



MERCER
COUNTY COMMUNITY COLLEGE

COURSE OUTLINE

Course Number	Course Title	Credits
NET240	Network Security	3
Hours: Lecture/Lab/Other	Pre-requisite	Implementation Semester & Year
2/2/0	NET130, NET244 Recommended	Fall 2022

Catalog description:

Explores security design considerations for enterprise networks through the evaluation of existing and planned technical environments, including identifying security risks and defining security baselines. Topics include controlling resource access using various security techniques. Hands-on exercises 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:

Cisco – Web Material ISBN:(OER Materials)

Course Student Learning Outcomes (SLO):

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

1. Analyze business security requirements, including strategies, structures, and processes. *[Supports ILG # 11; PLO # 1, 4]*
2. Evaluate a company's existing and planned technical environment. *[Supports ILG # 9,11; PLO # 2, 3, 5]*
3. Identify security risks and requirements and define security baselines. *[Supports ILG # 4; PLO # 1, 3, 7]*
4. Evaluate and implement corporate security policy. *[Supports ILG # 4; PLO # 3, 4]*
5. Evaluate and implement network security, including routers, firewalls and servers. *[Supports ILG # 2; PLO #4, 5, 6, 7]*

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 / Network Security] [Supports Course SLO # 1]

Learning Objectives

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

- Critical Cyber Concepts: Identity Introduction
- Introduction Network Security
- Importance of Network Security
- Network Security Issues
- Types of Security issues and attacks
- Analyze Advanced Persistent Threats

Unit II [Security Policy] [Supports Course SLOs # 2]

Learning Objectives

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

- Organizational Security
- Security Controls
- Establishing Network security policy
- The importance of protecting the network
- The security posture assessment process

Unit III [Evaluating Security Policy] [Supports Course SLO # 3]

Learning Objectives

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

- Risk Identification Process
- Introduction to Cisco Security Technologies
- Access control Lists
- Securing your network using Cisco Routers – the basics
- Securing the router Hands-on practice lab configuring Cisco router

Unit IV [Implementing Security Policy] [Supports Course SLO # 4]

Learning Objectives

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

- Explain security policies
- Phases of a social engineering attack: common, motivation, approaches
- Securing your network using Cisco routers – the basics
- Securing the router Hands-on practice lab configuring Cisco router

Unit V [Hands-on Practice Lab Configuring Cisco Router] [Supports Course SLO # 5]

Learning Objectives

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

- Explain difference between passive and active reconnaissance
- Reconnaissance Countermeasures
- Working with Routers to Secure Networks
- Manage DNS/Linux Servers and analysis Data
- Define and explain type(s) of information gathered with scanning

Unit VI [Implementing Security II] [Supports Course SLO # 4]

Learning Objectives

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

- Demonstrate an analyze functional issues of Directory Access Protocol (LDAP)
- Securing Routers and Switches
- Define critical aspects of securing switches

Unit VII [Implementing Security Policy III] [Supports Course SLO # 3]

Learning Objectives

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

- Establish Network Security Policy
- Securing your network using Cisco routers
- Controlling access to internal networks
- Securing the router Hands-on practice lab configuring Cisco router

Unit VIII [Security Cisco Routers] [Supports Course SLO # 5]

Learning Objectives

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

- Define Vulnerability Management Life Cycle
- Explain Network Vulnerability Systems and Analyses
- Demonstrate a functional knowledge top assessment tools for networks and mobile devices
- Compile, explain information expected from vulnerability reports
- Explain how role-based access management differs from attribute-based access management

Unit IX [Security Firewalls] [Supports Course SLO # 5]

Learning Objectives

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

- Define Malware
- Securing your network using a Firewall
- Controlling access to internal networks
- Hands-on practice lab configuring Cisco PIX Firewall
- Explain and demonstrate best methods for detecting malware
- Discuss difference between antivirus and anti-malware software

Unit X [Implementing Cisco PIX Firewalls] [Supports Course SLO # 5]

Learning Objectives

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

- Explain Intrusion Detection Systems
- Discuss detection systems methods to avoid intrusion
- Firewalls: different firewall architectures
- Analyze Web Servers: 3-way handshakes, web servers, traversal attacks
- Demonstrate and Analyze Network Access Control and Security levels

Unit XI [Network Security Servers] [Supports Course SLO # 4, 5]

Learning Objectives

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

- Securing your network Servers using a Firewall
- Controlling access to internal networks
- Hands-on practice lab configuring Cisco PIX Firewall Bluetooth Security
- Mobile Device Security
- Cloud Security
- Internet of Things Security

Unit XII [Intrusion Detection] [Supports Course SLO # 2, 3, 5]

Learning Objectives

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

- Hardware Analysis
- Security Information and Event Management (SIEM)
- *Introduction to Intrusion detection Systems (IDS)*
- *Hands-on practice lab*
- Asset and Change Management

Unit XIII [Group Project Implementation] [Supports Course SLO # 4, 5]

Learning Objectives

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

- Software Development
- Group Project Implementing
- Network Security to secure the network

Unit XIV [Secure Group Policies] [Supports Course SLO # 5]

Learning Objectives

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

- Data Analysis and Protection
- Group Project Implementing
- Network Security to secure the network infrastructure
- Implementing Cisco router, Cisco PIX Firewall and WIN 2000 Servers.

Evaluation of student learning:

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

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

- Cisco Lab assignments assessing students' hardware comprehension skills related to the unit objectives.
- Cisco 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