



# Broward Community College

## Course Outline

Status: A

COMMON COURSE NUMBER: CTS2310C

COURSE TITLE: Designing a Secure Microsoft Windows Network

CREDIT HOURS: 4

### CONTACT HOURS BREAKDOWN:

Lecture/Discussion 56

Lab 8

Other 0

Contact Hours/Week 4

### CATALOG COURSE DESCRIPTION:

This course provides students with the knowledge and skills necessary to design a security framework for small, medium, and enterprise networks by using Microsoft's Windows technologies. The skills developed by students completing this course will help prepare them for the Microsoft Designing a Secure Windows Network certification exam.

Prerequisite(s): CEN1300C, CEN1301C, CEN1315C, CEN1321C

Corequisite(s): None

### UNIT TITLES:

1. Assessing Security Risks
2. Introducing Windows Security
3. Planning Administrative Access
4. Planning User Accounts
5. Securing Windows-Based Computers
6. Securing File and Print Resources
7. Securing Communication Channels
8. Providing Secure Access to Non-Microsoft Clients
9. Providing Secure Access to Remote Users
10. Providing Secure Access to Remote Offices

11. Providing Secure Network Access to Internet Users
12. Providing Secure Internet Access to Network Users
13. Extending the Network to Partner Organizations
14. Designing a Public Key Infrastructure
15. Developing a Security Plan

## **I. Course Overview:**

After completing this course, students will be able to identify the security risks associated with managing resource access and data flow on the network; describe how key technologies within Windows are used to secure a network and its resources; plan a Windows administrative structure so that permissions are granted only to appropriate users; plan an Active Directory service structure that facilitates secure and verifiable user account creation and administration; define minimum security requirements for Windows-based domain controllers, application servers, file and print servers, and workstations; design a strategy for securing local storage of data and providing secure network access to file and printer resources; design end-to-end security for the transmission of data between hosts on the network; design a strategy for securing access for non-Microsoft clients within a Windows 2000-based network; design a strategy for securing local resources accessed by remote users who use dial-up or virtual private network (VPN) technologies; design a strategy for securing local resources accessed by remote offices within a wide area network (WAN) environment; protect private network resources from public network users; design a strategy for securing private network user access to public networks; design a strategy for authenticating trusted users over public networks; design a strategy for securing data and application access for the private network when accessed by trusted partners; plan for an e-commerce implementation between your organization and external business partners that facilitates business communication; and design a structured methodology for securing a Windows 2000 network.

## **II. Units:**

### **Unit 1: Assessing Security Risks**

#### General Outcome:

1.0 The students should be able to network security.

#### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

- 1.1 Describe the potential risks to different types of stored data.
- 1.2 Describe the potential risks from a denial of service.
- 1.3 Describe potential threats against network security.
- 1.4 Describe common industry standards for measuring network security.
- 1.5 Discuss methodologies for securing a Windows 2000 network.

## Unit 2: Introducing Windows Security

### General Outcome:

2.0 The students should be able to Active Directory's security features.

### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

- 2.1 Describe how security features in Active Directory provide a framework for designing a secure Windows network.
- 2.2 Describe the authentication methods that Windows provides for user and computer accounts.
- 2.3 Identify the methods that can be used to secure resource access in Windows 2000 networks.
- 2.4 Identify the encryption technologies that Windows 2000 supports.
- 2.5 Describe how encryption technologies are used to secure stored and transmitted data in a Windows 2000 network.
- 2.6 Describe how a Public Key Infrastructure (PKI) can be used to create a secure network.

### **Unit 3: Planning Administrative Access**

#### General Outcome:

3.0 The students should be able to administer access planning.

#### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

- 3.1 Select an administrative model for an organization.
- 3.2 Plan memberships in Windows administrative groups.
- 3.3 Plan secure local administrative access to the network.
- 3.4 Plan secure remote administrative access to the network.

## Unit 4: Planning User Accounts

### General Outcome:

4.0 The students should be able to plan user accounts.

### Specific Learning Outcomes:

Upon successful completion of this unit, the students will be able to:

- 4.1 Design an account policy and Group Policy strategy for user accounts.
- 4.2 Plan for the creation and location of user accounts within the domain and organizational unit (OU) structure.
- 4.3 Plan delegation of authority to user accounts.
- 4.4 Design an audit strategy that will track changes made to objects in Active Directory.

## Unit 5: Securing Windows-Based Computers

### General Outcome:

5.0 This unit introduces students to the processes of planning and deploying secure Windows-based computers.

### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

- 5.1 Plan physical measures to secure Windows-based Computers.
- 5.2 Evaluate the security requirements for Windows 2000-based computers with respect to their roles in the network.
- 5.3 Design security configuration templates to enforce security settings.
- 5.4 Evaluate the existing security configuration of a Windows-based computer.
- 5.5 Determine how to deploy security templates in a Windows network.

