CIT 263 - CYBERSECURITY PENETRATION TESTING

Course Description

In this course, students will learn and practice current security assessment techniques. This includes the ability to plan/scope an assessment, understand legal/compliance requirements, perform vulnerability scanning/penetrations tests and analyze/report on their findings. This course aligns with the CompTIA Pentest+ certification exam. Group 2 course.

Credit Hours

3

Contact Hours

4

Lecture Hours

2

Lab Hours

2

Required Prerequisites

CIT 240, or instructor permission.

Recommended Prerequisites or Skills Competencies

Passing of CompTIA Security+ certification exam

General Education Outcomes supported by this course

Critical Thinking - Direct

Course Learning Outcomes

Knowledge:

- Summarize security penetration techniques used to compromise systems.
- Summarize the importance of planning for an engagement.
- Compare and contrast different attacks and exploits.
- Summarize different types of attacks.
- Summarize mitigation strategies for discovered vulnerabilities.
- Summarize reporting and communication techniques for disclosing results.

Application:

- Develop a plan and scope for an engagement.
- Perform penetration tests using security tools.
- Analyze and report results of tests performed.

Integration:

- Evaluate penetration tools based on best practices.
- Discuss the importance of performing penetration tests and vulnerability assessments.

Human Dimension:

- Discuss how security assessments (or lack of) impact stakeholders.
- Collaborate work with others to complete a desired outcome.

Caring - Civic Learning:

- Explore ethical dilemmas related to security.
- Discuss corporate responsibility as it pertains to security.

Learning How to Learn:

- Seek out solutions to problems on their own.
- Research available resources on security.