

CSST 1340- System Administration and Virtualization

Sul Ross State University

Instructor: Thea Glenn

Office Location: ACR 109-B

Office Phone: 432-837- 8490

Text: 931-237-3324 (No text after 11pm or before 10am)

Email: tglenn2@sulross.edu

Office Hours: TBA

Class: 8:00 – 9:15 am Tuesday and Thursdays

Required Materials:

Textbook: the instructor will provide Textbook, labs, and workbooks.

Videos:

Ten things administrators should never do!

<https://www.youtube.com/watch?v=FzKSlsOgt5Q>

5 Windows System Tools You Must Have

<https://www.youtube.com/watch?v=tXu3isGqHNk>

Tutorial – 11 must know Command Prompt (CMD)

<https://www.youtube.com/watch?v=2Ey6VN7nqkA&index=4&list=PLfKydYnyblHe6RGOfocgkDyf07f9ifOI4>

Networking Command Line Tools

<https://www.youtube.com/watch?v=nH85pddWWAk>

Computer Science Program Learning Objectives

1. Understand the fundamental concepts of computer science including algorithms and data structures.
2. Understand modern computer systems, databases, and networking.
3. Display an understanding and ability to implement current programming methodologies.
4. Become proficient with system design based on object-oriented programming.
5. Work as a team in workgroup environments.

Course Description:

This course provides students with an understanding of the roles of an operating system, its basic functions, the services provided by the operating system, the skill to perform basic operations involved in system administration by utilizing virtualization technologies. It includes installation and secure configuration of a system, password policies, updates and patches, backups, and port security.

Course Objectives

After completing this course the students will be able to:

- Explain information security and how it applies to the Microsoft Windows operating systems.
- Explain security features of the Microsoft Windows operating systems.
- Implement secure access controls when setting up Microsoft Windows in a given organization.
- Set up encryption in a given organization to secure Windows environment.
- Install controls to protect a given Windows system from malware.
- Define and apply Group Policy controls in Microsoft Windows.
- Explain profile and audit tools to keep Windows systems secure.
- Perform backup and restore operations on a given Windows system.
- Design techniques to protect Windows networks from security vulnerabilities.
- Develop a security administration framework to ensure your organization meets its security policy goals.
- Identify and implement the most effective security controls to make computers and networks as secure as possible.
- Design techniques to protect given Windows application software from security vulnerabilities.
- Apply best practices for handling a given Microsoft Windows system and application incident.
- Include security concerns as early as possible in the software development process.
- Apply best practices to securing Microsoft Windows computers, networks, and applications.

Attendance:

Attendance Policy: Students are expected to attend every class. If class must be missed, the student is expected to get the notes from a classmate, and to check with me or on Blackboard

for announcements and updated assignments.

Students are expected to arrive to class on time. If a student is perpetually late, they will be asked to not attend class unless they can arrive on time. If tardiness becomes a problem for the class as a whole, people who arrive late will not be permitted to enter the class. If this stricter policy becomes necessary, there will be an announcement made in class.

It is policy of the university to drop a student with a grade of "F" if 9 hours or more of class are missed. For this course that would be 9 or more class sessions missed. For online courses student must log into blackboard within 3 weeks or will be withdrawn from the course with the grade of an "F"

Need for Assistance

Qualified students with disabilities needing academic or other accommodations to ensure full participation in the programs, services and activities at Sul Ross State University should contact the Disabilities Services Coordinator, in Counseling and Prevention Services, Ferguson Hall 112, Box C-117, Alpine, Texas 79832. Please notify me before the third day of classes.

Course Policies

Quizzes and assignments must be submitted on time. I have set up rules in BlackBoard so that assignments cannot be submitted after the due date.

Academic Dishonesty: Honesty in completing assignments is essential to the mission of the university and to the development of the personal integrity of the student. Cheating, plagiarism, or other kinds of academic dishonesty will not be tolerated and will result in appropriate sanctions that may include failing an assignment, failing the class, or being suspended or expelled. Suspected cases in this course may be reported to Student Life.

Posting of Grades

As soon as assignments, exams, and quizzes are graded, the grades will be posted in Blackboard.

Grading

Letter grades will be determined using a standard percentage point evaluation as outlined below. Please note that this is a tentative schedule and can change. Information pertaining to grades or changes to the schedule will be posted in Black Board via announcements.

