



BROWARD COMMUNITY COLLEGE

COURSE OUTLINE

LAST REVIEW: 2006-2007
(i.e. 2003-2004)

NEXT REVIEW: 2010-2011
(i.e. 2008-2009)

STATUS: A
(A, I, D)

COURSE TITLE: Implementing and Administering Security in a Microsoft Windows Server Network

COMMON COURSE NUMBER: CTS2326C

CREDIT HOURS: 4

CONTACT HOUR BREAKDOWN

(per 16 week term)

CLOCK HOURS: 0
(Voc. Course ONLY)

Lecture: **56** Lab: **8**

Clinic: **0** Other: **0**

PREREQUISITE(S): CEN1321C

COREQUISITE(S):

PRE/COREQUISITE(S):

COURSE DESCRIPTION: *(600 characters, maximum)*

This course is part of the Security Portfolio and will act as the primary entry point for IT Professionals at the implementation level and is for system administrators or system engineers who have the foundation implementation skills and knowledge for the deployment of secure Microsoft Windows Server based solutions. This course is not intended to provide design skills, but will cover planning skills at a level sufficient to enable decision making for the implementation process.

UNIT TITLES

1. Plan and configure an authorization and authentication strategy in a multi-forest organization.
2. Install, configure, and manage a certification authority (CA).
3. Configure, deploy, and manage certificates.
4. Plan, implement, and troubleshoot smart card certificates.
5. Plan, implement, and troubleshoot Encrypting File System (EFS).
6. Plan, configure, and deploy a secure member server baseline.
7. Plan, configure, and implement secure baselines for server roles.
8. Plan, configure, implement, and deploy a secure client computer baseline.
9. Plan and implement Software Update Services.
10. Plan, implement, and troubleshoot data transmission security.
11. Plan and implement security for wireless networks.
12. Plan and implement perimeter security with Internet Security and Acceleration Server (ISA) 2000.
13. Secure remote access.



BROWARD COMMUNITY COLLEGE

COURSE OUTLINE

Common Course Number: CTS2326C

UNITS

Unit 1 Plan and configure an authorization and authentication strategy in a multi-forest organization.

General Outcome:

1.0 The student shall:

- Identify Components of an Authentication Model
- Plan and Implement an Authentication Strategy
- Create Groups and Basic Group Strategy in Windows Server
- Create Trusts in Windows Server
- Plan, Implement, and Maintain an Authorization Strategy Using Groups
- Plan and Configure an Authentication and Authorization Strategy
- Plan and Implement a Resource Authorization Strategy
- Plan and Implement a Cross-Forest Authentication Strategy
- Plan and Implement an Authentication Policy

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 1.1 Describe the components, tools, and protocols that support authentication.
- 1.2 Plan and implement an authentication strategy in a multi-forest organization.
- 1.3 Determine the necessary group structure for a multi-domain or multi-forest environment.
- 1.4 Create trusts in a Windows Server environment.
- 1.5 Plan, implement, and maintain an authorization strategy in a multi-forest organization.



BROWARD COMMUNITY COLLEGE

COURSE OUTLINE

Common Course Number: CTS2326C

Unit 2 Install, configure and manage a certification authority (CA).

General Outcome:

2.0 The student shall:

- Have an Overview of a PKI
- Be Introduced to Certification Authorities
- Install a Certification Authority
- Manage a Certification Authority
- Back Up and Restore a Certification Authority
- Install and Configure a Certification Authority
- Install an Enterprise Subordinate Certification Authority
- Back up a Certification Authority

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 2.1** Describe a PKI.
- 2.2** Describe the applications and components that are used in a PKI.
- 2.3** Install a certification authority.
- 2.4** Create and publish Certificate Revocation Lists (CRLs) and Authority Information Access (AIA) distribution points.
- 2.5** Back up and restore a certification authority.



Common Course Number: CTS2326C

Unit 3 Configure, deploy and manage certificates.

