IT 0150 - PRINCIPLES OF CYBERSECURITY ANALYSIS

Catalog Description

Formerly known as CIS 153
Prerequisite: Completion of IT 120 with grade of "C" or better or CompTIA Security+ certification as determined by the Information Technology Department Chair
Hours: 72 (54 lecture, 18 laboratory)
Description: Learn how to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities, threats, and risks to an organization with the end goal of securing and protecting applications and systems within an organization. This course covers skills used by Information Security (IT) security analysts, vulnerability analysts, or threat intelligence analysts with a technical, “hands-on” focus on IT security analytics. Covers exam objectives relating to the CompTIA Cybersecurity Analyst (CSA+) industry certification. (CSU)

Course Student Learning Outcomes

- CSLO #1: Research, analyze and evaluate information to solve business problems using security concepts and software.
- CSLO #2: Design and produce security solutions incorporating current trends, and best practices.
- CSLO #3: Employ security concepts and terminology in professional communication.
- CSLO #4: Demonstrate marketable security career skills.

Effective Term

Fall 2023

Course Type

Credit - Degree-applicable

Contact Hours

72

Outside of Class Hours

90

Total Student Learning Hours

162

Course Objectives

Lecture Objectives:
1. Explain the purpose of practices used to secure a corporate environment.
2. Compare and contrast common vulnerabilities found in the following targets within an organization.
3. Distinguish threat data or behavior to determine the impact of an incident.
4. Explain the importance of communication during the incident response process.
5. Analyze common symptoms to select the best course of action to support incident response.
6. Summarize the incident recovery and post-incident response process.
7. Explain the relationship between frameworks, common policies, controls, and procedures.
8. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.
9. Explain application security best practices in the Software Development Life Cycle (SDLC).
Lab Objectives:
1. Apply environmental reconnaissance techniques using appropriate tools and processes.
2. Analyze the results of a network reconnaissance.
3. Implement or recommend the appropriate response and countermeasure for a network-based threat.
4. Implement an information security vulnerability management process.
5. Analyze the output resulting from a vulnerability scan.
6. Prepare a toolkit and use appropriate forensics tools during an investigation.
7. Use data to recommend remediation of security issues related to identity and access management.
8. Review security architecture and make recommendations to implement compensating controls.

General Education Information

- Approved College Associate Degree GE Applicability
- CSU GE Applicability (Recommended-requires CSU approval)
- Cal-GETC Applicability (Recommended - Requires External Approval)
- IGETC Applicability (Recommended-requires CSU/UC approval)

Articulation Information

- CSU Transferable

Methods of Evaluation

- Classroom Discussions
  - Example: As an out-of-class assignment that will be discussed in-class, students will find information on the Internet relating to an unintended release of personal identifiable information (PII) and discuss in class the cause of the information breach and the resulting potential damage to consumers. Student performance will be evaluated by the instructor based upon a rubric provided by the instructor.
- Objective Examinations
  - Example: Primarily composed of typical certification examination multiple choice style questions, designed to test the students knowledge relative to cybersecurity concepts and skills. As an example: The process of warning a software manufacturer about a vulnerability is commonly known as: a. Fair Disclosure b. Blue Ribbon Analysis c. Black Box Testing d. White Box Testing
- Problem Solving Examinations
  - Example: The series of online labs provide "hands-on" activities that provide students with defined problems that require a response in the form of utilization of a variety of tools (skill demonstration) in order to complete the exercise. As an example: Utilizing the available virtual lab environment, students shall configure, verify, and troubleshoot static and dynamic port security. Students shall issue a report, providing screen shots that confirm their lab activities. Student performance will be evaluated by the instructor based upon a rubric provided by the instructor.

- Skill Demonstrations
  - Example: The series of online labs provide "hands-on" activities that provide students with defined problems that require a response in the form of utilization of a variety of tools (skill demonstration) in order to complete the exercise. As an example: Utilizing the available virtual lab environment, students shall configure, verify, and troubleshoot static and dynamic port security. Students shall issue a report, providing screen shots that confirm their lab activities. Student performance will be evaluated by the instructor based upon a rubric provided by the instructor.

Repeatable

No

Methods of Instruction

- Laboratory
- Lecture/Discussion
- Distance Learning

Lab:

1. After instructor demonstrates, students will utilize the available virtual lab environment and complete a topology discover exercise that includes: Basic Scanning, Topology Discovery against Firewalls, OS Fingerprinting, Output Logs, and Zenmap the Nmap GUI. Students shall issue a written report of their findings. (Lab Objective 1)

Lecture:

1. Following a lecture based on an in-class discussion relating to secure coding (programming), students will prepare as a group "mini" project a summary of what steps will be taken to ensure attention is paid to a security framework as part of the software development activities. (Lecture Objective 9)

Distance Learning

1. After watching instructor video lecture, students utilize NETLAB+ virtual lab environment to configure, verify, and troubleshoot static and dynamic port security. Students shall issue a report, providing screen shots that confirm their lab activities. (Lab Objective 7)

Typical Out of Class Assignments

Reading Assignments

1. In preparation of an in-class discussion, read the chapter associated with "secure software development" and be prepared to discuss the ramifications of changing the law with regard to the implications associated with imposing liability on software development companies that is more in line with product liability that manufactures face (e.g., fitness for a particular purpose), relative to unintended data distribution. 2. Find information on the Internet relating to an unintended release of personal identifiable information (PII) and discuss in class the cause of the information breach and the resulting potential damage to consumers.

Writing, Problem Solving or Performance

1. Utilizing www.shodan.io, identify a vulnerable system accessible from a public Internet Protocol (IP) address, and issue a report detailing the nature of the vulnerability and potential damage that may result if the vulnerability continues to exist. 2. With reference to the above vulnerability identification assignment, draft a letter to the system owner, explaining the vulnerability, utilizing the principles associated with "fair disclosure", and providing the steps you will take if the vulnerability is not removed within a prescribed time period.

Other (Term projects, research papers, portfolios, etc.)

Required Materials

- CompTIA CySA+ Study Guide Exam CS0-002
  - Author: Mike Chapple, David Seidl
  - Publisher: Wiley
  - Publication Date: 2020
  - Text Edition: 2nd
  - Classic Textbook?: No
  - OER Link:
  - OER:

Other materials and-or supplies required of students that contribute to the cost of the course.