CSA 4372 – Intrusion Detection / Prevention Systems

Department of Computer Science

Semester Year (Spring 2026)

Faculty Information

Dr. Mainuddin Shaik
Email: Mainuddin.shaik@sulross.edu
Office Hours: Mondays & Wednesdays, 2:00 PM - 4:00 PM (via Teams or by appointment)

Course Description

This course examines the principles and practices of intrusion detection and prevention in modern computer networks and systems. Students study methods for identifying, analyzing, and responding to security threats using host-based and network-based detection techniques. Topics include attack models, logging and monitoring, signature-based and anomaly-based detection, deep packet inspection, alert analysis, and incident response. Emphasis is placed on conceptual understanding, system-level reasoning, and applied analysis rather than tool certification.

Course Materials

Required Textbook: None

Recommended Resources:

- Selected textbook chapters, and online readings provided by the instructor
- Supplemental materials may be posted on the course learning management system

Important Dates

- Jan 14 – First Day of Class (Introductions & course overview only)
- Jan 20 – Regular instruction begins (Week 2)
- Mar 9–13 – Spring Break (No class)
- Mar 16 – Mid-Semester (Midterm Project Part I due)
- Apr 29 – Last day to submit all coursework & Final Project due
- Apr 30 – Dead Day (No class; reserved for grading and feedback)

Program Student Learning Outcomes

Upon completion of this course, students will be able to:

- Explain fundamental concepts of intrusion detection and prevention systems
- Analyze cyber threats and attack patterns in networked environments
- Evaluate detection strategies for effectiveness and limitations
- Recognize ethical, legal, and privacy considerations in monitoring systems
- Apply system-level thinking to cybersecurity defense scenarios

Course Student Learning Outcomes

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

- Distinguish between host-based and network-based intrusion detection systems
- Explain signature-based and anomaly-based detection techniques
- Analyze logs, alerts, and traffic data to identify security incidents
- Evaluate trade-offs among detection accuracy, performance, and false positives
- Design a conceptual intrusion detection/prevention strategy for a given environment

Marketable Skills

Students completing this course will develop:

- Cybersecurity Analysis Skills – Understanding how intrusions occur and are detected
- Threat Modeling & Reasoning – Identifying attack vectors and defense strategies
- Security Monitoring Literacy – Interpreting logs, alerts, and detection outputs
- Risk & Trade-off Analysis – Balancing security, performance, and privacy
- Technical Communication – Explaining security findings and recommendations clearly

Course Assignments and Grading

Assignment Type	% of Final Grade	Description
Homework / Assignments	30%	Analytical exercises and case studies focused on threats, logs, and detection concepts.
Midterm Project (Part I)	30%	Threat analysis and conceptual IDS design for a defined environment.
Final Project (Part II)	40%	Integrated intrusion detection and prevention strategy with analysis and justification.
Total	**100%**	

Late Assignment Policy: Assignments are due by 11:59 pm on the due date. Late submissions accepted up to 48 hours with a 10% deduction per day. Work more than 48 hours late will not be accepted unless prior arrangements are approved by the instructor.

Course Schedule

Week	Topics	Project Contribution
1	No Class	Understand the course and do introductions
2	Introduction to Intrusion Detection & Threat Landscape/ Attack Models and Adversary Behavior	Project context and environment selection/ Threat modeling
3	Logging, Monitoring, and Data Sources	Log and data identification
4	Host-Based Intrusion Detection	Detection approach selection
5	Network-Based Intrusion Detection	Network monitoring design
6	Signature-Based Detection	Rule and signature rationale

Week	Topics	Project Contribution
7	Anomaly-Based Detection	Baseline and anomaly reasoning
8	**Midterm Project Due**	Completed detection design
9	Alert Analysis and Correlation	Alert interpretation
10	Deep Packet Inspection Concepts	Traffic analysis considerations
11	Intrusion Prevention & Response	Mitigation strategy
12	Performance, False Positives, and Tuning	Trade-off analysis
13	Ethics, Privacy, and Legal Considerations	Policy and ethics reflection
14	**Project completion (no new content)**	Integration and refinement

ADA Statement

SRSU Accessibility Services. Sul Ross State University (SRSU) is committed to equal access in compliance with the Americans with Disabilities Act of 1973. It is SRSU policy to provide reasonable accommodations to students with documented disabilities. It is the student's responsibility to initiate a request each semester for each class. Students seeking accessibility/accommodations services must contact Mrs. Mary Schwartze Grisham, LPC, SRSU's Accessibility Services Director or Ronnie Harris, LPC, Counselor, at 432-837-8203 or email mschwartze@sulross.edu or ronnie.harris@sulross.edu. RGC students can also contact Alejandra Valdez, at 830-758-5006 or email alejandra.valdez@sulross.edu. Our office is located on the first floor of Ferguson Hall, room 112, and our mailing address is P.O. Box C122, Sul Ross State University, Alpine. Texas, 79832.

