IT 0145 - INTRODUCTION TO CYBERSECURITY: ETHICAL HACKING

Catalog Description

Formerly known as CIS 152
Prerequisite: Completion of IT 120 with grade of "C" or better
Advisory: Completion of CSCI 50 with grade of "C" or better
Hours: 72 (54 lecture, 18 laboratory)
Description: Immerses IT Professionals in hands-on intensive environment providing in-depth knowledge and experience with current essential security systems. Provides understanding of perimeter defenses and leads to scanning and attacking networks; no real networks are harmed. Students learn how intruders escalate privileges and the steps to be taken to secure a system. Also covers Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows, and Virtual Creation. Focus includes legal and regulatory requirements, ethical issues, basic methodology and technical tools used for ethical hacking and penetration tests. Students establish a pre-test agreement with the enterprise, discover and exploit vulnerabilities, participate as a member of a pen test team and prepare a penetration test report. (CSU)

Course Student Learning Outcomes

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

Provides an in-depth understanding of how to effectively protect computer networks. Students will learn the tools and penetration testing methodologies used by ethical hackers. In addition, the course provides a thorough discussion of what and who an ethical hacker is and how important they are in protecting corporate and government data from cyber-attacks. Students will learn updated computer security resources that describe new vulnerabilities and innovative methods to protect networks. Also covered is a thorough update of federal and state computer crime laws, as well as changes in penalties for illegal computer hacking.

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

- Objective Examinations
  - Example: Based upon course readings and class discussions relating vulnerability findings and exploitation, students would be required to take a quiz relating to chapter content, and to explain issues pertaining to vulnerabilities and exploits. Example: In your own words (no copy/paste allowed) identify vulnerabilities in a system and take advantage of that vulnerability. Instructor will grade based on level of understanding shown in the response.
- Problem Solving Examinations
  - Example: Students will be provided with a virtualized environment with various operating systems to exploit. Students would have to determine the right tool to use for the system being tested. Students would also have to analyze the output of various security tools utilized during this engagement. Pass/Fail grading.
- Projects
  - Example: Given a specific scenario, students would be required to prepare a Penetration Testing report. Student performance would be based upon a rubric designed to incorporate both the requirements of a Pentest report, as identified course readings, and the clearness of plan response instructions.
- Skill Demonstrations
  - Example: Students will be provided lab assignments based on the weekly topic and required to complete the tasks outlined. See the lab example in 14b for sample. Example: Students will attempt to exploit systems and discuss their process. Students will capture images to show the process and submit for grading. Grading will be based on a complete set of images with proper notations as described in the instructions. Pass/Fail grading.

Repeatable

No

Methods of Instruction

- Laboratory
- Lecture/Discussion
- Distance Learning

Lab:

1. Instructor will guide students through hands-on lab exercise to test systems for vulnerabilities and exploit those vulnerabilities utilizing tools and techniques discussed in class. (Objectives 11-14)

Lecture:

1. Students will read weekly assignments related to exploiting system vulnerabilities. The instructor will lead a review discussion on the topics covered. (Objective 11)

Distance Learning

1. Following an online instructor lecture on penetration testing standards and policies, students will be provided with a written scenario, outlining a company's penetration testing standard and policies and will test an assets security to that policy. (Objective 24)

Typical Out of Class Assignments

Reading Assignments

1. Students read from the course text. For example, students read the textbook chapter on Analyzing Vulnerability Scans and answer end of chapter questions. 2. Students perform vulnerability scans in an isolated lab environment and analyze and exploit systems based on findings

Writing, Problem Solving or Performance

Example 1: Students will utilize Kali Linux tools to test the security of operating systems and network environments Example 2: Detail the specific differences between a vulnerability scan and a penetration test. Students will also discuss use case between the two scenarios.

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

Required Materials

- CompTIA PenTest+ Study Guide: Exam PT0-002
  - Author: David Seidl
  - Publisher: Sybex
  - Publication Date: 2021
  - 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.