COURSE DESCRIPTION

Provides instruction that shows students how to gather and analyze business requirements for a secure network infrastructure and design a security solution that meets those requirements.

Lecture – 3 hours per week

RECOMMENDED CO-REQUISITES OR PRE-REQUISITES


COURSE OBJECTIVES

This course is intended to serve as a resource to aid the student seeking Microsoft Certified System Engineer (MCSE) certification in Windows 2003, roughly mapping to the contents tested over in the Microsoft Exam 70-298 - Designing Security for a Microsoft Windows Server 2003 Network. Upon completion of this course, students will be able to:

Plan a framework for network security.
Identity threats to network security.
Analyze security risks.
Design security for physical and logical resources, including computers.
Design security for data
Design security for authentication.
Design security for data transmission.
Design security for network perimeters.
Design an incident response procedure.

Optional objectives that can be covered include:

Design an acceptable use policy.
Design policies for managing networks.
Design an operations framework for managing security.

COURSE CONTENT

Concept 1 - Planning for Network Security: Discuss the importance of security policies and procedures in a security design.

Concept 2 - Risk Assessment: Identifying and predicting likely threats to the network through use of a threat model.

Concept 3 - Risk Management Planning: Discuss risk management planning and how to determine what resources in an organization requires protection and how to categorize them in order to assign an appropriate level of protection.

Concept 4 - Securing Physical Resources: Discuss how to secure facilities, computers, and hardware.

Concept 5 - Securing Computer Resources: Discuss how to determine threats and analyze risks to computers on your network.
Concept 6 – Security Accounts: Discuss the threats and risks to accounts in an organization and how to secure them.

Concept 7 – Authentication Security: Discuss the threats and risks to authentication and how to design a secure authentication plan.

Concept 8 – Data Security Design: Examine the threats and risks to data and design a plan to secure data resources.

Concept 9 - Design Security Data Transmission: Examine the threats and risks to data transmission and design a secure data transmission plan.

Concept 10 - Design Security for Network Perimeters: Examine the threats to the points where the network connects to other networks, such as the Internet, and how to secure network perimeters.

Concept 11 - Design an Incident Response Procedure: Provides information about auditing and creating procedures to direct how to respond to security incidents.

STUDENT LEARNING OUTCOMES

Student must demonstrate the following skills:

Concept 1 - Planning for Network Security:
Describe common elements of security policies and procedures.
Create a security framework using the Microsoft Solutions Framework (MSF) process model.

Concept 2 - Risk Assessment:
Explain common network vulnerabilities and describe how attackers can use these vulnerabilities.
Use the STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege) threat model to predict threats to security.

Concept 3 - Risk Management Planning:
Explain the purpose of risk management and how it operates.
Draft the elements of a risk management plan.

Concept 4 - Securing Physical Resources:
Identify the threats to physical resources.
Develop a security plan that adequately secures physical resources.

Concept 5 - Securing Computer Resources:
Identify the threats to computer resources.
Develop a security plan to secure computer resources.

Concept 6 – Security Accounts:
Identify threats and risks to accounts.
Develop a security plan to secure an organization’s accounts.

Concept 7 – Authentication Security:
Identify the threats and risks to authentication.
Develop a secure authentication plan.

Concept 8 – Data Security Design:
Identify the threats and risks to data.
Develop a plan to secure data resources.
Concept 9 - Securing Data Transmission:
Identify threats to transmitting data.
Develop a plan to secure data during transmission.

Concept 10 – Securing the Network Perimeters:
Identify threats and risks to the network from other networks or the Internet.
Develop a design that secures network perimeters from identified threats and risks.

Concept 11 - Designing an Incident Response Procedure:
Explain the importance of auditing and incident response.
Design an auditing policy.
Identity key elements of an incident response plan.
Design an incident response procedure.