Sul Ross State University

Spring 2017

CSST 4372 Intrusion Detection and Preventive Systems

Instructor: Thea Glenn
M.S. Management Information Systems

Office Location: ACR 109-B **Office Phone**: 432-837- 8490

TEXT #: 931-237-3324 (No text after 11pm or before 10am on **weekends** and **holidays**)

Email: tglenn2@sulross.edu **Office Hours:** 9am – 1pm
F

Class: MAB 204 **Class Time:** TR 3:30 – 4:45

Text: Special Publication (NIST SP) - 800-94, 2007. Guide to Intrusion Detection and Prevention Systems, (IDPS). NIST Pubs
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-94.pdf

Course Objectives
This course provides students with knowledge and skills related to detecting and analyzing vulnerabilities and threats and taking steps to mitigate associated risks. It addresses deep packet inspection, log file analysis, cross log comparison and analysis, host or network based intrusion detection, honeynets and honeypots.Specific topic coverage includes the following (time permitting):

- Security capabilities, including information gathering, logging, detection, and prevention
- Performance, including maximum capacity and performance features
- Management, including design and implementation (e.g., reliability, interoperability, scalability, product security), operation and maintenance (including software updates), and training, documentation, and technical support
- Life cycle costs, both initial and maintenance costs.

Attendance
Attendance is different for an independent study. We will meet every so often so that I will make sure you understand the material and answer any questions you have. Please email me your questions. That way I will answer your question as clearly as possible.

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** (also means taking information off line and using it as your own content), 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. Please note that information online is not free even though there is public access to the information. When using online resources you must properly cite your reference in the paper as well as on the reference page.

Posting of Grades
Grades are on display in blackboard. Submitting assignments and test are done in blackboard. **Do not** email assignments or test to me everything is to be put into 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. Any changes that happen will be updated in Blackboard. Due Dates for assignments will also be posted in Blackboard.

Your final grade will be determined by calculating points based on the following weights:

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

The following is a tentative schedule and is subject to change

Week	Topics	Chapter Readings	Exams
1	Introduction	Chapter 1	
2	Intrusion Detection and Prevention Principles	Chapter 2	
3	IDPS Technologies	Chapter 3	
4	Network-Based IDPS	Chapter 4	
5	Wireless IDPS	Chapter 5	
6	Network Behavior Analysis (NBA) System	Chapter 6	
7	Host-Based IDPS	Chapter 7	
8	Using and Integrating Multiple IDPS Technologies	Chapter 8	
9	IDPS Product Selection	Chapter 9	
10	Firewall Design and Management	Chapter 10	
11	Appendix A	Chapter 11	

12	Appendix B	Chapter 12	
13	Appendix C	Chapter 13	
14	Appendix D	Chapter 14	Final Exam