Cybersecurity Operations (6304)

Teacher Resources

Instructional Scenarios

Design Your Companies Authentication Backend

Duty/Concept Area(s): Using Desktop and Mobile Systems Concepts

Scenario:
You are currently employed at WebWidgets Incorporated as a security consultant working on the redesign and development of their authentication systems. Your job is to design the backend authentication systems for a variety of outward-facing services. You need to provide compelling arguments as to what type of authentication and authorization solutions can satisfy the security and usability needs.

WebWidgets Incorporated has the following services that their employees need to access when outside the company network:

- Webmail service
- Gitlab repositories
- Team management system
- Web admin panels

The team has already had an initial briefing where they discussed the possibility of hosting all services on their internal network or using software-as-a-service (SaaS) solutions. The CEO has expressed concerns over security, but also knows they cannot sacrifice major accessibility.

You need to explore popular methods for managing multiple services through a single-sign on (SSO) either provided by a service or housed locally. You will also have to consider the possible vulnerabilities that an SSO introduces and how those can be mitigated.

After weighing the possibilities and choosing a design, you will need to prepare a presentation for the CEO consisting of two options for your team.

Big Question:
How do modern-day systems manage network accounts for authentication and authorization through a variety of services?

Focused Questions:

- What is SSO?
- What is SaaS?
- What are common industry solutions for SSO (internal or provided) and SaaS?

- What types of threats should be considered when implementing SSO or SaaS?
- How can these threats be mitigated?

SOL Correlation:
C/T 9-12.2, C/T 9-12.3, C/T 9-12.4, C/T 9-12.5

Project-Based Assessment:
Student(s) will work to create a presentation to compare to possible designs for the company's new infrastructure.

Instructional scenario submitted by Karl Meister, Norview High School, Norfolk Public Schools, 2021.

Lockdown at International Hotel

Duty Area(s): Exploring Digital Forensics

Scenario:
Please refer to the resource link below for more information.
https://cyber.instructure.com/courses/6/pages/aics
Module 1: International Hotel Lockdown

Big Question:
How do agencies like the Department of Homeland Security investigate an incident using digital forensics and various media?

Focused Questions:

- Based on the evidence, how might you go about constructing a list of key names or groups that can be responsible for the incident?
- Based on the evidence gathered, what is the timeline of events?
- What type of information did you glean from the .txt file?

Based on the evidence, were you able to identify connections between any of the key figures involved?

Project-Based Assessment:

Groups can be graded on the following:

- Opening Statements (clear, well organized, and relevant)
- Addressed Issues (coverage of topic)
- Supporting Facts (provided facts that support the topic)
- Persuasiveness (arguments are clear and convincing)
- Teamwork (all members contributed to briefing)
- Organization (addressed likely culprit and gave clear recommended response)
- Overall preparedness, effectiveness, and professionalism

Resources: Cyber.org/Cyber Society/AICS
https://cyber.instructure.com/courses/6/pages/aics

Instructional scenario submitted Jennifer Marden, Loudoun County High School, Loudoun County Public Schools, 2021; Kristi Rice, Spotsylvania High School, Spotsylvania County Public Schools, 2021, and Katrina Riggleman, Riverbend High School, Spotsylvania County Public Schools, 2012.

Entrepreneurship Infusion Units

Entrepreneurship Infusion Units may be used to help students achieve additional, focused competencies and enhance the validated tasks/competencies related to identifying and starting a new business venture. Because the unit is a complement to certain designated courses and is not mandatory, all tasks/competencies are marked "optional."

Curriculum Resources

The Academic Initiative of the Cyber Innovation Center offers access to its curricula at no cost to K-12 teachers. These lessons could be used to supplement the following tasks:

- Task 40: Describe cybersecurity threats to an organization. (How Businesses Secure Information)
- Task 43: Describe the cyberattack surface of various organizations (How Businesses Secure Information)
- Task 64: Distinguish among types of ethical concerns. (Privacy vs. Security)
- Task 73: Explain the concept of "personally identifiable information." (You are the Data)
- Task 74: Explain how and why personal data is valuable to both an individual and to the organizations. (You are the Data)
- Task 75: Identify ways to control and protect personal data. (You are the Data)
- Task 77: Analyze the social and legal significance of the ongoing collection of personal digital information. (Your Permanent Electronic Record)

The National Institute of Standards and Technology has published the *Glossary of Key Information Security Terms*, which has been extracted from federal standards, publications, reports, and instructions.

The SANS Institute offers free professional development curricula focused on the fundamentals of cybersecurity. The course covers operating systems, networking, and systems administration.

The Virginia Cyber Range is a Commonwealth of Virginia initiative with a mission to enhance cybersecurity education for students in the Commonwealth's public high schools, colleges, and universities. The Virginia Cyber Range seeks to increase the number of fully prepared students entering the cybersecurity workforce in operations, development, and research. The Virginia Cyber Range provides an extensive Courseware Repository for educators and a cloud-hosted Exercise Area environment for hands-on cybersecurity labs and exercises for students.

AFA CyberPatriot is the National Youth Cyber Education Program created by the Air Force Association to inspire K-12 students toward careers in cybersecurity or other science, technology, engineering, and mathematics (STEM) disciplines critical to our nation's future. At the core of the program is the National Youth Cyber Defense Competition, the nation's largest cyber defense competition that puts high school and middle school students in charge of securing virtual networks.

Net Etiquette

"What do I need to know about technology?" Northern Virginia Community College

"Netiquette," Justice Institute of British Columbia

Coding Standards

"SEI CERT Coding Standards," Software Engineering Institute, Carnegie-Mellon University

Open Web Application Security Project (OWASP), focused on improving the security of software.

Job-related Tools and Data

CyberSeek: Provides detailed data about supply and demand in cybersecurity fields, including an interactive state-by-state map which shows the field where demand is highest. For job seekers, educators, school counselors, and students.

"Breaking the Code on a Career in Cybersecurity": Virginia Space Grant Consortium's free video series, which features interviews with cyber professionals about their career pathways.