



MERCER
COUNTY COMMUNITY COLLEGE

COURSE OUTLINE

Course Number NET244	Course Title Network Defense and Countermeasures	Credits 3
Hours: Lecture/Lab/Other 2/2/0	Pre-requisite NET104	Implementation Semester & Year Fall 2022

Catalog description:

Examines current risks and threats combined with structured safeguarding of an organization's critical electronic assets. Provides a foundation for those new to information security as well as those responsible for protecting network services, devices, traffic, and data. Broad-based, in-depth coverage prepares students for further study in other specialized security fields. Hands-on activities reinforce certification exam objectives.

General Education Category:
Not GenEd

Course coordinator:
Winston H. Maddox, Professor
Networking, Information Technology and Cybersecurity
609.570.3867, maddoxw@mccc.edu

Required texts & Other materials:

CompTIA – TESTOut Web Material ISBN:(978-1-935080-44-2)

Course Student Learning Outcomes (SLO):

Upon successful completion of this course, the student will be able to:

- Determine appropriate placement of a hub, Ethernet switch, or router. [Supports ILG # 4; PLO # 1, 3]
- Use software to identify addresses, protocols, and connectivity status in a network containing multiple interconnected devices. [Supports ILG # 2, 4, 9; PLO # 2, 4]
- Interconnect switches and routers according to a given network design specification. [Supports ILG # 4; PLO # 3, 5, 6]
- Configure switches and routers to support a specified list of protocols and technologies. [Supports ILG # 2, 4, 11; PLO #4, 6, 7]
- Configure access lists to control access to network devices or segments and general network traffic. [Supports ILG # 9, 11; PLO # 5, 6, 7]
- Verify that switches and routers, as well as their configured network services and protocols, operate as intended within a given network specification. [Supports ILG # 9, 11; PLO # 5, 6]

Course-specific Institutional Learning Goals (ILG):

Institutional Learning Goal 2. Mathematics. Students will use appropriate mathematical and statistical concepts and operations to interpret data and to solve problems.

Institutional Learning Goal 4. Technology. Students will use computer systems or other appropriate forms of technology to achieve educational and personal goals.

Institutional Learning Goal 9. Ethical Reasoning and Action. Students will understand ethical frameworks, issues, and situations.

Institutional Learning Goal 11. Critical Thinking: Students will use critical thinking skills understand, analyze, or apply information or solve problems.

Program Learning Outcomes (PLO) for Information Technology – Cybersecurity Concentration (A.A.S.)

1. Describe the elements of information security, including possible threats and attack vectors as well as the motives, goals, and objectives of information security attacks;
2. Explain what steps can be taken to secure a system, and provide secure network management and reporting;
3. Secure routers and switches and their associated networks, including installing, troubleshooting, and monitoring network devices to maintain integrity, confidentiality, and availability of data and devices;
4. Prevent common security threats, including implementing firewall and VPN technologies and perimeter defenses, conducting vulnerability and penetration testing, and scanning networked systems;
5. Describe the security weaknesses inherent in wireless networks, and implement solutions to address them;
6. Use printed and online technical documentation, and demonstrate written and oral communication skills;
7. Work effectively individually and in workgroups to install and implement information security technology

Units of study in detail – Unit Student Learning Outcomes:

Unit I [INTRODUCTION SECURITY] [Supports Course SLO # 1]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Security Landscape
- Security Concepts
- Defense Planning
- Layered Security Model

Unit II [Threats, Attacks, and Vulnerabilities] [Supports Course SLOs # 2, 5]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Understanding Attacks
- General Attack Strategy
- Explain malware
- Social Engineering
- Vulnerability Concerns

Unit III [Physical] [Supports Course SLO # 3]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Physical Threats
- Implement Physical Security
- Device & Network Protection
- Environmental Controls
- Securing Environmental Systems

