SEC 150: Secure Communications

COURSE DESCRIPTION:

Prerequisites: None
Corequisites: None

This course provides an overview of current technologies used to provide secure transport of information across networks. Topics include data integrity through encryption, Virtual Private Networks, SSL, SSH, and IPSec. Upon completion, students should be able to implement secure data transmission technologies.
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 components of secure data transmission.
   1. Explain network threats, mitigation techniques, and the basics of securing a network.
   2. Describe LAN security considerations and implement endpoint and Layer 2 security features.
   3. Describe methods for implementing data confidentiality and integrity.
   4. Secure administrative access on Cisco routers.

B. Configure cryptographic elements for communication support.
   1. Secure administrative access with AAA.
   2. Implement firewall technologies to secure the network perimeter.
   3. Configure IPS to mitigate attacks on the network

C. Implement secure data transmission using Virtual Private Networks.
   1. Apply symmetric and asymmetric encryption to appropriate activity
   2. Implement management of Public Key Infrastructure and certificates
   3. Harden systems to increase security
   4. Assess vulnerability to identify and manage risk and threats
   5. Implement secure virtual private networks
   6. Implement a firewall configuration using the CLI
   7. Implement a firewall configuration and VPNs using GUI
   8. Test network security and create a technical security policy

OUTLINE OF INSTRUCTION:

I. Modern Network Security Threats - Explain network threats, mitigation techniques, and the basics of securing a network
   a. Securing Networks - Explain network security
   b. Network Threats - Describe various types of threats and attacks
   c. Mitigating Threats - Explain tools and procedures to mitigate the effects of malware and common network attacks.

II. Securing Network Devices - Secure administrative access on Cisco routers

  a. Securing Device Access - Configure secure administrative access
  b. Assigning Administrative Roles - Configure command authorization using privilege levels and role-based CLI
  c. Monitoring and Managing Devices - Implement the secure management and monitoring of network devices.
  d. Using Automated Security Features - Use automated features to enable security on IOS-based routers.

III. Authentication, Authorization and Accounting - Secure administrative access with AAA
  a. Purpose of AAA - Explain how AAA is used to secure a network.
  b. Local AAA Authentication - Implement AAA authentication that validates users against a local database.
  c. Server-Based AAA - Explain server-based AAA authentication and its communication protocols.
  d. Server-Based AAA Authentication - Implement server-based AAA authentication using TACACS+ and RADIUS protocols.
  e. Server-Based AAA Authorization and Accounting - Configure server-based AAA authorization and accounting

IV. Implementing Firewall Technologies - Implement firewall technologies to secure the network perimeter
  a. Access Control Lists - Implement access control lists (ACLs) to filter traffic and mitigate network attacks on a network.
  b. Firewall Technologies - Configure a classic firewall to mitigate network attacks.
  c. Zone-Based Policy Firewalls - Implement Zone-Based Policy Firewall using CLI.

V. Implementing Intrusion Prevention - Configure IPS to mitigate attacks on the network
  a. IPS Technologies - Explain how network-based IPS is used to help secure a network.
  b. IPS Signatures - Explain how signatures are used to detect malicious network traffic.
  c. Implement IPS - Configure Cisco IOS IPS operations using CLI.

VI. Securing the Local Area Network - Describe LAN security considerations and implement endpoint and Layer 2 security features
  a. Endpoint Security - Explain endpoint vulnerabilities and protection methods.
  b. Layer 2 Security Considerations - Implement Layer 2 security features.

VII. Cryptographic Systems - Describe methods for implementing data confidentiality and integrity
  a. Cryptographic Services - Explain how the types of encryption, hashes, and digital signatures work together to provide confidentiality, integrity, and authentication.
  b. Basic Integrity and Authenticity - Explain how cryptographic hashes are used to ensure data integrity and authentication.
  c. Confidentiality - Explain how encryption algorithms are used to ensure data confidentiality.
  d. Public Key Cryptography - Explain how a public key infrastructure is used to ensure data confidentiality and provide authentication.

VIII. Implementing Virtual Private Networks - Implement secure virtual private networks
  a. VPNs - Explain the purpose of VPNs.
  b. IPsec VPN Components and Operation - Explain how IPsec VPNs operate.
  c. Implementing Site-to-Site IPsec VPNs with CLI - Configure a site-to-site IPsec VPN, with pre-shared key authentication, using CLI.

IX. Implementing the Cisco Adaptive Security Appliance - Implement an ASA firewall configuration using the CLI.
  a. Introduction to the ASA - Explain how the ASA operates as an advanced stateful firewall.
  b. ASA Firewall Configuration - Implement an ASA firewall configuration.

X. Advanced Cisco Adaptive Security Appliance - Implement an ASA firewall configuration and VPNs using ASDM

a. ASA Security Device Manager - Implement an ASA firewall configuration.

b. ASA VPN Configuration - Configure remote-access VPNs on an ASA.

XI. Managing a Secure Network Test network security and create a technical security policy.

a. Network Security Testing - Explain the various techniques and tools used for network security testing.

b. Developing a Comprehensive Security Policy - Explain how to develop a comprehensive security policy.