Student Responsibilities Statement

All full-time and part-time students are responsible for familiarizing themselves with the Student Handbook and the Undergraduate & Graduate Catalog and for abiding by the University rules and regulations. Additionally, students are responsible for checking their Sul Ross email as an official form of communication from the university. Every student is expected to obey all federal, state and local laws and is expected to familiarize themselves with the requirements of such laws.

SRSU Distance Education Statement

Students enrolled in distance education courses have equal access to the university's academic support services, such as library resources, online databases, and instructional technology support. For more information about accessing these resources, visit the SRSU website.

Students should correspond using Sul Ross email accounts and submit online assignments through Blackboard, which requires a secure login. Students enrolled in distance education courses at Sul Ross are expected to adhere to all policies pertaining to academic honesty and appropriate student conduct, as described in the student handbook. Students in web-based courses must maintain appropriate equipment and software, according to the needs and requirements of the course, as outlined on the SRSU website. Directions for filing a student complaint are located in the student handbook.

Counseling

Sul Ross has partnered with TimelyCare where all SR students will have access to nine free counseling sessions. You can learn more about this 24/7/365 support by visiting Timelycare/SRSU. The SR Counseling and Accessibility Services office will continue to offer in-person counseling in Ferguson Hall room 112 (Alpine campus), and telehealth Zoom sessions for remote students and RGC students.

Libraries

The Bryan Wildenthal Memorial Library and Archives of the Big Bend in Alpine offer FREE resources and services to the entire SRSU community. Access and borrow books, articles, and more by visiting the library's website, library.sulross.edu/. Off-campus access requires logging in with your LoboID and password. Librarians are a tremendous resource for your coursework and can be reached in person, by email (srsulibrary@sulross.edu), or by phone (432-837-8123).

No matter where you are based, public libraries and many academic and special libraries welcome the general public into their spaces for study. SRSU TexShare Cardholders can access additional services and resources at various libraries across Texas. Learn more about the TexShare program by visiting library.sulross.edu/find-and-borrow/texshare/ or ask a librarian by emailing srsulibrary@sulross.edu.

Mike Fernandez, SRSU Librarian, is based in Eagle Pass (Building D-129) to offer specialized library services to students, faculty, and staff. Utilize free services such as InterLibrary Loan (ILL), ScanIt, and Direct Mail to get materials delivered to you at home or via email.

Academic Integrity

Students in this class are expected to demonstrate scholarly behavior and academic honesty in the use of intellectual property. Students should submit work that is their own and avoid the temptation to engage in behaviors that violate academic integrity, such as turning in work as original that was used in whole or part for another course and/or professor; turning in another person's work as one's own; copying from professional works or internet sites without citation; collaborating on a course assignment, examination, or quiz when collaboration is forbidden. Students should also avoid using open AI sources ***unless permission is expressly given*** for an assignment or course. Violations of academic integrity can result in failing assignments, failing a class, and/or more serious university consequences. These behaviors also erode the value of college degrees and higher education overall.

Classroom Climate of Respect

Importantly, this class will foster free expression, critical investigation, and the open discussion of ideas. This means that all of us must help create and sustain an atmosphere of tolerance, civility, and respect for the viewpoints of others. Similarly, we must all learn how to probe, oppose and disagree without resorting to tactics of intimidation, harassment, or personal attack. No one is entitled to harass, belittle, or discriminate against another on the basis of race, religion, ethnicity, age, gender, national origin, or sexual preference. Still, we will not be silenced by the difficulty of fruitfully discussing politically sensitive issues.

Supportive Statement

I aim to create a learning environment for my students that supports various perspectives and experiences. I understand that the recent pandemic, economic disparity, and health concerns, or even unexpected life events may impact the conditions necessary for you to succeed. My commitment is to be there for you and help you meet the learning objectives of this course. I do this to demonstrate my commitment to you and to the mission of Sul Ross State University to create a supportive environment and care for the whole student as part of the Sul Ross Familia. If you feel like your performance in the class is being impacted by your experiences outside of class, please don't hesitate to come and talk with me. I want to be a resource for you.

AI Policy Required for Inclusion in All Syllabi

September 4, 2025

A. To promote transparency, academic integrity, and consistency across the curriculum, each course syllabus must include a clearly articulated statement addressing the use of generative artificial intelligence (AI) technologies, including large language models (LLMs).

