COURSE OUTLINE

Course Number	Course Title	Credits
NET 241	**Cyber Security Analytics**	**3**
Hours: Lecture/Lab/Other	**Co- or Pre-requisite**	**Implementation Semester & Year**
2/2/0	**NET104, NET120**	**Fall 2023**

Catalog description:

Determine, analyze, and plan for threats to and vulnerabilities of computer information technology software and hardware systems. Emphasis includes risk mitigation, compliance and assessment involving proactive threat intelligence to manage organizational security, monitoring for indicators of compromise, and incident response applying basic digital forensics 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:

CompTIA – TESTOut Web Material ISBN:(978-1-935080-73-2)

Course Student Learning Outcomes (SLO):

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

1. Threats and vulnerabilities: use proactive threat intelligence to manage organizational security and vulnerability activities. **[Supports ILG # 4; PLO # 1, 2, 3]**
2. Software and systems: employ security solutions to manage infrastructure and understand software and hardware assurance best practices **[Supports ILG # 4,9; PLO # 2, 4, 5]**
3. Compliance and assessment: apply security concepts for risk mitigation and learn the importance of frameworks, policies, procedures, and controls. **[Supports ILG # 4 ; PLO # 3, 5, 7, 8]**
4. Security operations and monitoring: analyze security-monitoring data and apply configuration changes to existing controls as a way to improve security... **[Supports ILG # 4,11; PLO #4, 6, 8]**
5. Incident response: use the appropriate procedures, check potential indicators of compromise, and apply basic digital forensics techniques. **[Supports ILG # 2, 9; PLO # 2, 3, 6]**
6. Administer Group Accounts, including planning and creating, understanding Default Groups, and special Administrator Groups. **[Supports ILG # 9, 11 ; PLO # 4, 5, 6, 7]**
7. Secure network resources, including understanding and implementing NTFS permissions, special permissions, copying and moving files and folders, and troubleshooting permission problems. [**Supports ILG # 4, 9,11; PLO # 3, 5, 6, 8]**

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 for Cyber Security Analytics (PLO)

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;
8. Pass industry certifications, including CompTIA's Security+; EC-Council's CEH (Certified Ethical Hacker); and Cisco's CCENT, CCNA, and CCNA: Security.

Units of study in detail – Unit Student Learning Outcomes:

Unit I [INTRODUCTION / Cyber Security Analytics] [Supports Course SLO # 1]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Critical Cyber Concepts: Identity Introduction
- Using the Lab Simulator
- Explore Multiple Defense Issues
- Overview Threat(s) Intentional/Unintentional
- Install Cyber Analysis Software
- Analyze Advanced Persistent Threats
- Install Network Attached Storage Device (NAS)

Unit II [Penetration Testing and Threat Hunting] [Supports Course SLOs # 2]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Organizational Security
- Security Controls
- Attack Frameworks
- Threat Intelligence Sharing

Unit III [Risk Identification Process] [Supports Course SLO # 3]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Risk Identification Process
- Risk Calculation
- Explain difference between quantitative and qualitative analysis
- Risk Communication and Training
- Define the calculation for single loss expectancy
- Explain roles of the different security teams: Red, Blue and White
- Define the calculation for single/ annual loss expectancy

Unit IV [Social Engineering] [Supports Course SLO # 4]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Explain social engineering
- Phases of a social engineering attack: common, motivation, approaches
- Manage Physical Security
- Countermeasures and Prevention
- Demonstrate knowledge of natural disasters can effect on company's physical assets
- Identify vulnerabilities and asset criticality

Unit V **[Reconnaissance Overview] [**Supports Course SLO # 5]

Learning Objectives

The student will be able to…: Explain and Demonstrate

- Reconnaissance Overview
- Explain difference between passive and active reconnaissance
- Reconnaissance Countermeasures
- Identify the concept of enumeration
- *Manage DNS/Linux Servers and analysis Data*
- *Perform a System* Scan
- *Define and explain* type(s) of information gathered with scanning

Unit VI **[Enumeration Overview] [**Supports Course SLO # 6]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Discuss Enumeration Overview
- Explain Simple Network Management Protocol (SNMP) used
- Perform: Enumeration with Nmap, Metaploit an MSSQL Metasploit
- Enumeration Countermeasures
- Demonstrate the use of Domain Name System (DNS) attack countermeasures
- Demonstrate an analyze functional issues of Directory Access Protocol (LDAP)

Unit VII **[Vulnerability Assessment] [**Supports Course SLO # 3]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Explain the top nine areas to research when conducting an assessment
- Identify are seven types of assessments
- Define Vulnerability Management Life Cycle
- Explain Vulnerability Scoring Systems and Analyses
- Demonstrate a functional knowledge top assessment tools for networks and mobile devices
- Compile, explain information expected from vulnerability reports

Unit VIII **[Identity and Access Management Security] [**Supports Course SLO # 5, 7]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Identity and access management important to an organization
- Explain how role-based access management differs from attribute-based access management
- Privilege Escalation: privilege escalation attacks, prevention and resolution
- Identity and Access Management Threats: Spraying and Stuffing
- Explain Certificate Management: Purpose, Use, in different environments
- Given a scenario, analyze the output from common vulnerability assessment tools

Unit IX **[Combat Malware] [**Supports Course SLO # 5, 7]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Define Malware
- Explain and demonstrate best methods for detecting malware
- Discuss difference between antivirus and anti-malware software
- Demonstrate the use of Open Ports, with Netsta
- Explain Open Port use from a Remote Computer
- *Explain Sniffing:* tools: used for network sniffing
- *Explain* and provide an analysis of DoS/DDoS and prevention methods

Unit X **[Intrusion Detection Systems] [**Supports Course SLO # 5, 7]

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 **[Wireless Security] [**Supports Course SLO # 5, 7]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Explain Critical aspects of Wireless Security
- Discuss critical aspects of wireless security
- Explain Wi-Fi Encryption protocols
- Bluetooth Security
- Mobile Device Security
- Cloud Security
- Internet of Things Security

Unit XII **[Hardware Analysis] [**Supports Course SLO # 5, 7]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Hardware Analysis
- Security Information and Event Management (SIEM)
- Log Review
- Asset and Change Management
- Virtualization Management

Unit XIII **[Software Development Overview] [**Supports Course SLO # 5, 7]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Software Development
- Software Development Life Cycle (SDLC) Integration
- Automation
- Application programming interface (API) integration

Unit XIV **[Data Analysis and Protection] [**Supports Course SLO # 5, 7]

Learning Objectives

The student will be able to… Explain and Demonstrate

- Data Analysis and Protection
- Discuss: Uniform Resource Locator (URL) and Domain Name System (DNS)
- DNS analysis - domain generation algorithm

Evaluation of student learning:

Evaluation of student learning: [Evaluates SLOs #1, 2, 3, 4, 5, 6, 7]

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