Wayne County Community College District

COURSE SYLLABUS

CIS 278 Certified Authorization Professional

CREDIT HOURS: 3.00 **CONTACT HOURS:** 45.00

COURSE DESCRIPTION:

This course will prepare students to understand the formalized processes for assessing risk, establishing security requirements, proper documentation, and the implementation and maintaining of network authorization policies. Students will be taught using the CAP common body of knowledge and how to utilize it to harden an organization's security posture.

Through lectures, discussions, demonstrations, textbook exercises, and classroom labs, students will also develop the skills and knowledge necessary to help prepare them for the Certified Authorization Professional (CAP) certification exam.

PREREQUISITES/ COREQUISITES: *CIS 110, CIS 240*

EXPECTED COMPETENCIES: *Upon completion of this course, the student will:*

Operation of IP Data Networks

- Identify key issues plaguing the information security world, incident management process, and penetration testing
- Classify various types of footprinting, footprinting tools, and countermeasures
- Demonstrate network scanning techniques and scanning countermeasures
- Describe enumeration techniques and enumeration countermeasures
- Explain system hacking methodology, steganography, steganalysis attacks, and covering tracks
- Classify different types of Trojans, Trojan analysis, and Trojan countermeasures
- Explain the working of viruses, and virus analysis
- Classify worms, malware analysis procedure, and countermeasures
- Explain packet sniffing techniques and how to defend against sniffing
- Describe social Engineering techniques, identify theft, and social engineering countermeasures
- Identify DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Discuss session hijacking techniques and countermeasures
- Illustrate different types of webserver attacks, attack methodology, and countermeasures

- Illustrate different types of web application attacks, web application hacking methodology, and countermeasures
- Discuss SQL injection attacks and injection detection tools
- Explain Wireless Encryption, wireless hacking methodology, wireless hacking tools, and Wi-Fi security tools
- Describe mobile platform attack vector, and roid vulnerabilities, jailbreaking iOS, windows phone 8 vulnerabilities, mobile security guidelines, and tools
- Illustrate Firewall, IDS and honeypot evasion techniques, evasion tools, and Countermeasures
- Discuss various types of buffer overflows, how to mutate a buffer overflow exploit, buffer overflow detection tools, and countermeasures
- Discuss different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks and cryptanalysis tools
- Explain various types of penetration testing, security audit, vulnerability assessment, and penetration testing roadmap

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