1. This statement should specify whether such technologies are permitted, restricted, or prohibited within the context of the course, and define any conditions under which their use is acceptable (e.g., for drafting, idea generation, or coding assistance).
2. Faculty are encouraged to align their guidance with the institution's academic integrity policies, information security guidelines on the use of AI, and the norms of their discipline.
3. Including this statement is required to ensure that students understand the expectations surrounding generative AI and LLMs and to support informed, responsible engagement with these emerging technologies in academic work.
4. The following language is **required** to be included in each syllabus:

> *The University does not recommend or endorse any specific AI tools or resources. Students should be aware that many generative AI tools (e.g., ChatGPT, Google Gemini, Microsoft Copilot) store user input and may use this data to train future models. For this reason, students should never upload or share personal, confidential, or identifiable information—such as names, ID numbers, health data, or assignment submissions containing such details—into any generative AI platform. When using AI tools, students should verify whether the tool complies with student privacy standards as indicated by the University. Faculty may recommend specific tools that better align with institutional data privacy policies, but ultimate responsibility for data protection rests with users.*

Students are encouraged to use faculty-recommended platforms when engaging in coursework involving generative AI. The University is not liable for any adverse experience or impact when students interact with these tools.

B. The following examples may be adopted as course policy for syllabi, or they may serve as prompts for faculty to create their own course policy.

1. No use of generative AI tools permitted

   This course assumes that work submitted by students will be generated by the students themselves, working individually or in groups as directed by class assignment instructions. This policy indicates the following constitute violations of academic honesty: a student has another person/entity do the work of any substantive portion of a graded assignment for them, which includes purchasing work from a company, hiring a person or company to complete an assignment or exam, and/or using generative AI tools (such as ChatGPT).

   In this course, every element of class assignments must be fully prepared by the student. The use of generative AI tools for any part of your work will be treated as plagiarism. If you have questions, please contact me.

   All assignments should be fully prepared by the student. Developing strong competencies in the skills associated with this course, from student-based brainstorming to project development, will prepare you for success in your degree pathway and, ultimately, a competitive career. Therefore, the use of generative AI tools to complete any aspect of assignments for this course are not permitted and will be treated as plagiarism. If you have questions about what constitutes a violation of this statement, please contact me.

2. Generative AI is permitted in specific contexts and with acknowledgment

   The emergence of generative AI tools (such as ChatGPT and DALL-E) has sparked interest among many students in our discipline. The use of these tools for brainstorming ideas, exploring possible responses to questions or problems, and creative engagement with the materials may be useful for you as you craft responses to class assignments. While there is no substitute for working directly with your instructor, the potential for generative AI tools to provide automatic feedback, assistive technology and language assistance is clearly developing. Please feel free to reach out to me well in advance of the due date of assignments for which you may be using generative AI tools and I will be happy to discuss what is acceptable.

   In this course, students shall give credit to AI tools whenever used, even if only to generate ideas rather than usable text or illustrations. When using AI tools on assignments, add an appendix showing (a) the entire exchange, highlighting the most relevant sections; (b) a description of precisely which AI tools were used (e.g. ChatGPT private subscription version or DALL-E free version), (c) an explanation of how the AI tools were used (e.g. to generate ideas, turns of phrase, elements of text, long stretches of text, lines of argument, pieces of evidence, maps of the conceptual territory, illustrations of key concepts, etc.); (d) an account of why AI tools were used (e.g. to save time, to surmount writer's block, to stimulate thinking, to handle mounting stress, to clarify prose, to translate text, to experiment for fun, etc.). Students shall not use AI tools during in-class examinations, or assignments unless explicitly permitted and instructed. Overall, AI tools should be used wisely and reflectively with an aim to deepen understanding of subject matter.

   It is a violation of university policy to misrepresent work that you submit or exchange with your instructor by characterizing it as your own, such as submitting responses to assignments that do not acknowledge the use of

generative AI tools. Please feel free to reach out to me with any questions you may have about the use of generative AI tools before submitting any content that has been substantially informed by these tools.

In this course, we may use generative AI tools (such as ChatGPT) to examine the ways in which these kinds of tools may inform our exploration of the topics of the class. You will be informed as to when and how these tools will be used, along with guidance for attribution if/as needed. Any use of generative AI tools outside of these parameters constitutes plagiarism and will be treated as such.

Understanding how and when to use generative AI tools (such as ChatGPT, DALL-E) is quickly emerging as an important skill for future professions. To that end, you are welcome to use generative AI tools in this class as long as it aligns with the learning outcomes or goals associated with assignments. You are fully responsible for the information you submit based on a generative AI query (such that it does not violate academic honesty standards, intellectual property laws, or standards of non-public research you are conducting through coursework). Your use of generative AI tools must be properly documented and cited for any work submitted in this course.

