ITCT 275 - ETHICAL HACKING AND SYSTEMS DEFENSE 3 CREDITS

SYLLABUS

CATALOG DESCRIPTION

A study on the code of conduct and ethics of attacking systems. Focus on some fundamentals of system defense, including common countermeasures of configurations and software to prevent unauthorized system access. May be preparation for an industry certification exam.

Prerequisites: ITCT 115

Co-requisite: 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. Describe the role of an ethical hacker.
2. Differentiate between what you can or cannot do legally as an ethical hacker.
3. Critique the physical security attacks and their vulnerabilities.
4. Describe the different types of malicious software.
5. Classify the different methods of protecting against malware attacks.
6. Evaluate the different types of network attacks and how they can be prevented.
7. Research the different types of port scans currently being used; the tools available to most hackers; their purpose, and function.

8. Uncover how shell scripting is used to automate security tasks.
9. Critique the advantages and disadvantages of different Intrusion Detection (IDS) technology currently available.
10. Critique the advantages and disadvantages of different software firewall technology currently available.
11. Investigate honeypots, their purpose and usefulness in a network security plan.