Miami Dade College

Course Description

CTS2310 | Design, Implement, Manage Network Security | 4.00 credits

This course provides the information and skills necessary to design, implement, manage, maintain, and troubleshoot security in a Microsoft Windows Server network infrastructure. It is intended for students preparing to be IT systems engineers and security specialists who are responsible for implementing and managing security policies and procedures for an organization. Prepares students for the MCSE Security specialization. Pre/ corequisite: CTS 2306; may be waived for individuals with current MCSA certification or equivalent experience.

Course Competencies

Competency 1: The student will demonstrate an understanding of the ability to analyze business and technical requirements for designing security by:

1. Analyzing existing policies and procedures, sensitivity of data, cost, legal requirements, end-user impact, interoperability, scalability and risk.
2. Designing a framework for security design and implementation, including prevention, detection, isolation, and recovery.
3. Analyzing technical constraints when designing security.

Competency 2: The student will demonstrate an understanding of the ethical use of computers and networks in the design, implementation, and managing of networks by:

1. Formulating how to implement an acceptable use policy.
2. Designing methods to safeguard and prevent the infringement of intellectual property rights.
3. Planning network infrastructure to preserve privacy.
4. Describing measures to prevent the illegal uses of computer.

Competency 3: The student will demonstrate an understanding of current best practices and tools for creating the logical design for network infrastructure security by:

1. Designing a public key infrastructure (PKI) using Certificate Services.
2. Designing a logical authentication strategy.
3. Designing security for network management using current best practices and tools to manage the risk of network management.
4. Designing a security update infrastructure.

Competency 4: The student will demonstrate an understanding of current best practices and tools for creating the physical design for network and client infrastructure security by:

1. Designing security for perimeter, transmission, and name resolution services.
2. Designing authentication and transmission security for public and private wireless LANS.
3. Designing security for Internet Information Services (IIS) including user authentication, minimizing attack surfaces, monitoring, and content management.
4. Designing security for communication between networks using VPN (Virtual Private Network).
5. Designing security for extranet communications.
6. Defining role-based server baseline security templates and plans to manage change to these templates.
7. Designing a client authentication strategy, including account and password security requirements.

8. Designing a security strategy for client remote access, including remote access policies and authentication and auditing using RADIUS.
9. Designing a strategy for securing client computers, including hardening the operating system (OS) and restricting user access to OS feature.

Competency 5: The student will demonstrate an understanding of current best practices and tools for designing an access control strategy for data by:

1. Designing an access control strategy for directory services, including strategies for delegation, auditing, groups and permission structures.
2. Designing an access control strategy for files and folders, including strategies for encryption, permissions, backup and recovery and auditing requirements.
3. Designing an access control strategy for the registry, including permissions and auditing requirements.

Competency 6: The student will demonstrate an understanding of current best practices and tools for implementing and managing and troubleshooting security policies by:

1. Planning security templates based on computer role.
2. Configuring, deploying, and troubleshooting security templates.

Competency 7: The student will demonstrate an understanding of current best practices and tools for implementing, managing and troubleshooting Patch Management by:

1. Planning the deployment of service packs and hot fixes, including applicationcompatibility testing, planning batch deployments and creating a rollback strategy.
2. Assessing the current status of service packs and hot fixes.
3. Deploying service packs and hot fixes on new and existing servers and clientcomputers.

Competency 8: The student will demonstrate an understanding of current best practices and tools for implementing, managing and troubleshooting network communications security by:

1. Planning IP Security (IPSec) deployment.
2. Configuring IPSec policies to secure communication between networks and hosts, including special considerations for server roles.
3. Deploying, managing, and troubleshooting IPSec policies.
4. Planning and implementing security for wireless networks, including encryption and authentication methods, policies and software for wireless client support.
5. Deploying, managing, and configuring Secure Sockets Layer (SSL) certificates for network transmission security.
6. Configuring security for remote access users, including authentication methods, VPN protocols, and standardizing client configuration for remote access.

Competency 9: The student will demonstrate an understanding of current best practices and tools for planning, configuring and troubleshooting authentication, authorization, and Public Key Infrastructure by:

1. Planning and configuring authentication.
2. Planning group structure.
3. Planning and configuring authorization through access control lists and user rights Assignment.
4. Planning requirements for digital signatures.
5. Installing, managing, and configuring certificate services, including installation and management of certificate authorities (CAs), template configuration, revocation lists, archival and recovery of keys, backup and restoration of CAs.

Learning Outcomes:

1. Critical Thinking
2. Ethical Issues
3. Social Responsibility