Course number and name
CSC 442 – Introduction to Cyber Security

Credits and contact hours
3 credit hours

Instructor’s or course coordinator’s name
Jean Gourd

Text book, title, author, and year
None

Other supplemental materials
None

Brief description of the content of the course (catalog description)
Overview of cyber security; provides students with practical cyber security experience based on theoretical foundations. Topics include: computer network defense, computer network attack, wireless security.

Prerequisites or co-requisites
CSC 450

Indicate whether a required, elective, or selected elective (as per Table 5-1) course in the program
Selected elective

Specific outcomes of instruction, ex. The student will be able to explain the significance of current research about a particular topic.
• This course is designed to provide students with practical cyber security experience while additionally expanding upon the theoretical foundation established in earlier courses such as advanced data structures and algorithms, operating systems and computer networks. Although introduction to a wide range of topics will be covered, the course will primarily focus on computer network defense, computer network attack, and wireless security.

Explicitly indicate which of the student outcomes listed in Criterion 3 or any other outcomes are addressed by the course.
(a) An ability to apply knowledge of computing and mathematics appropriate to the program's student outcomes and to the discipline;
(b) An ability to analyze a problem, and identify and define the computing requirements appropriate to its solution;
(c) An ability to design, implement and evaluate a computer-based system, process, component, or program to meet desired needs;
(d) An ability to function effectively on teams to accomplish a common goal;
(e) An understanding of professional, ethical, legal, security and social issues and responsibilities; and
(i) An ability to use current techniques, skills, and tools necessary for computing practice.

Brief list of topics to be covered

- Physical security
- Reconnaissance and footprinting
- Malware
- Defense in depth and defense in breadth
- Overview of covert channels
- Overview of digital forensics and steganography
- Overview of network attack
- Ethics
- Wireless Security
- Overview of security policy, legal issues, and information warfare