INTRUSION DETECTION (ITSY 2330 6A1)

INSTRUCTOR CONTACT INFORMATION

Instructor:	Susan Joiner
Email:	sljoiner@lit.edu
Office Phone:	409-247-5326
Office Location:	TA4 Room 103A
Office Hours:	MWF 7:30-8:00am; 12:00-3:00pm TR 7:30-8:00am; 12:00-3:00pm

CREDIT

3 Semester Credit Hours (2 hours lecture, 4 hours lab)

MODE OF INSTRUCTION

Traditional

PREREQUISITE/CO-REQUISITE:

None

COURSE DESCRIPTION

Computer information systems security monitoring, intrusion detection, and crisis management. Includes alarm management, signature configuration, sensor configuration, and troubleshooting components. Emphasizes identifying, resolving, and documenting network crises and activating the response team.

COURSE OBJECTIVES

Upon completion of this course, the student will be able to

- Build IDS sensors and attach them to the network (hardware and software).
- Install and manage a secure communication link between all sensors and the monitor.
- Install and manage event database(s); analyze an event and trends.
- Install, manage, and interpret syslog servers and system logs.
- Identify legal and policy issues associated with system and network monitoring.
- Deploy, implement, and test IDS security plan.

REQUIRED TEXTBOOK AND MATERIALS

Cengage MindTap access to *Hands-On Ethical Hacking and Network Defense, 4th Edition*, Wilson, Robert S., Simpson, and Antill; Cengage, 2023

    a. **How to buy** your Course Materials
Step 1: Sign into **Blackboard** and click on **this course**
Step 2: Click on the Cengage link: **Getting Started** in the *Getting Started with Cengage MindTap* section.
Step 3: Create or sign into your Cengage account to access or purchase the materials for this

course.

> **NOTE**: If you are taking additional courses that use Cengage materials, you can save by purchasing a Cengage Unlimited plan, which gives you access to all Cengage eTextbooks and online homework platforms for one price. Visit cengage.com/unlimited or your campus bookstore to learn more.

b. Beware of sites that are selling discounted codes. These sources are likely unauthorized sellers who have acquired access codes illegally, and transactions with such sources may pose a risk to your personal information.

c. Need help? Visit startstrong.cengage.com for step-by-step registration instructions and videos.

ATTENDANCE POLICY
Three absences are allowed. If a student is tardy to class or departs early three (3) times, it will be equal to one (1) absence. Each absence beyond three absences will result in a 2-point deduction from your final grade.

DROP POLICY
If you wish to drop a course, you are responsible for initiating and completing the drop process by the specified drop date as listed on the Academic Calendar. If you stop coming to class and fail to drop the course, you will earn an "F" in the course.

STUDENT EXPECTED TIME REQUIREMENT
For every hour in class (or unit of credit), students should expect to spend at least two to three hours per week studying and completing assignments. For a 3-credit-hour class, students should prepare to allocate approximately six to nine hours per week outside of class in a 16-week session OR approximately twelve to eighteen hours in an 8-week session. Online/Hybrid students should expect to spend at least as much time in this course as in the traditional, face-to-face class.

COURSE CALENDAR (Subject to change)

DATE	TOPIC	READINGS	ASSIGNMENTS (Due on this Date)
Week 1 1/16-1/21	Ethical Hacking Overview	Module 1	Lab 1-1 Quiz 1 1/28/2024
Week 2 1/21-1/28	TCP/IP Concepts Review	Module 2	Quiz 2 1/28/2024
Week 3 1/28-2/4	Network and Computer Attacks	Module 3	Lab 3-1 Lab 3-2 Lab 3-3 Lab 3-4 Quiz 3

