Sul Ross State University
Course Syllabus
CSA 4372: Intrusion Detect / Prevent
Fall 2023

Instructor: Neal Xiong
Office Location: BAB-00306
Office Telephone Number: 404-645-4067
Email Address: neal.xiong@sulross.edu
Office Hours: MTWR 12:15-2:00 pm, W 2:00-3:30 pm, T 9:00-11:00 am, + by appointment
Time and Place of Class Meetings: TR 2:00-3:15 pm, at BAB-00302

Course Description:

CSST 4372 Intrusion Detection/ Prevention Systems (3-0). 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. Prerequisite: CS3310 Computer Science

Note: It is about 3 Credit Hours.

Course Prerequisites and/or Co-requisites:

CS 3310 (may be concurrent).

Course Learning Objective

Students are introduced to the related development in secure from conceptual models of a requirement to an actual system. The course covers external view of the secure problems, challenges, practice applications, and technology models to include administration, architecture, and others. You need to be able to use customized codes to analyze and remedy computer security issues. We will use a language that is commonly used by secure professionals and apply it to specific secure program practice problems.

Student Learning Outcomes (SLO):

During this course, students should be able to:

- Use correct syntax and structure in the selected secure language
- Use common programming structures to write efficient and effective code
- Demonstrate an understanding of the fundamental data types.
- Write simple decision making statements, assignment statements, and I/O statements.
- Use functions and parameters to develop problem solutions on the computer
- Create simple programs related to secure program practice problems and situations.

Marketable Skills:

1. Students will develop logical and analytical skills

2. Students will use problem-solving skills
3. Students will know computing methodologies in demand by public and private sectors

Instructional Methods / Strategies:
Virtual Meeting Room: TR, 2:00-3:15 pm, at BAB 00302.
Blended / Partial: Zoom or Microsoft Teams (confirmed by Dept.).
Online: All contents are post online (confirmed by Dept.).

Instructional Methods / Strategies:
The course is a combination of lecture, class discussion, hands-on lab work, assignments, peer review, and reading outside of class.

Students will be required to check their email daily:
Make sure that your email address in Blackboard is set up correctly in case I use the Blackboard email system.

Weekly activities include some or all of the following:

- Reading assigned material
- Researching assigned topics
- Participating in one or more assigned Discussions Boards by posting a contribution and responding to contributions of other students and/or the instructor
- Participating in Discussion Board forums related in Individual Projects
- Participating in Discussion Board forums related to Group Projects
- Submitting status reports on project progress
- Writing and posting papers
- Preparing and posting PowerPoint presentation
- Communicating with the instructor or other class members

Learning Outcome Assessment Methods include:

- 2-3 exams, and one of these will be the comprehensive final exam
- Assignments, and you will get full credit for completed homework.

For specific dates and point values, see the end of this document.

Instructional Materials

Recommended but not required Materials:

- Introduction to Computer Networks and Cybersecurity, Chwan-Hwa (John) Wu, J. David Irwin, 2013 by CRC Press is an imprint of the Taylor & Francis Group, Boca Raton, London, New York, USA. International Standard Book Number-13: 978-1-4665-7214-0 (eBook).
- Open source book: https://greenteapress.com/wp/think-python-2e/
- Python 3 Reference: https://docs.python.org/3/reference/

- Python 3 Tutorial: https://docs.python.org/3/tutorial/
- Starting out with Programming Logic and Design, 3rd Ed, by Tony Gaddis, ISBN-13: 978-0132805452, ISBN-10: 0132805456, Pearson.
- Python in easy steps, McGrath, Mark, ISBN-13: 978-1840785968, In easy steps.

TEXT: None. You will be required to watch certain online lectures or read selected online readings. Details will be found on Blackboard as assignments are made.

Grading Policy / Scale:

For classes taught on one campus only, you still need to come to class. For classes taught on both campuses simultaneously, the designation of the class is ITV. Classrooms are reserved for the whole semester, not for selected dates of the semester.

