UNIVERSITY OF THE INCARNATE WORD
School of Mathematics, Science and Engineering

Course Syllabus

Basic Information

Term	**Fall 2021**		
Course Title	*Intrusion, Detection, and Response*		
Course Code	CIS 3370		
Credit Hours	3.0		
Classroom	Building: BSH, 323		
Class Schedule	Tue & Thur: 12:00 PM – 1:15 PM		
Prerequisite Course	None		
Course Professor	Dr. Gonzalo De La Torre Parra		
Department Offering the Course	Computer Information Systems and Cyber Security		
Department Chair	Dr. Michael Frye		
School	School of Mathematics, Science and Engineering		
Contact Email	TBD		
Contact Number	TBD		
Office and Location	TBD		
Office Hours	Mon, Wed	11:00 AM – 12:00 PM	❄ *Also available by appointment*
	Mon, Wed	1:30 PM – 3:00 PM	
Number of Lectures	28		

2 Catalog Description

Learn the concepts of Network Security Monitoring. We will cover the different tools for data collection, types and placement of sensors in the network. Detection methods of information that may indicate compromise. Analysis data to include packet analysis and analysis methods.

3 Course Overview

This course is intended for anyone interested in learning how the vast amounts of data generated today are input and stored and organized and protected and accessed. Databases are the power behind BannerWeb, Blackboard, search engines, commercial websites (why this course is part of the Website Development Specialization), and how businesses secure the vast amount of data and information that they have or

create. Learning to create an effective and efficient organizational infrastructure, how to securely input and process data. Securing information is required by laws and regulation. This is a necessary skills for all managers of computer technology as databases and database management becomes increasingly important in our computer-dependent and cloud-oriented worlds.

Fifty years ago, we stored information on paper in folders in boxes or a filing cabinet. Contact information was stored on 3x5 cards in a Rolodex device. Today this information is stored electronic format on company servers or in the cloud. This has increased the risk of compromise of the data. To help protect the data, different types of network security monitoring devices and software is used monitor and respond to possible intrusions or compromise of this data.

4 Course Resources

1. Textbook: Applied Network Security Monitoring: Collection, Detection, and Analysis, 1st edition, Chris Sanders, Jason Smith, Syngress publishing, ISBN: 978-0-12-417208-1

2. Internet Access/Word Processing: Students will need Internet access and will require administrative access to a computer system to successfully complete the activities in this course. It is the responsibility of the student to not only have access to the internet, but to have access to a word processor (MS Office/Open Office/Google Docs) for course activities. UIW facilitates these resources on campus.

3. Email and Blackboard Learn: For this course, we will correspond using the UIW email system. Blackboard Learn may be used throughout the semester to provide a student-instructor forum for sharing information.

5 Course Outcomes

Upon completion of this course, students will be able to understand the basics of network security monitoring, along with the different tools and methods used to perform security monitoring. Be able to analysis the type and placement of sensors and security devices. How to analysis threat data.

Accomplishment of this outcome will be assessed by quizzes and exams along with performance of the installation of and configuration of security devices.

6 Assessment

Course objective will be assessed by:

- Attendance
- Mid-terms and final course examinations of course material presented.
- Group project where each student will be evaluated by their contribution to the overall success of the project

7 Grading Activities, Criteria, and Guidelines

- Class Attendance (10%): Students are expected to attend class but are provided with 3 excused absences as stated in 1.6 and it is evaluated as follows:
  - 0 - 2 absences
  - 3 absences 5% of the final grade will be deducted
  - 4 withdraw from class
  - Note: Students entering the classroom more than **15 minutes** after class starts will be **counted as being absent**

- Two Mid-Term Exams (20% each) - Exam will generally include multiple choice, True/False selection, fill-in the blank, and short answer questions. Material from the discussion, slides, and lecture notes will comprise most of the mid-term content.
- Group project (30%) - Functional Security Monitoring Software, Attack simulation, and Detection Presentation (20%), Group project status report (10%).
  - Status report: Each group should submit a status report in MS Word to Blackboard. The report should include current status of the project, challenges (if any) and next step.
  - Presentation: Prepare a 5 slides presentation and a demo showcasing the successful deployment of your Security Monitoring Software, simulated attack generation, and attack detection using the software of your preference..
  - Blackboard Discussion: Post your project to Blackboard group project discussion area and be able to answer questions from your peers. Each group must provide a minimum of two comments/questions to two different groups. Each group is responsible about answering all the questions related to their project.
- Final Exam (20%) - The final exam will be given on the scheduled date per UIW final exam scheduling. This end of course exam can be over anything we have covered during the course. Please do not schedule anything that might conflict with the final exam. No one will be excused from it and there will be no make-up exam dates.

Evaluation Criteria Letter grades will be determined using a standard percentage point evaluation as outlined below. The final grade will be computed on the following weights:

Evaluation Event	Grade Percentage
Attendance	10
Mid Term Exam 1	20
Mid Term Exam 2	20
Group Project	30
Final Course Exam	20
Total	100

8 General Student Information

Teaching Strategy: This is an in person course. This means that we will meet twice a week in class unless I tell you otherwise. Please monitor your email for weekly announcements. Students are responsible about attending all classes and attendance will be recorded via GradesFirst.

