room



3rd Challenge

Instructions:

1. Find the Folio Number for Ponce de Leon Middle School.
2. The last digit of the folio number is the third and final number of the lock.

Hint: Ponce de Leon Middle School is a property located in Miami Dade County.
(Use the property search tool)

Below is the answer key for each challenge:

1st Challenge

Provide a message that must be decoded using the Caesar Cipher Decoder & Encoder:

Caesar Cipher Decryption (<https://md5decrypt.net/en/Caesar/>)

The first number of the lock is 3

Shift/key number: 7

2nd Challenge

Use the MX ToolBox DNS Lookup tool to find the IP Address of a web site.

DNS Look Up <https://mxtoolbox.com/DnsLookup.aspx>

The last digit of the IP Address is the second number of the lock: 9

Type	Domain Name	IP Address	TTL
A	enrichedfoods.org	216.55.149.9	60 min

3rd Challenge

Use the Miami Dade Property Search to look up the Folio Number for Ponce de Leon Middle School.

Use the school address: 5801 Augusto St, Coral Gables, FL 33146, in the property search by address.

https://www.miamidade.gov/pa/property_search.asp

The last digit of the folio is the last number of the lock, which is 03-4129-026-2210, is 0