

SYLLABUS

DATE OF LAST REVIEW:	02/2013
CIP CODE:	11.0901
SEMESTER:	Departmental Syllabus
COURSE TITLE:	Operating System Security (Windows 2008 Server)
COURSE NUMBER:	CIST-0254
CREDIT HOURS:	4
INSTRUCTOR:	Departmental Syllabus
OFFICE LOCATION:	Departmental Syllabus
OFFICE HOURS:	Departmental Syllabus
TELEPHONE:	Departmental Syllabus
EMAIL:	Departmental Syllabus <i>KCKCC-issued email accounts are the official means for electronically communicating with our students.</i>
PREREQUISITES:	CIST-0161 System Manager (Windows 2008 Server)
REQUIRED TEXT AND MATERIALS:	Please check with the KCKCC bookstore, http://www.kckccbookstore.com for the required text for your particular class.
COURSE DESCRIPTION:	This course covers the design and manages security of a Microsoft 2008 Local Area Network and domains. Security includes: Controlling access to resources, Auditing access to resources, Authentication, and Encryption. Student will demonstrate practical knowledge and will prepare for the Microsoft Certification Exam.
METHOD OF INSTRUCTION:	A variety of instructional methods may be used depending on content area. These include but are not limited to: lecture, multimedia, cooperative/collaborative learning, labs and demonstrations, projects and presentations, speeches, debates, and panels, conferencing, performances, and learning experiences outside the classroom. Methodology will be selected to best meet student needs.

COURSE OUTLINE:

- I. Analyze factors that influence company strategies.
 - A. Identify company priorities.
 - B. Identify the projected growth and growth strategy
 - C. Identify relevant laws and regulations
 - D. Identify the company's tolerance for risk
 - E. Identify the total cost of operations

- II. Analyze the impact of the security design on the existing and planned technical environment
 - A. Assess existing systems and applications
 - B. Identify existing and planned upgrades and rollouts
 - C. Analyze technical support structure
 - D. Analyze existing and planned network and systems management
 - E. Analyzing Security Requirements

- III. Design a security baseline
 - A. Identify domain controllers, operations masters, application servers, file and print servers, RAS servers, desktop computers, and portable computers, and Internet access
 - B. Identify the required level of security for each resource

- IV. Designing a Windows 2008 Security Strategy
 - A. Design an Encrypting File System strategy
 - B. Design a security group strategy
 - C. Design a delegation of authority strategy
 - D. Design an authentication strategy
 - E. Design an authentication strategy for integration with other systems

- V. Design a Public Key Infrastructure
 - A. Design Certificate Authority (CA) hierarchies
 - B. Identify certificate server roles
 - C. Manage certificates
 - D. Integrate with third-party CAs
 - E. Map certificates

- VI. Design Windows 2008 network services security
 - A. Design DNS security
 - B. Design Remote Installation Services (RIS) security
 - C. Design SNMP security
 - D. Design Terminal Services security

- VII. Provide secure access between private networks
 - A. Provide secure access within a LAN
 - B. Provide secure access within a WAN
 - C. Provide secure access across a public network

- VIII. Design an IPSec solution
 - A. Design an IPSec encryption scheme
 - B. Design an IPSec management strategy
 - C. Design negotiation policies
 - D. Design security policies
 - E. Design IP filters

F. Define security levels

EXPECTED LEARNER OUTCOMES:

- A. Upon completion of the course the student will be able to demonstrate knowledge of Win2008 security, the structure of Win2008, and knowledge of file systems.
- B. Upon completion of the course the student will be able to analyze the existing and planned business models, business and security requirements for the end user, the structure of IT management, the internal and external security risks, and the company size and user and resource distribution..
- C. Upon completion of the course the student will be able to analyze the method of accessing data and systems, network roles and responsibilities, design a security baseline for a Windows 2008 network that includes domain controllers, identify the required level of security for each resource.
- D. Upon completion of the course the student will be able to design an audit policy, a delegation of authority strategy, security policies for sites, domains, and organizational units, an Encrypting File System strategy, an authentication strategy, and a security group strategy.
- E. Upon completion of the course the student will be able to identify certificate server roles, design Certificate Authority (CA) hierarchies, and manage certificates.
- F. Upon completion of the course the student will be able to design Windows 2008 DNS security, Remote Installation Services (RIS) security, SNMP security, Terminal Services security.
- G. Upon completion of the course the student will be able to design a Security Solution for Access between Networks, provide external users with secure access to private network resources, secure access within a LAN, and design Windows 2008 security for remote access users.
- H. Upon completion of the course the student will be able to design an IPSec encryption scheme, an IPSec management strategy, IP filters, and demonstrate an ability to meet deadline

COURSE COMPETENCIES:

Upon completion of the course the student will be able to demonstrate knowledge of Win2008 security, the structure of Win2008, and knowledge of file systems.