General Outcome:

3.0 The student shall:

- Have an Overview of Digital Certificates
- Deploy and Revoke User and Computer Certificates
- Configure Certificate Templates
- Manage Certificates
- Deploy and Manage Certificates
- Configure Multipurpose Certificate Templates
- Configure Certificate Auto-enrollment
- Update a Certificate Template
- Implement a Key Archiving Strategy

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 3.1** Configure certificate templates in a Microsoft Windows Server PKI environment.
- 3.2** Deploy, enroll, and revoke certificates in a Windows Server PKI environment.
- 3.3** Describe the applications and components that are used in a PKI.
- 3.4** Export, import, and archive certificates and keys in a Windows Server PKI environment.



Common Course Number: CTS2326C

Unit 4 Plan, implement and troubleshoot smart card certificates.

General Outcome:

4.0 The student shall:

- Be Introduced to Multifactor Authentication
- Plan and Implement a Smart Card Infrastructure
- Manage and Troubleshoot a Smart Card Infrastructure
- Implement Smart Cards
- Configure a Smart Card Enrollment Station
- Enroll Users for Smart Cards

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 4.1** Describe the concepts of and applications for multifactor authentication.
- 4.2** Plan and implement a smart card infrastructure.
- 4.3** Manage and troubleshoot a smart card infrastructure.



Common Course Number: CTS2326C

Unit 5 Plan, implement and troubleshoot Encrypting File System (EFS).

General Outcome:

5.0 The student shall:

- Be Introduced to EFS
- Implement EFS in a Standalone Microsoft Windows XP Environment
- Plan and Implement EFS in a Domain Environment
- Implement EFS File Sharing
- Troubleshoot EFS
- Plan, Implement, and Troubleshoot Encrypted File System
- Implement Certificates to Support EFS
- Configure Group Policy to Support EFS

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 5.1** Describe EFS and how it works.
- 5.2** Implement EFS in a standalone Microsoft Windows Client environment.
- 5.3** Plan and implement EFS in a domain environment that has a PKI.
- 5.4** Implement EFS file sharing.
- 5.5** Troubleshoot EFS problems.



Common Course Number: CTS2326C

Unit 6 Plan, configure and deploy a secure member server baseline.

General Outcome:

6.0 The student shall:

- Have an Overview of a Member Server Baseline
- Plan a Secure Member Server Baseline
- Configure Additional Security Settings
- Deploy Security Templates
- Secure Servers by Using the Security Configuration Wizard
- Plan a Member Server Baseline
- Plan a Secure Member Server Baseline

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 6.1** Describe the components that make up a secure member server baseline.
- 6.2** Plan a secure member server baseline.
- 6.3** Configure additional security settings.
- 6.4** Deploy security templates.
- 6.5** Secure servers by using the Security Configuration Wizard (SCW)



Common Course Number: CTS2326C C

Unit 7 Plan, configure and implement secure baselines for server roles.

General Outcome:

7.0 The student shall:

- Plan and Configure a Secure Baseline for Domain Controllers
- Plan and Configure a Secure Baseline for DNS Servers
- Plan and Configure a Secure Baseline for Infrastructure Servers
- Plan a Secure Baseline for File and Print Servers
- Plan and Configure a Secure Baseline for IIS Servers

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 7.1** Plan and configure a secure baseline for domain controllers.
- 7.2** Plan and configure a secure baseline for Domain Name System (DNS) servers.
- 7.3** Plan and configure a secure baseline for infrastructure servers.
- 7.4** Plan a secure baseline for file and print servers.
- 7.5** Plan and configure a secure baseline for Internet Information Services (IIS) servers.



Common Course Number: CTS2326C

Unit 8 Plan, configure implement, and deploy a secure client computer baseline.

General Outcome:

8.0 The student shall:

- Plan and Implement a Secure Client Computer Baseline
- Secure Applications on Client Computers
- Plan and Implement a Software Restriction Policy
- Implement Security for Mobile Clients
- Plan, Implement, Configuring, and Deploying a Secure Client Computer Baseline
- Plan Security Templates for Client Computers
- Implement Security Templates for Client Computers

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 8.1** Plan a secure client computer baseline.
- 8.2** Secure applications on client computers.
- 8.3** Plan and implement a software restriction policy on client computers.
- 8.4** Implement security on mobile computers.