To ensure all students have an equal opportunity to succeed and to preserve the integrity of the course, students are not permitted to submit text that is generated by artificial intelligence (AI) systems such as ChatGPT, Bing Chat, Claude, Google Bard, or any other automated assistance for any classwork or assessments. This includes using AI to generate answers to assignments, exams, or projects, or using AI to complete any other course-related tasks. Using AI in this way undermines your ability to develop critical thinking, writing, or research skills that are essential for this course and your academic success. Students may use AI as part of their research and preparation for assignments, or as a text editor, but text that is submitted must be written by the student. For example, students may use AI to generate ideas, questions, or summaries that they then revise, expand, or cite properly. Students should also be aware of the potential benefits and limitations of using AI as a tool for learning and research. AI systems can provide helpful information or suggestions, but they are not always reliable or accurate. Students should critically evaluate the sources, methods, and outputs of AI systems. Violations of this policy will be treated as academic misconduct. If you have any questions about this policy or if you are unsure whether a particular use of AI is acceptable, please do not hesitate to ask for clarification.

3. Students are encouraged to use generative AI tools in coursework

The use of generative AI is encouraged with certain tasks and with attribution: You can choose to use AI tools to help brainstorm assignments or projects or to revise existing work you have written. When you submit your assignment, I expect you to clearly attribute what text was generated by the AI tool (e.g., AI-generated text appears in a different colored font, quoted directly in the text, or use an in-text parenthetical citation).

Designers commonly use AI-content generation tools in their work. In this course, using AI-content generation tools is permitted and will be a normal and regular part of our creative process when it is used according to the below criteria. In this course, neglecting to follow these requirements may be considered academic dishonesty. (1) For each assignment, you are required to include a paragraph that explains which AI content-generation tool you used, the dates you used it, and the prompts you used to generate the content according to the MLA style guide. (2) During critique, it is important to describe the precedents you used and

how any source content was transformed. When showing or presenting images or other content you generated using an AI-tool, cite that image or content following the MLA style guide. If you need help referencing your creative work, contact me to collaborate.
Students are invited to use AI platforms to help prepare for assignments and projects (e.g., to help with brainstorming or to see what a completed essay might look like). I also welcome you to use AI tools to help revise and edit your work (e.g., to help identify flaws in reasoning, spot confusing or underdeveloped paragraphs, or to simply fix citations). When submitting work, students must clearly identify any writing, text, or media generated by AI. This can be done in a variety of ways. In this course, parts of essays generated by AI should appear in a different colored font, and the relationship between those sections and student contributions should be discussed in cover letters that accompany the essay submission.

Appendix: Semester Project Grading Rubric

CSA 4372 – Intrusion Detection / Prevention Systems

Midterm Project – Part I: Threat Analysis & Detection Design (30%)

Criterion	Exemplary	Proficient	Developing	Weight
Problem Definition & System Context	Clear, realistic system and threat environment	Adequate description with minor gaps	Vague or poorly defined context	10%
Threat Identification & Attack Vectors	Comprehensive identification of relevant threats	Most key threats identified	Limited or unclear threat analysis	15%
Detection Approach Selection	Well-justified IDS approach (host/network/hybrid)	Reasonable selection with partial justification	Poorly justified or inappropriate choice	20%
Detection Methodology	Clear rationale for signature and/or anomaly-based detection	Partial explanation of detection methods	Minimal or incorrect explanation	20%
Logging & Monitoring Strategy	Thoughtful selection of data sources and logs	Basic monitoring strategy	Incomplete or unclear strategy	20%
Organization & Clarity	Professional, well-structured, and clearly written	Generally clear with minor issues	Disorganized or difficult to follow	15%

Final Project – Part II: Integrated IDS/IPS Strategy (40%)

Criterion	Exemplary	Proficient	Developing	Weight
Integration of Part I	Seamlessly extends and refines midterm analysis	Mostly integrated with minor gaps	Weak continuity from Part I	15%
Alert Analysis & Interpretation	Clear, logical interpretation of alerts and events	Adequate interpretation	Superficial or unclear analysis	15%
Prevention & Response Strategy	Well-designed mitigation and response workflow	Basic response strategy	Minimal or unrealistic response	20%
False Positives & Performance Trade-offs	Insightful discussion of tuning and trade-offs	Limited discussion of trade-offs	Little or no consideration	15%
Ethical, Legal & Privacy Considerations	Thoughtful and accurate discussion	Basic awareness shown	Missing or incorrect discussion	15%
System-Level Reasoning	Strong end-to-end security reasoning	Adequate system perspective	Fragmented or isolated analysis	10%
Professional Presentation	Clear diagrams, polished writing, strong structure	Minor documentation issues	Unclear or incomplete submission	10%