Wayne County Community College District

COURSE SYLLABUS

CIS 274 Certified Ethical Hacker

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

COURSE DESCRIPTION:

This course provides the “how to” of Intrusion Detection, Policy Creation, Social Engineering, DDoS Attacks, Buffer Overflows and Virus Creation. Using virtual environments, students will learn and demonstrate how to scan, test, hack, and secure their own systems. Students will also develop an understanding of how perimeter defenses work scan and attack their own networks.

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 Ethical Hacker (CEH) certification exam.

PREREQUISITES/ COREQUISITES: *CIS 272*

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

- Describe key issues plaguing the information security world, incident management process, and penetration testing
- Explain various types of foot printing tools, and countermeasures
- Describe network scanning techniques and scanning countermeasures
- Explain enumeration techniques and enumeration countermeasures
- Distinguish between system hacking methodology, steganography, steganalysis attacks, and covering tracks
- Distinguish between different types of Trojans, Trojan analysis, and Trojan countermeasures
- Explain the working of viruses, virus analysis, computer 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
- Demonstrate DoS/DDoS attack techniques, botnets, DDoS attack tools, and DoS/DDoS countermeasures
- Explain session hijacking techniques and countermeasures
- Recognize different types of webserver attacks, attack methodology, and countermeasures

- Recognize different types of web application attacks, web application hacking methodology, and countermeasures
- Recognize SQL injection attacks and injection detection tools
- Describe and test Wireless encryption, wireless hacking methodology, wireless hacking tools and wi-fi security tools
- Explain mobile platform attack vector, android vulnerabilities, jailbreaking iOS, windows pho 8 vulnerabilities, mobile security guidelines, and tools
- Demonstrate firewall, IDS and honeypot evasion techniques, evasion tools, and countermeasures
- Explain various types of buffer overflows, how to mutate a buffer overflow exploit, buffer overflow detection tools, and countermeasures
- Recognize different types of cryptography ciphers, Public Key Infrastructure (PKI), cryptography attacks, and cryptanalysis tools
- Demonstrate various types of penetration testing, security audit, vulnerability assessment, a 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