Wayne County Community College District

COURSE SYLLABUS

CIS 272 Security +

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

COURSE DESCRIPTION:

This course provides the broad-based knowledge necessary to prepare for further study in specialized Cybersecurity fields and teaches primary topics relating to securing network services, network devices and network traffic. Students will learn about IT industry-wide security topics, including communication security, infrastructure security, cryptography, access control, authentication, external attack, and operational and organization security. Other topics included in this course are protocols used in Linux, UNIX, and Windows in addition to the TCP/IP suite component protocols, and Ethernet operations.

Through lectures, discussions, demonstrations, textbook exercises, and classroom labs, students will also develop the skills and knowledge necessary to help prepare them for the Security+ certification exam.

PREREQUISITES/ COREQUISITES: *CIS 270*

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

- Identify network perimeter security and elements of an effective security policy.
- Classify encryption, including the three main encryption methods used in internetworking.
- Discuss universal guidelines and principles for effective network security, as well as guidelines to create effective specific solutions.
- Describe security principles and security attack identification.
- Identify Firewall types and common firewall terminology.
- Explain Firewall system planning including levels of protection.
- Illustrate Network firewall deployment.
- Discuss Network security including industry security evaluation criteria and guidelines used to determine three security levels.
- Identify Mechanisms used to implement security systems, tools to evaluate key security parameters, techniques for security accounts, and threats to Windows and UNIX systems.
- Illustrate Permissions identification, assignment and usage, system defaults, and security commands.

- Explain System patches and fixes including application of system patches.
- Classify Windows 2000 Registry modifications, including lockdown and removal of services for effective security in Windows 2000 and Linux.
- Identify security auditing principles, security auditor's chief duties and network risk factor assessment.
- Identify security auditing and discovery processes, audit plans, network-based and host based discovery software.
- Apply Penetration strategies and methods including identification of potential attacks.
- Identify User activities baseline, log analysis, and auditing of various activities.
- Interpret Security policy compliance and assessment reports.
- Review Operating system add-ons, including personal firewalls and native auditing.
- Identify threats to, and protecting wireless networks

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