Course number and name:	**CS 10218: Ethical Hacking Fundamentals**
Credits and contact hours:	3 credits / 3 contact hours
Instructor's or course coordinator's name:	Sally Tarabah
Text book, title, author, and year:	(optional textbook) *Cert Guide – CEH Version 10*, 3rd edition, by Michael Gregg and Omar Santos, 2018

Specific course information

Catalog description: This course introduces students to ethical hacking, security testing, and network defense/counter measures. Students who have strong knowledge of computer and networking learn how to protect networks by using an attacker's technique to compromise network and systems security. Hands-on lab activities enable students to learn how to protect network/systems by using the tools and methods used by hackers to break into networks/systems. Discussion topics include: hacker methodology and tools, how hackers operate, as well as setting up strong countermeasures to protect networks/systems.

Prerequisites: None

Type of Course: ☐ Required ☒ Elective ☐ Selected Elective

Specific goals for the course:

1. This course presents an overview of the principles and practices of Ethical Hacking.
2. Students will learn current trends in high technology crime, followed by an exploration of formal methodologies and best practices for the security professionals.

Required List of Topics to Be Covered:

1. Ethical Hacking basics and terminology
2. Essential network security
3. Target selection and information gathering
4. Malware threats
5. Sniffing tools, as well as the difference between active and passive sniffing
6. Web hacking, application attacks, and how SQL injection works
7. Wireless technology
8. Intrusion Detection Systems and Firewalls
9. What is a honeypot and honeynet, and how they are used
10. Fundamentals of attacking cryptographic systems
11. Cloud computing security issues
12. The importance of Physical Security