Course number and name:	**CS 10215: Penetration Testing Fundamentals**
Credits and contact hours:	3 credits /3 contact hours
Instructor's or course coordinator's name:	Kevin Campbell
Text book, title, author, and year:	**Oriyano & Solomon. Hacker Techniques, Tools, and Incident Handling,** Third Edition, Burlington, MA: Jones & Bartlett, 2020(ISBN 9781284147803) **Virtual Lab Access** ISBN: 978-1-284-17265-2 Course ID: 949242

Specific course information

Catalog description: The purpose of this course is to give students of all backgrounds and experience levels a well-researched and engaging introduction to the realm of penetration testing. With real-world examples that reflect today's most important and relevant security topics, this course addresses how and why people attack computers and networks, so that students can be armed with the knowledge and techniques to successfully combat hackers. Because the world of information security changes so quickly and is often the subject of much hype, this course also aims to provide a clear differentiation between hacking myths and hacking facts. Many hands-on exercises are included, which allow students to practice skills as they are learned.

Prerequisites: CS 01210 Introduction to Computer Networks and Data Communications

Type of Course: ☐ Required ☒ Elective ☐ Selected Elective

Specific goals for the course:

1. Explain the history and current state of hacking and penetration testing, including ethical and legal implications
2. Describe fundamental TCP/IP concepts and technologies related to networking
3. Describe cryptology
4. Identify common information gathering tools and techniques
5. Perform system hacking, and web and database attacks.
6. Analyze vulnerabilities exploited by hackers
7. Identify common types of malware and the threats they pose
8. Perform network traffic analysis and sniffing by using appropriate tools
9. Perform incident handling by using appropriate methods
10. Identify security controls and defensive technologies

Required List of Topics to Be Covered:

1. TCP/IP
2. Cryptography
3. Physical Security
4. Footprinting and Port Scanning
5. Enumeration
6. Web and Database Attacks
7. Malware
8. Social Engineering
9. Incident Response
10. Defensive Technologies