			2/4/2024
Week 4 2/4-2/11	Footprinting and Social Engineering	Module 4	Lab 4-1 Lab 4-2 Quiz 4 2/11/2024
Week 5 2/11-2/18	Port Scanning	Module 5	Lab 5-1 Quiz 5 2/18/2024
Week 6 2/18-2/25	Enumeration	Module 6	Lab 6-1 Quiz 6 2/25/2024
Week 7 2/25-3/3	Programming for Security Professionals	Module 7	Quiz 7 3/3/2024
Week 8 3/3-3/10	Desktop and Server OS Vulnerabilities	Module 8	Lab 8-1 Quiz 8 3/10/2024
Week 9 3/17-3/24	Embedded Operating Systems: The Hidden Threat	Module 9	Case Project 9-3 Quiz 9 3/24/2024
Week 10 3/24-3/31	Hacking Web Servers	Module 10	Lab 10-1 Lab 10-2 Lab 10-3 Quiz 10 3/31/2024
Week 11 3/31-4/7	Hacking Wireless Networks	Module 11	Lab 11-1 Quiz 11 4/7/2024
Week 12 4/7-4/14	Cryptography	Module 12	Lab 12-1 Lab 12-2 Quiz 12 4/14/2024
Week 13 4/14-4/21	Network Protection Systems	Module 13	Lab 13-1 Quiz 13 4/21/2024
Week 14 4/21-4/28	Hands-On Ethical Hacking Final Project	Module 14	Quiz 14 4/28/2024
Week 15 4/28-5/5	Hands-On Ethical Hacking Final Project (continued)	Module 14	Quiz 14 5/5/2024
Week 16 5/5-5/9	Final Exam	Final Exam	Final Exam 5/2/2024

COURSE EVALUATION

Final grades will be calculated according to the following criteria:

- Labs   40%
- Module Quizzes   15%
- Final Project   15%
- Final Exam   30%

GRADING SCALE

90 – 100   A
80 – 89   B
70 – 79   C
60 – 69   D
0 – 59   F

LIT does not use +/- grading scales

ACADEMIC DISHONESTY

Students found to be committing academic dishonesty (cheating, plagiarism, or collusion) may receive disciplinary action. Students need to familiarize themselves with the institution's Academic Dishonesty Policy available in the Student Catalog & Handbook at http://catalog.lit.edu/content.php?catoid=3&navoid=80#academic-dishonesty.

TECHNICAL REQUIREMENTS

The latest technical requirements, including hardware, compatible browsers, operating systems, etc. can be online at https://lit.edu/online-learning/online-learning-minimum-computer-requirements. A functional broadband internet connection, such as DSL, cable, or WiFi is necessary to maximize the use of online technology and resources.

DISABILITIES STATEMENT

The Americans with Disabilities Act of 1990 and Section 504 of the Rehabilitation Act of 1973 are federal anti-discrimination statutes that provide comprehensive civil rights for persons with disabilities. LIT provides reasonable accommodations as defined in the Rehabilitation Act of 1973, Section 504 and the Americans with Disabilities Act of 1990, to students with a diagnosed disability. The Special Populations Office is located in the Eagles' Nest Room 129 and helps foster a supportive and inclusive educational environment by maintaining partnerships with faculty and staff, as well as promoting awareness among all members of the Lamar Institute of Technology community. If you believe you have a disability requiring an accommodation, please contact the Special Populations Coordinator at (409)-951-5708 or email specialpopulations@lit.edu. You may also visit the online resource at Special Populations - Lamar Institute of Technology (lit.edu).

STUDENT CODE OF CONDUCT STATEMENT
It is the responsibility of all registered Lamar Institute of Technology students to access, read, understand and abide by all published policies, regulations, and procedures listed in the *LIT Catalog and Student Handbook*. The *LIT Catalog and Student Handbook* may be accessed at www.lit.edu. Please note that the online version of the *LIT Catalog and Student Handbook* supersedes all other versions of the same document.

STARFISH
LIT utilizes an early alert system called Starfish. Throughout the semester, you may receive emails from Starfish regarding your course grades, attendance, or academic performance. Faculty members record student attendance, raise flags and kudos to express concern or give praise, and you can make an appointment with faculty and staff all through the Starfish home page. You can also login to Blackboard or MyLIT and click on the Starfish link to view academic alerts and detailed information. It is the responsibility of the student to pay attention to these emails and information in Starfish and consider taking the recommended actions. Starfish is used to help you be a successful student at LIT.

ADDITIONAL COURSE POLICIES/INFORMATION
Course Policies
1. No food, drinks, use of tobacco products, or vaping products in class.
2. Electronic devices not being used for the class, such as phones and headphones, must be turned off while in class.
3. Do not bring children to class.
4. Any work submitted after the assigned due date will **receive a 10% deduction**.
5. A grade of 'C' or better must be earned in this course for credit toward degree requirement.
6. It is the student's responsibility to verify transferred grades and ask for corrections if needed.
7. All work is due before the final exam date. Nothing will be graded after the final exam.

Certification Requirement
CSNT majors are required to earn certification in one of the following areas prior to graduation.
- A+ Certification
- Network+ Certification
- Security+ Certification
- Linux+ Certification
- Cisco Certified Network Associate (CCNA)