Common Course Number: CTS2326C

Unit 9 Plan and implement Software Update Services.

General Outcome:

9.0 The student shall:

- Be Introduced to Software Update Management
- Implement Microsoft Baseline Security Analyzer
- Install Windows Server Update Services
- Manage a WSUS Infrastructure
- Plan and Implementing Software Updates
- Configure MBSA Integration with WSUS Server

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 9.1** Describe the need for update management and the tools that you can use to implement update management strategies.
- 9.2** Implement MBSA.
- 9.3** Install WSUS.
- 9.4** Manage a WSUS infrastructure.



BROWARD COMMUNITY COLLEGE COURSE OUTLINE

Common Course Number: CTS2326C

Unit 10 Plan, implement and troubleshoot data transmission security.

General Outcome:

10.0 The student shall:

- Secure Data Transmission Methods
- Be Introduced IPsec
- Plan and Implement Data Transmission Security Using IPsec
- Troubleshoot IPsec Communications
- Implement and Troubleshoot Data Transmission Security
- Plan IPsec Security
- Implement IPsec Security

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 10.1** Describe various methods for securing data transmission.
- 10.2** Describe the purpose and function of IPsec.
- 10.3** Plan and implement data transmission security using IPsec.
- 10.4** Troubleshoot IPsec communication.



Common Course Number: CTS2326C

Unit 11 Plan and implement security for wireless networks.

General Outcome:

11.0 The student shall:

- Be Introduced to Securing Wireless Networks
- Implement 802.1x Authentication
- Plan a Secure WLAN Strategy
- Implement a Secure WLAN
- Troubleshoot Wireless Networks
- Plan and Implement Security for Wireless Networks
- Configure Active Directory for Wireless Networks
- Configure Certificate Templates and Certificate Autoenrollment
- Configure Remote Access Policies for Wireless Devices
- Configure Group Policy for Wireless Networks

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 11.1** Describe the components and features of a secure wireless LAN (WLAN) and a wireless infrastructure.
- 11.2** Plan a secure WLAN infrastructure.
- 11.3** Implement a secure WLAN infrastructure.
- 11.4** Troubleshoot WLAN errors and components.



BROWARD COMMUNITY COLLEGE COURSE OUTLINE

Common Course Number: CTS2326C

Unit 12 Plan and implement perimeter security with Internet Security and Acceleration Server (ISA) 2000.

General Outcome:

12.0 The student shall:

- Be Introduced to Internet Security and Acceleration Server
- Install and Managing ISA Server
- Secure a Perimeter Network by Using ISA Server
- Publish Servers on a Perimeter Network
- Plan a Perimeter Network
- Implement a Perimeter Network
- Secure an ISA Server Computer

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 12.1** Describe the ISA Server features.
- 12.2** Install and manage ISA Server.
- 12.3** Configure a perimeter network by using ISA Server.
- 12.4** Publish servers on a perimeter network by using ISA Server.



Common Course Number: CTS2326C

Unit 13 Secure remote access.

General Outcome:

13.0 The student shall:

- Be Introduced to Remote Access Technologies and Vulnerabilities
- Plan a Remote Access Strategy
- Deploy Network Access Quarantine Control Components
- Implement a Secure VPN Solution
- Configure a VPN Connection
- Configure the VPN Server for Remote Access Quarantine
- Configure a Connection Manager Service Profile

Specific Measurable Learning Outcomes:

Upon successful completion of this unit, the student shall be able to:

- 13.1** Describe the various remote access technologies used for remote access and the threats associated with remote access.
- 13.2** Plan a remote access strategy.
- 13.3** Implement and configure a virtual private network (VPN) server.
- 13.4** Deploy Network Access Quarantine Control components.