I record attendance and give attendance points. You can only get attendance points if we are in the same classroom, or if you are online when I am on the opposite campus. Partial session attendance may result in partial points. Missed class meeting may receive attendance points if you provide proper documentation, at my discretion. Participation points may be unevenly distributed over the semester (i.e. not each day gets equal points).

Lab computers are a shared resource. You would not want to start a test and have computer problems because someone spilled food or drink on the keyboard. The first time I see you bring food or drink into a lab, I will give you one (1) penalty point. Each subsequent infraction earns you fifty (50) penalty points.

Grading

The grade you earn in this course will be based upon the accumulation of points that will be distributed in this manner:

GRADES: Grades will be calculated in the following manner:
Exams (2~3)
Lab or workshop exercises (5～6),
Homework (HW2+)

The instructor reserves the right to lower the cutoffs for each grade, but he will not raise the cutoff. In other words, an 86% may end up being an A at the instructor's discretion, but a 91% is guaranteed to be an A. I will let you know after each exam what the current grading scale is.

For simplicity, we use a 1,00-point scale (calculated as a percentage %).

90+ = A
80 - 89 = B
70 - 79 = C
60 - 69 = D
less than 60= F

The Family Educational Rights and Privacy Act of 1974 (FERPA) governs university policies regarding family educational and privacy rights. Copies of the act, policies and regulations are maintained in the Office of Admissions and Records, John Vaughn Library, and the Office of the Vice President of Academic Affairs. Students can find their course grades in the Blackboard

gradebook. I will NOT post grades elsewhere, nor provide grades via telephone, or any other manner in violation of FERPA or any other local, state, or federal regulations.

Assignments Information:

- Homework assignments count for a significant part of the course. (Almost) all homework assignments work with the Peer Review feature in Blackboard. This means, that you will be required to review and give constructive feedback on the homework of other students in the class, and that you will receive feedback on your assignment from other students in the class. The review period is always for one week after the due date for the assignment. Reviews are anonymous. You do not know the identity of the students giving you feedback (unless they let you know), and the students reviewing your work will not know who you are (unless you add your name to the assignment). Otherwise, I am the only one who knows who reviews whom. You earn points both for doing the homework and for doing the reviews. Of course, I will be reviewing your assignments too. I will use them to show examples of good work and examples of room for improvement.
- You will get full credit for homework you turn in, no matter how good or bad. If you don't turn it in on time, Blackboard automatically switches to the review period and you get no points for homework submission. I want you to get into the habit of working regularly.
- I discuss the homework on the first day of the week, and then your peer reviews will be available. Your reviews may be evaluated critically, and you can lose points there. If someone to review did not turn in homework, you will see a message that the user did not submit the assignment and gets an automatic zero. Make sure to click the Submit button so you get the full points for your review.
- Be sure to review the feedback from your peers after the review period has ended.
- All students must complete their own assignments, but **assistance from other students both during class time and outside class time is encouraged**. This does not include copying and pasting someone else's material or files. If two students work together, the two do the assignment twice - from scratch. If three students work together, the three do the assignment three times - from scratch. You will find that each time gets easier and faster; that you start finding improvements on the next try, and that you never really end up with exactly the same file. Repetition is an integral part of the learning process. Of course, group assignments are limited to the group.
- All work is due at the date and time indicated in the schedule. When the time to submit has passed, the assignment automatically switches from submission mode to review mode. There is no opportunity to make up missed or late assignments. You can still get points for reviewing your peers' work.
- Check your homework assignments in the Grades page. You can download and check the files you submitted there.
- I will only grade work submitted over Blackboard. Do not email files. If you make a mistake, or would like to send different files before the due date, just send all the assignment files again. If you must send multiple files, make sure to send them all together. If Blackboard only allows you to attach one file, create a compressed (zipped) file. If you want to, you can also send a backup copy of assignments to neal.xiong@sulross.edu. It is an email address that I do not monitor actively, but an email with assignment attached, sent before the due date, would be a consideration for adjustments to your final grade under my instructor discretion.