- 1. Student should be able to demonstrate knowledge of Win2008 security.
- 2. Student should be able to show the structure of Win2008.
- 3. Student should be able to have a working knowledge of file systems.

Upon completion of the course the student will be able to analyze the existing and planned business models, business and security requirements for the end user, the structure of IT management, the internal and external security risks, and the company size and user and resource distribution

- 4. Student should be able to analyze the existing and planned business models.
- 5. Student should be able to analyze business and security requirements for the end user.
- 6. Student should be able to analyze the structure of IT management.
- 7. Student should be able to analyze internal and external security risks.
- 8. Student should be able to analyze company size and user and resource distribution.

Upon completion of the course the student will be able to analyze the method of accessing data and systems, network roles and responsibilities, design a security baseline for a Windows 2008

network that includes domain controllers, identify the required level of security for each resource.

9. Student should be able to analyze the method of accessing data and systems.
10. Student should be able to analyze network roles and responsibilities. Roles include administrative, user, service, resource ownership, and application.
11. Student should be able to Design a security baseline for a Windows 2000 network that includes domain controllers.
12. Student should be able to identify the required level of security for each resource. Resources include printers, files, shares, Internet access, and dial-in access.

Upon completion of the course the student will be able to design an audit policy, a delegation of authority strategy, security policies for sites, domains, and organizational units, an Encrypting File System strategy, an authentication strategy, and a security group strategy.

13. Student should be able to design an audit policy.
14. Student should be able to design a delegation of authority strategy.
15. Student should be able to of security policies for sites, domains, and organizational units.
16. Student should be able to design an Encrypting File System strategy.
17. Student should be able to design an authentication strategy.
18. Student should be able to design a security group strategy.

Upon completion of the course the student will be able to identify certificate server roles, design Certificate Authority (CA) hierarchies, and manage certificates.

19. Student should be able to identify certificate server roles.
20. Student should be able to design Certificate Authority (CA) hierarchies.
21. Student should be able to manage certificates.

Upon completion of the course the student will be able to design Windows 2008 DNS security, Remote Installation Services (RIS) security, SNMP security, Terminal Services security.

22. Student should be able to design Windows 2008 DNS security.
23. Student should be able to design Windows 2008 Remote Installation Services (RIS) security.
24. Student should be able to design Windows 2008 SNMP security.
25. Student should be able to design Windows 2008 Terminal Services security.

Upon completion of the course the student will be able to design a Security Solution for Access between Networks, provide external users with secure access to private network resources, secure access within a LAN, and design Windows 2008 security for remote access users.

26. Student should be able to design a Security Solution for Access between Networks.
27. Student should be able to provide external users with secure access to private network resources.
28. Student should be able to provide secure access within a LAN.
29. Student should be able to design Windows 2000 security for remote access users.

Upon completion of the course the student will be able to design an IPSec encryption scheme, an IPSec management strategy, IP filters, and demonstrate an ability to meet deadline.

30. Student should be able to design an IPSec encryption scheme.
31. Student should be able to design an IPSec management strategy.
32. Student should be able to design IP filters.
33. The student will demonstrate an ability to meet deadline.

**ASSESSMENT OF LEARNER
OUTCOMES:**

Student progress is evaluated by means that include, but are not limited to, exams, written assignments, and class participation.

SPECIAL NOTES:

This syllabus is subject to change at the discretion of the instructor. Material included is intended to provide an outline of the course and rules that the instructor will adhere to in evaluating the student's progress. However, this syllabus is not intended to be a legal contract. Questions regarding the syllabus are welcome any time.

Kansas City Kansas Community College is committed to an appreciation of diversity with respect for the differences among the diverse groups comprising our students, faculty, and staff that is free of bigotry and discrimination. Kansas City Kansas Community College is committed to providing a multicultural education and environment that reflects and respects diversity and that seeks to increase understanding.

Kansas City Kansas Community College offers equal educational opportunity to all students as well as serving as an equal opportunity employer for all personnel. Various laws, including Title IX of the Educational Amendments of 1972, require the college's policy on non-discrimination be administered without regard to race, color, age, sex, religion, national origin, physical handicap, or veteran status and that such policy be made known.

Kansas City Kansas Community College complies with the Americans with Disabilities Act. If you need accommodations due to a documented disability, please contact the Director of the Academic Resource Center, in Rm. 3354 or call at: 288-7670.

All enrolled students at Kansas City Kansas Community College are subject to follow all rules, conditions, policies and procedures as described in both the Student Code of Conduct as well as the Student Handbook. All Students are expected to review both of these documents and to understand their responsibilities with regard to academic conduct and policies. The Student Code of Conduct and the Student Handbook can be found on the KCKCC website.