AP Cybersecurity: Summer Bridging Assignment

Course: Advanced Placement Cybersecurity

Due Date: First day of class

Weight: 100 points

Course Introduction

Welcome to AP Cybersecurity! This course explores the mechanics of the internet, how data is protected, how adversaries exploit vulnerabilities, and how we defend global infrastructure. To hit the ground running, you must complete this three-part summer assignment.

Part 1: The Foundations of Cryptography (By-Hand Lab)

Total: 30 Points

Before we use computers to encrypt terabytes of data, you must understand the logic behind data obfuscation.

Task A: The Caesar Cipher

The Caesar Cipher is a classic substitution cipher where each letter in the plaintext is shifted a certain number of places down the alphabet.

1. **Decrypt** the following ciphertext, which was encrypted using a **Right Shift of 7** (+7): AOPZ PZ AOL ZAHYA VM JBYLYZLJBMPAF
2. **Encrypt** your first and last name using a **Left Shift of 3** (-3). Show your work by mapping out the original letters to their cipher counterparts.

Task B: The Pigpen Cipher

1. Research the **Pigpen Cipher** (sometimes called the Masonic cipher).
2. In a brief paragraph (3–5 sentences), explain how geometric symbols are used to substitute letters. Why is this considered a "weak" cipher by modern standards?

Part 2: Current Events & Threat Analysis

Total: 30 Points

Cybersecurity changes daily. To understand the stakes of this course, you need to look at real-world impacts.

Task: The Incident Report

Find a news article from the last 12 months detailing a major cybersecurity incident (e.g., a data breach, ransomware attack, or critical vulnerability exploit). Write a **300–400 word brief** answering the following points. *Do not just copy and paste; use your own words.*

- **The Target:** Who was attacked? (An agency, a corporation, a hospital, etc.)
- **The Vector:** How did the attackers get in? (e.g., phishing email, unpatched software, compromised credentials)
- **The Impact:** What was stolen, disrupted, or held for ransom? What was the financial or societal cost?
- **The Mitigation:** What has the organization done—or what *should* they have done—to prevent this?
- **Source Citation:** Include a clean URL and the title/author of the article.

Part 3: Ethics, Law, and the "Cyber Mindset"

Total: 40 Points

In cybersecurity, the tools you use to defend a network can also be used to attack one. Ethics are paramount.

Task: Scenario Analysis

Read the following scenario and write a response (150–250 words) answering the prompt below.

> **Scenario:** Jordan is a high school student who notices that the school's online grading portal has a flaw: by changing a single number in the URL web address, any student can view the report card of any other student. Jordan does not change any grades. However, to prove the flaw exists, Jordan takes a screenshot of a friend's report card (with permission) and emails it to the school's principal to alert them.

Discussion Prompts:

1. Did Jordan behave ethically? Why or why not?
2. What is the difference between a **White Hat**, **Gray Hat**, and **Black Hat** hacker? Which category does Jordan's behavior fall into?
3. If you discovered this flaw, how would you have handled it differently to ensure you stayed within legal and ethical boundaries?