Cyber Security (Elective)

Course # COMP 4031

Credits 6

Pre-requisites and Co-requisites: Operating Systems, Computer Networks, Fundamentals of Programming

Course Description

This course introduces the core security concepts and skills needed to monitor, detect, analyze and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organizations. It emphasizes the practical application of the skills needed to maintain and ensure security operational readiness of secure networked systems. This course aligns with the Cisco Certified CyberOps Associate certification. Students who successfully complete this course will acquire the knowledge and skills that are required to pass the certification.

Course Learning Outcomes

Upon the completion of the course, students will be able to:

- Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
- Explain the role of the Cybersecurity Operations Analyst in the enterprise.
- Explain the features and characteristics of the Linux Operating System.
- Analyze the operation of network protocols and services.
- Explain the operation of the network infrastructure.
- Classify the various types of network attacks.
- Use network monitoring tools to identify attacks against network protocols and services.
- Explain how to prevent malicious access to computer networks, hosts, and data.
- Explain the impacts of cryptography on network security monitoring.
- Explain how to investigate endpoint vulnerabilities and attacks.
- Evaluate network security alerts.
- Analyze network intrusion data to identify compromised hosts and vulnerabilities.
- Apply incident response models to manage network security incidents.

Course Assessments and Grading

Item	Weight
Attendance	12%
Quizzes	16%
Lab assignments	22%
Midterm exam	20%
Final exam	30%