Tests

- You can only take the tests in the classroom. Some tests will be done with paper and pencil in class. Online tests will be password protected and the password will only be available to students in class. For classes alternating between Tahlequah and Broken Arrow, someone else will monitor the test in Broken Arrow. Students in the BA section are welcome to come to Tahlequah so you can ask me to help with computer problems.
- Unless specifically announced in writing, all tests are closed book and done without any aids. This includes cellphones. Turn off your cellphone before the test and do not turn it on until you have left the classroom.

The final exam is comprehensive. If you miss one of the earlier tests, you can ask by email to neal.xiong@sulross.edu to have the score on the comprehensive final to replace the score on the missed test.

My Teaching Philosophy

I think that the following promote better learning, so I build them into my courses.

- Multiple-choice tests are a poor tool to measure if students learn. I mainly use MC quizzes to force students to read the material. In programming courses, you work mostly on programs.
- You need frequent feedback on how you are doing. I use low-stakes testing (frequent, small assignments, few points) for regular homework, and high-stakes testing (infrequent, large tests, high points) to test “for real”.
- Repetition helps. We practice the same thing at least once, but preferably multiple times, before the test.
- A great way to learn is to review someone else’s work, evaluate it on clear criteria, and providing constructive feedback. I use peer grading for homework. Everything can be anonymous (for the students). Unless you choose otherwise, peer reviewers do not know the identity of the student reviewed, and students whose work is reviewed do not know who reviewed them.
- Regular work helps. I use that in my courses by setting clear dates for assignments, and providing timely feedback. Over the years, I have noticed more and more that one of the main reasons students fail is poor planning. Cramming before a test just does not work in the long run. I make the chunks smaller and more frequent, but that only works if both I as instructor and you as student work on that together.
- Peer pressure is a positive thing. In class, I show examples of your homework to show anonymous examples great work and not-so-great work. If you want your reviewer to know your name, reveal it in the Comments box on submission. Do not put it in the files you send. Be proud if I show your work as an example of great work, and you do not have to be embarrassed if your work is criticized – just do better next time.
- Life happens. Some will say that "sh*t happens". You get sick; the car breaks down, etc. I record all class sessions on Collaborate, so it is easy to catch up with the material if something happens.
- Coming to class helps. I have C students making As because they come to class and turn in work on time. I have A students getting Cs because they underestimate the material, skip class, and think that they can make it all up on the final. Of course, I also have A students making As and C students making Cs. To encourage you to attend, I give attendance points. Please check

your attendance points in the gradebook and if you did not get the points, contact me so I can check.

- You need to know how you are doing in the class. I use a very simple system: for example, 1,000 points in the course. As soon as you have 700 points, you have EARNED a C. When you get to 800 points, you have EARNED a B.

Class and Instructor Policies

Attendance is required with 100 credit points, and hope everyone can enjoy this course. If there is any special case, please contact with your instructor directly.

Academic Policies / Required Information

Please go to our university website for required information pertaining to:

- Academic Misconduct
- American with Disabilities Act
- Inclement Weather/Disaster Policy
- Release of Confidential Information
- Student Handbook
- Teach Act
- Textbook Information
- Title IX
- Library Services
- Distance Education Statement

Dropping the Class

Each semester, SRSU sets a deadline during the semester when students may drop a course with an automatic "W". The deadline is available at the Academic Calendar of the university. Your work is reviewed regularly and promptly, and I post the grades as soon as possible. Knowing your current points total and how many points you can still earn, tells you your standing in the class. If you do not do well before the deadline to drop with a "W," consider dropping the class.