## Unit 6: Securing File and Print Resources

### General Outcome:

6.0 The students should be able to design a secure file and print resources.

### Specific Learning Outcomes:

Upon successful completion of this unit, students will be able to:

- 6.1 Describe the security provided in the file systems supported by Windows.
- 6.2 Design a security strategy for protecting data such as files, folders, print resources, and the registry by using discretionary access control lists (DACLS).
- 6.3 Design a strategy for the protection and recovery of file resources encrypted with Encrypting File System (EPS).
- 6.4 Design an audit strategy to monitor file and print resource access.
- 6.5 Design a secure backup and restore procedure that allows for disaster recovery.
- 6.6 Plan for virus protection in a network security design.

## Unit 7: Securing Communication Channels

### General Outcome:

7.0 The students should be able to secure communication channels.

### Specific Learning Outcomes:

Upon successful completion of this unit, students will be able to:

- 7.1 Assess potential risks to transmitted data on the network wire in the local area network (LAN).
- 7.2 Design a strategy for providing authentication and data privacy by applying security at the application layer.
- 7.3 Design a strategy for providing authentication and data privacy by applying security at the Internet Protocol (IP) layer.
- 7.4 Design an Internet Protocol Security (IPSec) strategy for encrypting private network data transmissions.

## **Unit 8: Providing Secure Access to Non-Microsoft Clients**

### General Outcome:

8.0 The students should be able to provide secure access to non-Microsoft clients.

### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

- 8.1 Identify the risks associated with allowing UNIX clients access to a Windows network.
- 8.2 Identify the risks associated with allowing NetWare clients access to a Windows network.
- 8.3 Identify the risks associated with allowing Macintosh clients access to a Windows network.
- 8.4 Secure common network services that are operating in a heterogeneous network.
- 8.5 Monitor a heterogeneous network for security breaches and identify the risks of unauthorized network monitoring.

## **Unit 9: Providing Secure Access to Remote Users**

### General Outcome:

9.0 The students should be able to provide secure access to remote users.

### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

- 9.1 Identify the risks associated with providing network access to remote users.
- 9.2 Design a secure network for remote users who access the network by using dial-up connections.
- 9.3 Design a secure network for remote users who access the network by using VPN connections.
- 9.4 Design a secure network for remote users by centralizing the security configuration of remote access servers.

## Unit 10: Providing Secure Access to Remote Offices

### General Outcome:

10.0 The students should be able to provide secure access to remote offices.

### Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

10.1 Describe the difference between a private network and a public network.

10.2 Plan a secure connection between two remote networks by using a VPN.

10.3 Plan a secure connection between two remote networks by using a VPN.

10.4 Identify the security requirements that must be considered while planning secure connections between remote offices.

## **Unit 11: Providing Secure Network Access to Internet users**

### General Outcome:

11.0 This unit introduces students to Internet security issues.

### Specific Learning Outcomes:

Upon successful completion of this unit, students will be able to:

11.1 Analyze the potential threats that are introduced when a private network is connected to the Internet.

11.2 Design a firewall strategy for protecting private network resources.

11.3 Design a secure method for exposing private network resources to the internet.

11.4 Plan to secure public access to a screened subnet.

## Unit 12: Providing Secure Internet Access to Network Users

### General Outcome:

12.0 This unit introduces students to Internet-user security issues.

### Specific Learning Outcomes:

Upon successful completion of this unit, students will be able to:

12.1 Design a strategy for protecting private network resources from the public network.

12.2 Plan which users, computers, and protocols are allowed access to the Internet.

12.3 Design the Microsoft Proxy Server settings for maintaining security when local network users access the Internet.

12.4 Design the client-side requirements for maintaining security when local network users access the Internet.

## Unit 13: Extending the Network to Partner Organizations

### General Outcome:

13.0 The students should be able to extend the network to "partner" security issues.

### Specific Learning Outcomes:

Upon successful completion of this unit, students will be able to:

- 13.1 Describe the connection methods that can be used to provide access to partner organizations.
- 13.2 Describe the ways to provide secure access to data, applications, and communications shared with trusted partners.
- 13.3 Design a secure framework that allows partners to use tunnel connections, dial-up connections, and Terminal Services to access the private network.
- 13.4 Design an Active Directory service structure for partners.
- 13.5 Design a secure framework for authenticating partners from trusted domains.

## Unit 14: Designing a Public Key Infrastructure

### General Outcome:

14.0 The students should be able to design a public key infrastructure.

### Specific Learning Outcomes:

Upon successful completion of this unit, students will be able to:

- 14.1 Describe the basic components of PKI.
- 14.2 Define how certificates can be used in a PKI to certify applications and services.
- 14.3 Define the basic functions of certificates within a certificate life cycle.
- 14.4 Choose between public and private certification authorities (CAs).
- 14.5 Plan a hierarchy for organizing CAs in a network.
- 14.6 Use certificate mapping to apply user permissions to users who are not included in your organization's Active Directory service.
- 14.7 Plan recovery and maintenance strategies for CAs.

**Unit 15: Developing a Security Plan**

General Outcome:

15.0 The students should be able to develop a security plan.

Specific Learning Outcomes:

Upon successful completion of this unit, the students should be able to:

15.1 Design a security plan that will meet the security requirements of an organization.

15.2 Define the security requirements for local and remote networks, public and private networks, and trusted business partners.

15.3 Develop strategies to maintain the network security plan.