SAN JUAN COLLEGE
Success Matters

ITCT-240 PENTEST+ 3 CREDITS

SYLLABUS

CATALOG DESCRIPTION

This hands-on course focuses on offense through penetration testing and vulnerability assessment. Students will learn penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks. Students will also learn skills required to customize assessment frameworks to effectively collaborate on and report findings. May be preparation for an industry certification exam.

Prerequisites: ITCT 235

Semester Offered: On Demand

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. **Plan and Scope**
    a. Explain the importance of planning for an engagement

   b. Describe key legal concepts
   c. Explain the importance of scoping an engagement properly
   d. Describe the key aspects of compliance-based assessments

2. **Information Gathering and Vulnerability Identification**
   a. Conduct information gathering using appropriate techniques
   b. Perform a vulnerability scan
   c. Analyze vulnerability scan results
   d. Describe the process of leveraging information to prepare for exploitation
   e. Explain weaknesses related to specialized systems

3. **Attacks and Exploits**
   a. Compare and contrast social engineering attacks
   b. Exploit network-based vulnerabilities
   c. Exploit wireless and RF-based vulnerabilities
   d. Exploit application-based vulnerabilities
   e. Exploit local host vulnerabilities
   f. Summarize physical security attacks related to facilities
   g. Perform post-exploitation techniques

4. **Penetration Testing Tools**
   a. Use Nmap to conduct information-gathering exercises
   b. Compare and contrast various use cases of tools
   c. Analyze tool output or data related to a penetration test
   d. Analyze a basic script in Bash, Python, Ruby, and/or PowerShell

5. **Reporting and Communication**
   a. Use report writing and handling best practices
   b. Explain post-report delivery activities
   c. Recommend mitigation strategies for discovered vulnerabilities
   d. Explain the importance of communication during the penetration testing process