Changes: This outline is a guideline and not a contract. As such, I may alter it if it seems to be in the best interest of the class to do so. I will discuss prominent changes with you and post them on Blackboard. I will make every attempt to hold graded activities on the date scheduled

Attendance: Class attendance is mandatory, students are expected to attend and participate in all scheduled meetings. Students are also expected to show active participation in the course and complete each learning module assignments on-time via Blackboard and show active participation. Students are allowed up to 3 excused absences throughout the semester. There are only two types of excused absences as the following:

- Planned Absences. Students must notify instructors in writing at least two weeks prior to planned absences such as participation in an official university function, observance of a religious holy day or active military service. If the absence is for military service the student should provide to each instructor a copy of the military orders. The University of the Incarnate Word welcomes persons of diverse backgrounds and is therefore committed to providing reasonable accommodations for students

wanting to attend religious observances and who will miss class. Students must inform instructors at least two weeks prior to attending a religious observance. Students use the form found in the UIW Student Handbook Student Code of Conduct to request accommodations from the instructor.

- Illness or other extenuating circumstances. Students should notify the instructor directly of absence due to illness or other extenuating circumstance.

  Students who are not able to attend a course are responsible for dropping the course by the appropriate deadline. Instructors may not automatically drop a student from a course. Students who do not attend, accumulate 4 or more absences, and who do not officially drop the course will be reported to the dean of student success and will receive a failing grade for the course.

Makeup Policy: Homework assignments only may be reassessed up to 1 week late with a fixed, post-evaluation penalty of 25%. No make-up work will be accepted more than 7 calendar days past the due date. There will be no accommodations for missed group project submissions or exams and students will receive a zero for that grade.

Academic Integrity Statement: The highest standards of academic honesty are expected in the course. Forms of academic dishonesty include, but are not limited to cheating, plagiarism, counterfeit work, falsification of academic record, unauthorized reuse of work, theft, and collusion. See the student handbook for definitions and procedures for investigation of claims of academic dishonesty. `http://www.uiw.edu/campuslife/documents/uiwstudenthandbook1618.pdf`

Disability Accommodations: The University of the Incarnate Word is committed to providing a supportive, challenging, diverse and integrated environment for all students. In accordance with Section 504 of the Rehabilitation Act â Subpart E, Title III of the Americans with Disabilities Act (ADA), and Title III of the ADA Amendments Act of 2008 (ADAAA), the University ensures accessibility to its programs, services and activities for qualified students with documented disabilities. To qualify for services, the student must provide Student Disability Services with the appropriate documentation of his or her disability at the time services and/or accommodations are requested.

Title IX Information: Unlawful discrimination has no place at the University of the Incarnate Word. It violates the University's core values, including its commitment to equal opportunity and inclusion, and will not be tolerated. The University of the Incarnate Word prohibits sexual misconduct, that can include: (1) sex and gender based discrimination; (2) sexual and sex and gender based harassment (including a hostile environment based on sex or gender); (3) sexual assault; (4) sexual exploitation; (5) stalking; and (6) relationship violence (including dating and domestic violence). For more information, or to report an incident, please visit www.uiw.edu/titleix.

Pregnancy Accommodations: Under the Department of Education's (DOE) regulations implementing Title IX of the Education Amendments of 1972, the University does not discriminate against any student on the basis of pregnancy or pregnancy related conditions. To request reasonable accommodations for disability, temporary disability (e.g., injury, surgery) or pregnancy, please contact:

Student Disability Services
4301 Broadway CPO 286
Administration Building â Suite 105
San Antonio, TX 78209
(210) 829-3997 (210) 829-6078

Academic Grade Assignments: According to the Undergraduate Catalog the following is how letter grades will be assigned at the University.

Grade	Numeric Range	Grade Points	Comments
A	93 - 100	4.00	Indicates a superior grasp of the subject matter of the course. Demonstrates initiative and originality in approaching problems. Appropriately synthesizes course information with ability to relate knowledge to new situations.
A-	90 - 92	3.70	
B+	87 - 89	3.30	Indicates better than average grasp of the subject matter of the course and ability to appropriately apply principles with intelligence.
B	83 - 86	3.00	
B-	80 - 82	2.70	
C+	77 - 79	2.30	Indicates an acceptable grasp of the essential knowledge elements of the course.
C	70-76	2.00	
D+	67 - 69	1.30	Indicates less than average performance in the course.
D	63 - 66	1.00	
D-	60 - 62	0.07	
F	<60	0.00	Indicates failure to master the minimum essentials of the course material. The course must be repeated.

9 Course Schedule

Wk	Date	Topic	Comments
1	08/24	Course Overview/Syllabus	
	08/26	Course Syllabus and Introduction	
2	08/31	NSM Intro presentation review	
	09/02	What is Security presentation Review	
3	09/07	Selection of software project	
	09/09	Security Framework presentation review	
6	09/14	Software installation progress review	
	09/16	Information Sharing presentation review	
7	09/21	Reputation presentation review	
	09/23	Software installation progress review	
8	09/28	Midterm I Review	
	09/30	Midterm I	
9	10/05	Reputation presentation review	
	10/07	Software installation progress review	
10	10/12	SEIM presentation review review	
	10/14	The Cyber Kill Chain	
11	10/19	Nmap network Scanning presentation review	
	10/21	Demonstrate NMap	
12	10/26	Wireshark presentation review	
	10/28	Wireshark trace presentation review	
13	11/2	Midterm II Review	
	11/4	Midterm II	
14	11/9	Intrusion Detection Systems presentation review	
	11/11	Security Tools presentation review	
15	11/16	Software installation progress review	
	11/19	Web Attacks presentation review	