CREDIT HOURS: 3.00

CONTACT HOURS: 45.00

COURSE DESCRIPTION:
This course will teach students the latest security industry recommendations and how to properly protect servers from attacks in a variety of settings. Students will learn how to keep servers reconfigure the operating system to fully protect it, and scan hosts for known security problems. By the end of the course, students will have a solid understanding of the security architectures used by Windows and Linux

PREREQUISITES:
CIS 110 and CIS 210 and 240

EXPECTED COMPETENCIES:
Upon completion of this course, the student will be familiar with:

1. Introduction to Security
2. Malware and Social Engineering Attacks
3. Application and Network Attacks
4. Vulnerability Assessment and Mitigating Attacks
5. Host, Application, and Data Security
6. Network Security
7. Administering a Secure Network
8. Wireless Network Security
9. Access Control Fundamentals
10. Authentication and Account Management
11. Basic Cryptography
12. Advanced Cryptography
13. Business Continuity
14. Risk Mitigation

ASSESSMENT METHODS:
Student performance may be assessed by examination, quizzes, case studies, oral conversation, group discussion, oral presentations. The instructor reserves the option to employ one or more of these assessment methods during the course.

GRADING SCALE:
90%-100% = A

80%-89.9%= B
70%-79.9%= C
60%-69.9%= D
<60% = E