If you decide to drop after the deadline to drop with an automatic "W," there is a second deadline for withdrawing from the class. You will only get a "W" if you are passing at the time of withdrawal based on the University's policy:

> .....Withdrawal after Twelfth Week: If a student formally withdraws from single classes or completely from the University after the twelfth week, the instructor will assign a W or F depending on the student's standing in the class at the time of withdrawal. A "W" will be assigned if the student was passing at the time of withdrawal. An F will be assigned if the student was failing at the time of withdrawal.....

I follow this policy, so please do not ask to give you a W after the deadline for withdrawing with a W. Furthermore, instructors have the option dropping students from the class under the Academic Withdrawals policy. This is what the policy says:

> "Students who enroll in a course or courses and have poor attendance or participation as determined by the instructor may be administratively withdrawn "AW." Students who are withdrawn for non-attendance or administratively withdrawn will be responsible for payment

and repaying any financial aid received for the course or courses that must be returned to the provider."

Finally, faculty must report students who do not attend the course. We usually have to do this in the second week of the course. Logging into an online course is not sufficient to constitute attendance. You need to have participated in some way - a discussion board, assignment, etc.

Academic Dishonesty

The navigation menu on the left has a special button for academic integrity. This is the university policy. Read it, and notice that the sanction for being caught cheating is up to the instructor. The following applies to all courses I teach: **My standard sanction for any cheating is an F in the course.**

General Policies:

Students are expected to check on Blackboard for announcements and updated assignments. You are expected to check your Sul Ross e-mail account. When meeting through Zoom or Microsoft Teams, make sure your first name and at least last initial are visible. Preference will be that your video is available, but please make sure you are properly dressed.

Americans With Disabilities Act:

Sul Ross State University (SRSU) is committed to equal access in compliance with 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 Rebecca Greathouse Wren, LPC-S, SRSU's Accessibility Services Coordinator at 432-837-8203 (please leave a message and we'll get back to you as soon as we can during working hours), or email rebecca.wren@sulross.edu. Our office is located on the first floor of Ferguson Hall (Suite 112), and our mailing address is P.O. Box C-122, Sul Ross State University, Alpine, Texas, 79832.

Library Services:

The Sul Ross Library offers 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 your LoboID and password. Check out materials using your photo ID. Librarians are a tremendous resource for your coursework and can be reached in person, by email (srsulibrary@sulross.edu), or phone (432-837-8123).

Distance Education Statement:

Students enrolled in distance education courses have equal access to the university's academic support services, such as Smarthinking, 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 secure login information to verify students' identities and to protect students' information. The procedures for filing a student complaint are included in the student

handbook. 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.

Diversity Statement:
"I aim to create a learning environment for my students that supports a diversity of thoughts, perspectives and experiences, and honors your identities (including race, gender, class, sexuality, religion, ability, socioeconomic class, age, nationality, etc.). I also understand that the crisis of COVID, economic disparity, and health concerns, or even unexpected life events could 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 an inclusive 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."

Class Calendar with Assignment Due Dates

Sections	Topic(s)	Assignments
1	Installing and configuring Python • Command line • Paths • pip • IDLE • Online compiler (repl.it) • Interpreters • Notebooks • Editor / IDE	Install and configure Python 3 and relevant tools
2	Introduction to Python • Interpreter • Compiler • Syntax	Use the Python interpreter to execute Python commands Create and execute simple Python programs
3	Python Code • Flow Control • Loops • Functions	Write a Python program demonstrating use of these concepts
		Midterm exam
4	Python Data Types • Tuples	Write a Python program

	• Lists • Dictionaries • Strings	demonstrating use of these concepts
5	Using External Libraries (some possibilities) • Pattern Matching with Regular Expressions • Reading and Writing Files • Debugging • Web Scraping • Working with CSV Files and JSON Data • Time, Scheduling Tasks, and Launching Programs • Sending Email and Text Messages • SCAPY Network Tool • Port Scanning Recommend reading ppt 7	Write Python programs demonstrating use of some of the listed concepts (TBA)
		Final exam

[Note: you may add any additional sections or appendices that you would like to include in your syllabus.]