Unit IV [Networks and Host Design and Diagnosis] [Supports Course SLO # 4]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Design Manageable Network Plan
- Windows System Hardening
- Operating System Hardening
- File Server Security
- Linux Host Security

Unit V [Devices and infrastructures] [Supports Course SLO # 4, 5]

Learning Objectives

The student will be able to...: Explain and Demonstrate

- Security Appliances
- Configure Network Security Appliance Access
- Configure Demilitarized Zones
- Configure Firewalls
- Configure Network Address Translation
- Explain Virtual Private Networks

Unit VI [Identity, Access and Account Management] [Supports Course SLO # 6]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Explain Access Control Models
- Discuss Authentication Methods
- Biometrics & Authentication technologies
- Explain Authorization
- Windows User Management
- Explain Active Directory

Unit VII [Cryptography and PKI] [Supports Course SLO # 3]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Explain Cryptography Concepts
- Cryptography Implementation
- Discuss Hashing & Algorithms
- File Encryption & File Systems
- Public Key Infrastructure

Unit VIII [Wireless Threats] [Supports Course SLO # 5]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Wireless Network Overview
- Configuring Wireless Connections
- Wireless Attacks
- Wireless Defenses
- Authentication and Access Methods

**Unit IX [Virtualization, Cloud Security & Securing Mobile Devices]
[Supports Course SLO # 4, 5]**

Learning Objectives

The student will be able to... Explain and Demonstrate

- Host Virtualization
- Virtual Networking
- Software-Defined Networking
- Cloud Services & Security
- Mobile Device Management
- BYOD Security

Unit X [Securing Data & Applications] [Supports Course SLO # 3, 6]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Data Transmission Security
- Applying SSL to Website
- Data Loss Prevention
- Web Application Attacks
- Application Development & Security

Unit XI [Securing Assessments] [Supports Course SLO # 4, 6]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Explain and demonstrate Penetration Testing
- Monitoring and Reconnaissance
- Intrusion Detection
- Security Assessment Techniques
- Protocol Analyzers & Network Attacks

Unit XII [Incident Response, Forensics & Recovery] [Supports Course SLO # 3, 4]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Explain Incident Response
- Mitigation of an Incident
- Log Management, Windows Logging
- Digital Forensics, File and Packet Manipulation
- Redundancy, Backup & Restore

Unit XIII [Risk Management] [Supports Course SLO # 3, 6]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Organizational Security Policies
- Managing Third Parties
- Risk Management, Types & Tolerance
- Business Continuity Planning
- Email Security, Securing Email Server

Unit XIV [Governance & Compliance] [Supports Course SLO #4, 5, 6]

Learning Objectives

The student will be able to... Explain and Demonstrate

- Auditing Windows Security Log
- Configure Advance Audit Policy
- Management Controls and Frameworks
- Sensitive Data & Privacy Breaches
- File Shredding & Hard Drive Wiping

Evaluation of student learning:

Evaluation of student learning: [Evaluates SLOs #1, 2, 3, 4, 5, 6]

Students' achievement of the course objectives evaluated through use of the following:

- TESTOut Lab assignments assessing students' hardware comprehension skills related to the unit objectives.
- TESTOut Lab Chapter quizzes assessing students' comprehension of software computer concepts related to the unit objectives.
- Research and Final Research presentation assessing students' comprehension through the use of word, PowerPoint and graphics to demonstrate knowledge
- Basic programming Labs and Quizzes assignments assessing students' basic comprehension of cyber defense and analysis functions and skills related to the unit objectives.
- Exams and Final Research Presentation assessing students' comprehension of computer concepts and applications related to the unit objectives.

Grade Criteria

Item	Percent	Description
TESTOut Labs	10%	Activity-based lab Assignment Cyber Analysis
TESTOut Quizzes	10%	15 Question quiz for each unit of Cyber Defense Concepts
Exams	35%	3 Assignment based on your IT Topics leading to the final project
Final Research Presentation	45%	Professional Cyber Analysis Presentation