

COURSE OUTLINE

CMSY-262

Introduction to Encryption and VPN Technology
3 Semester Hours

HOWARD COMMUNITY COLLEGE

Description

Upon completion of this course, students will be able to identify and apply principles of encryption. Students will be able to describe and validate the methodology of VPN installs. The concepts of virtual private networks and data encryption will become part of the student's skill set. This course is designed with a computer administrator operator in mind. A computer professional with an MCSE or equivalent would have adequate background knowledge. Prerequisites: CMSY-162 - Introduction to Network Security Systems, or a fairly extensive background in computer administration. (3 hours lecture, 1 hour lab)

Overall Course Objectives

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

1. Define the concepts of privileged access and restricted access to certain data.
2. Understand and identify encryption algorithms.
3. Demonstrate the use of a packet sniffer in order to determine whether data traversing a network is safe.
4. Employ the use of public key encryption and SSL for website assurance.
5. Identify the different tunneling protocols used for VPN connectivity.
6. Demonstrate the capability of establishing a VPN and determining whether the traffic is encrypted or not.
7. Identify specific needs for physical security to protect network systems.

Major Topics

- I. Define encryption algorithms and their applications
 - A. Private key encryption
 1. DES, 3DES, AES
 - B. Public key encryption
 1. RSA, SSL
 - C. One way hash
 1. SHA, MD5
- II. Creating a secure website
 - A. Define our certificate
 - B. Install and test SSL
- III. VPN tunneling protocols
 - A. PPTP – Point-to-Point tunneling protocol
 - B. IPSec – IP Security
 - C. L3TP – Layer 2 tunneling protocol

- IV. VPN tunnel communications
 - A. Establish a tunnel with secure communication
 - B. Use a packet sniffer to determine if the traffic is encrypted or not
 - C. Understand the limitations of VPN's and when they should be used
- V. Physically securing your systems
 - A. Use of manned facility requirements such as:
 - 1. Restricted areas
 - 2. Escort requirements
 - 3. Alarms
 - B. Use of technical controls such as:
 - 1. Smart/Dumb cards
 - 2. Biometric access
 - 3. Fire Detection and Prevention

Course Requirements

Grading/exams/projects: This course is more advanced than the introductory course. It has much more extensive hands-on labs and configuration of network systems. During the course, the students will be exposed to VPN, encryption, and encryption technology. Students will be expected to establish a VPN and determine if it is functioning correctly. Grading will be based upon a combination of exams and labs. The labs will be hands-on system configuration with the students having to properly configure and implement a VPN system.

Other Course Information

- Access Control Systems and Methodology
 - Identification and Authentication techniques
 - Method of attacks
 - Monitoring
- Cryptography
 - Basic concepts within cryptology
 - Public and private key algorithms in terms of their applications and uses
- Law, Investigation and Ethics
 - Define characteristics of Due care
- Physical Security
 - Threats, Vulnerabilities, and Countermeasures related to physically protecting the enterprise's sensitive information assets
- Security Architecture and Models
 - Security models in terms of confidentiality, integrity, and availability
- Security Management Practices
 - Data classification
 - Risk management and tools
 - Roles and responsibilities
- Telecommunications, Network and Internet Security
 - Communications and Network Security
 - Internet Protocols
 - Network Attacks and Countermeasures