SAN JUAN COLLEGE
Success Matters

ITCT 245 – CYBERSECURITY ANALYST+ 3 CREDITS

SYLLABUS

CATALOG DESCRIPTION

An introduction that explores various methods for attacking and defending a network, security concepts and attack methodologies. Topics may include Internet architecture, routing, addressing, topology, fragmentation and protocol analysis, and the use of various utilities to explore TCP/IP. May be preparation for an industry certification exam.

Prerequisites: ITCT 115

Co-requisites: ITCT 235

Semester Offered: Spring

Common Student Learning Outcomes

Upon successful completion of San Juan College programs and degrees, the student will demonstrate competency in…

BROAD AND SPECIALIZED LEARNING

Students will actively and independently acquire, apply, and adapt skills and knowledge with an awareness of global contexts.

CRITICAL THINKING

Students will think analytically and creatively to explore ideas, make connections, draw conclusions and solve problems.

CULTURAL AND CIVIC ENGAGEMENT

Students will act purposefully, reflectively, and ethically in diverse and complex environments.

EFFECTIVE COMMUNICATION

Students will exchange ideas and information with clarity in multiple contexts.

INFORMATION LITERACY

Students will be able to recognize when information is needed and have the ability to locate, evaluate, and use it effectively.

INTEGRATING TECHNOLOGIES

Students will demonstrate fluency in the application and use of technologies in multiple contexts.

Student work from this class may be randomly selected and used anonymously for assessment of course, program, and/or institutional learning outcomes. For more information, please refer to the Dean of the appropriate School.

Course Learning Outcomes

Upon successful completion of the course, the student will be able to…

1. Apply environmental reconnaissance techniques using appropriate tools and processes.
2. Implement or recommend the appropriate response and countermeasure.

3. Analyze the output resulting from a vulnerability scan.
4. Compare and contrast common vulnerabilities found in the following targets within an organization.
5. Explain the importance of communication during the incident response process.
6. Analyze common symptoms to select the best course of action to support incident response.
7. Explain the relationship between frameworks, common policies, controls, and procedures.
8. Review security architecture and make recommendations to implement compensating controls.
9. Make use of application security best practices while participating in the Software Development Life Cycle (SDLC).
10. Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.