SEC 160: Security Administration I

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course provides an overview of security administration and fundamentals of designing security architectures. Topics include networking technologies, TCP/IP concepts, protocols, network traffic analysis, monitoring, and security best practices. Upon completion, students should be able to identify normal network traffic using network analysis tools and design basic security defenses.
Course Hours per Week: Class, 2. Lab, 2. Semester Hours Credit, 3.

LEARNING OUTCOMES:

Upon completing requirements for this course, the student will be able to:

a. Identify security best practices.
    a. Explain the role of the Cybersecurity Operations Analyst in the enterprise.
    b. Install virtual machines to create a safe environment for implementing and analyzing cybersecurity threat events.
    c. Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.
    d. Explain the features and characteristics of the Linux Operating System.
b. Identify normal network traffic using network analysis tools.
    a. Analyze the operation of network protocols and services.
    b. Explain the operation of the network infrastructure.
    c. Classify the various types of network attacks.
    d. Use network monitoring tools to identify attacks against network protocols and services.
c. Demonstrate methods for keeping networks and their computers secure.
    a. Use various methods to prevent malicious access to computer networks, hosts, and data.
    b. Explain the impacts of cryptography on network security monitoring.
    c. Explain how to investigate endpoint vulnerabilities and attacks.
    d. Evaluate network security alerts.
    e. Analyze network intrusion data to identify compromised hosts and vulnerabilities.
    f. Apply incident response models to manage network security incidents.

OUTLINE OF INSTRUCTION:

I. Cybersecurity and the Security Operations Center - Explain the role of the Cybersecurity Operations Analyst in the enterprise.
    a. The Danger - Explain why networks and data are attacked.
    b. Fighters in the War Against Cybercrime - Explain how to prepare for a career in Cybersecurity operations.

II. Windows Operating System - Explain the Windows Operating System features and characteristics needed to support cybersecurity analyses.

a. Windows Overview - Explain the operation of the Windows Operating System.
b. Windows Administration - Explain how to secure Windows endpoints.

III. Linux Operating System - Explain the features and characteristics of the Linux Operating System.
a. Using Linux - Perform basic operations in the Linux shell.
b. Linux Administration - Perform basic Linux administration tasks.
c. Linux Clients - Perform basic security-related tasks on a Linux host.

IV. Network Protocols and Services - Analyze the operation of network protocols and services.
a. Network Protocols - Explain how protocols enable network operations.
b. Ethernet and Internet Protocol (IP) - Explain how the Ethernet and IP protocols support network communication.
c. Connectivity Verification - Use common testing utilities to verify and test network connectivity.
d. Address Resolution Protocol - Explain how the address resolution protocol enables communication on a network.
e. The Transport Layer and Network Services - Explain how transport layer protocols and network services support network functionality.
f. Network Services - Explain how network services enable network functionality.

V. Network Infrastructure - Explain the operation of the network infrastructure.
a. Network Communication Devices - Explain how network devices enable wired and wireless network communication.
b. Network Security Infrastructure - Explain how devices and services are used to enhance network security.
c. Network Representations - Explain how networks and network topologies are represented.

VI. Principles of Network Security - Classify the various types of network attacks.
a. Attackers and Their Tools - Explain how networks are attacked.
b. Common Threats and Attacks - Explain the various types of threats and attacks.

VII. Network Attacks: A Deeper Look - Use network monitoring tools to identify attacks that against network protocols and services.
a. Observing Network Operation - Explain network traffic monitoring.
b. Attacking the Foundation - Explain how TCP/IP vulnerabilities enable network attacks.
c. Attacking What We Do - Explain how common network applications and services are vulnerable to attack.

VIII. Protecting the Network - Use various methods to prevent malicious access to computer networks, hosts, and data.
a. Understanding Defense - Explain approaches to network security defense.
b. Access Control - Explain access control as a method of protecting a network.
c. Network Firewalls and Intrusion Prevention - Explain how firewalls and other devices prevent network intrusions.
d. Content Filtering - Explain how content filtering prevents unwanted data from entering the network.
e. Threat Intelligence - Use various intelligence sources to locate current security threats.

IX. Cryptography and the Public Key Infrastructure - Explain the impacts of cryptography on network security monitoring.
a. Cryptography - Use tools to encrypt and decrypt data.
b. Public Key Cryptography - Explain how the public key infrastructure (PKI) supports network security.

X. Endpoint Security and Analysis - Explain how to investigate endpoint vulnerabilities and attacks.
a. Endpoint Protection - Use a tool to generate a malware analysis report.

    b. Endpoint Vulnerability Assessment - Classify endpoint vulnerability assessment information.

XI. Security Monitoring - Evaluate network security alerts.

    a. Technologies and Protocols - Explain how security technologies affect security monitoring.
    b. Log Files - Explain the types of log files used in security monitoring

XII. Intrusion Data Analysis - Analyze network intrusion data to identify compromised hosts and vulnerabilities

    a. Data Collection - Explain how security-related data is collected.
    b. Data Preparation - Arrange a variety of log files in preparation for intrusion data analysis.
    c. Data Analysis - Analyze intrusion data to determine the source of an attack.

XIII. Incident Response and Handling - Explain how network security incidents are handled by CSIRTs.

    a. Incident Response Models - Apply incident response models to an intrusion event.
    b. CSIRTs and NIST 800-61r2 - Apply standards specified in NIST 800-61r2 to a computer security incident.
    c. Case-Based Practice Given a set of logs, isolate a threat actor and recommend an incident response plan.