Final grades will be determined by the following criteria:

Assignments	30%
Labs	30%
Group Presentation	40%

Each activity uses the following grade scale:

A	90 - 100 points
B	80 - 89 points
C	70 – 79 points
D	60 – 69 points
F	Below 60 points

The table following is a tentative schedule of the planned assignments. The legend for assignments is below the table:

Grading Category	Activity Title
<i>Lesson 1: Microsoft Windows and the Threat Landscape</i>	
Required Readings	Chapter 1, “Microsoft Windows and the Threat Landscape”
Lab	Virtualization Management
<i>Lesson 2: Security in the Microsoft Windows Operating System</i>	
Required Readings	Chapter 2, “Security in the Microsoft Windows Operating System”
Assignment	Enabling Remote Access
Assignment	Remote Access Policy Executive Summary Report
Lab	Implementing Access Controls with Windows Active Directory
<i>Lesson 3: Access Controls in Microsoft Windows</i>	
Required Readings	Chapter 3, “Access Controls in Microsoft Windows”
Assignment	Adding Active Directory
Assignment	Active Directory Executive Summary Report
Lab	Using Access Control Lists to Modify File System Permissions on Windows Systems
<i>Lesson 4: Microsoft Windows Encryption Tools and Technologies</i>	
Required Readings	Chapter 4, “Microsoft Windows Encryption Tools and Technologies”

Grading Category	Activity Title
Assignment	Recommendations for Access Controls
Assignment	Access Controls Procedure Guide
Lab	Configuring BitLocker and Windows Encryption
Required Readings	Chapter 5, "Protecting Microsoft Windows Against Malware"
Assignment	Encryption and BitLocker Activity
Assignment	Communication Policy Procedure Guide
Lab	Identifying and Removing Malware from Windows Systems
<i>Lesson 6: Group Policy Control in Microsoft Windows</i>	
Required Readings	Chapter 6, "Group Policy Control in Microsoft Windows"
Assignment	Identifying Types of Malware Infection
Assignment	Malware Policy Procedure Guide
<i>Lesson 7: Microsoft Windows Security Profile and Audit Tools</i>	
Required Readings	Chapter 7, "Microsoft Windows Security Profile and Audit Tools"
Lab	Managing Group Policy Objects Within the Microsoft Windows Environment
Assignment	Group Policy Objects List
<i>Lesson 8: Microsoft Windows Backup and Recovery Tools</i>	
Required Readings	Chapter 8, "Microsoft Windows Backup and Recovery Tools"
Discussion	Minimizing Recovery Time Strategies
Assignment	Auditing Tools for Windows Systems
Assignment	Security Audit Procedure Guide
Lab	Creating a Scheduled Backup and Replicating System Folders
<i>Lesson 9: Microsoft Windows Network Security</i>	
Required Readings	Chapter 9, "Microsoft Windows Network Security"
Assignment	Procedure Guide on Restoring a System
Required Readings	Chapter 10, "Microsoft Windows Security Administration"

Grading Category	Activity Title
Assignment	Network Security Requirements Policy
Assignment	Network Security Controls
<i>Lesson 11: Hardening the Microsoft Windows Operating System</i>	
Required Readings	Chapter 11, “Hardening the Microsoft Windows Operating System”
Assignment	Security Administration Using the Plan-Do-Check-Act (PDCA) Cycle
Lab	Securing Servers with the Security Configuration Wizard and Windows Firewall
<i>Lesson 12: Microsoft Application Security</i>	
Required Readings	Chapter 12, “Microsoft Application Security”
Assignment	Hardening Windows Authentication, Networking, and Data Access
Lab	Securing Internet Client and Server Applications on Windows Systems
<i>Lesson 13: Microsoft Windows Incident Handling and Management</i>	
Required Readings	Chapter 13, “Microsoft Windows Incident Handling and Management”
Assignment	Policy for Securing the Windows Environment
Assignment	Best Procedures to Secure Windows Applications
Lab	Protecting Digital Evidence, Documentation, and the Chain of Custody
<i>Lesson 14: Microsoft Windows and the Security Life Cycle</i>	
Required Readings	Chapter 14, “Microsoft Windows and the Security Life Cycle”
Discussion	Best Practices in Managing Changes to Windows Systems and Applications
Assignment	Evidence Collection Policy
Assignment	Windows Incident Handling Tools
<i>Lesson 15: Best Practices for Microsoft Windows and Application Security</i>	

Grading Category	Activity Title
Required Readings	Chapter 15, “Best Practices for Microsoft Windows and Application Security”
Assignment	Software Development Management Policies
Lab	Hardening Windows Server Security Using Microsoft Baseline Security Analyzer
Final	Group Presentation