# Intrusion Detection
# (ITSY 2330)

**Credit:** 3 semester credit hours (2 hours lecture, 4 hours lab)

**Prerequisite/Co-requisite:** None

## Course Description

This course covers computer information systems security monitoring, intrusion detection, and crisis management. It includes alarm management, signature configuration, sensor configuration, and troubleshooting components and emphasizes identifying, resolving, and documenting network crises and activating the response team.

## Required Textbook and Materials

1. 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.
2. Computer Networking and Troubleshooting Technology and Cybersecurity students are required to have one 64 GB or larger capacity USB Flash Drive to be used for the duration of the time to complete their respective degree.

## Course Objectives

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

1. Manage and maintain computer information systems security monitoring, intrusion detection, and crisis management.
2. Configure and manage alarm management, signature configuration, sensor configuration, and troubleshoot components.
3. Identify, resolve, and document network crises and activate the response team.

## Course Outline

1. **MODULE 1. ETHICAL HACKING OVERVIEW**
    a. Introduction to Ethical Hacking
    b. What You Can Do Legally
    c. What You Cannot Do Legally
2. **MODULE 2. TCP/IP CONCEPTS REVIEW**
    a. Overview of TCP/IP
    b. IP Addressing
    c. Overview of Numbering Systems
3. **MODULE 3. NETWORK AND COMPUTER ATTACKS**
    a. Malicious Software (Malware)
    b. Protecting against Malware Attacks
    c. Intruder Attacks on Networks and Computers
    d. Addressing Physical Security
4. **MODULE 4. FOOTPRINTING AND SOCIAL ENGINEERING**
    a. Using Web Tools for Footprinting
    b. Conducting Competitive Intelligence
    c. Using Domain Name System Zone Transfers
    d. Introduction to Social Engineering
5. **MODULE 5. PORT SCANNING**
    a. Introduction to Port Scanning
    b. Using Port-Scanning Tools
    c. Conducting Ping Sweeps
    d. Understanding Scripting
6. **MODULE 6. ENUMERATION**
    a. Introduction to Enumeration
    b. Enumerating Windows Operating Systems
    c. Enumerating *nix Operating System
7. **MODULE 7. PROGRAMMING FOR SECURITY PROFESSIONALS**
    a. Introduction to Computer Programming
    b. Learning the C Language
    c. Understanding HTML Basics
    d. Understanding Perl
    e. Understanding Object-Oriented Programming Concepts
    f. Understanding Python
    g. An Overview of Ruby
8. **MODULE 8. DESKTOP AND SERVER OS VULNERABILITIES**
    a. Windows OS Vulnerabilities
    b. Tools for Identifying Vulnerabilities in Windows
    c. Best Practices for Hardening Windows Systems
    d. Linux OS Vulnerabilities

9. **MODULE 9. EMBEDDED OPERATING SYSTEMS: THE HIDDEN THREAT**
    a. Introduction to Embedded Operating Systems
    b. Windows and Other Embedded Operating Systems
    c. Vulnerabilities of Embedded OSs
10. **MODULE 10. HACKING WEB SERVERS**
    a. Understanding Web Applications
    b. Understanding Web Application Vulnerabilities
    c. Tools for Web Attackers and Security Testers
11. **MODULE 11. HACKING WIRELESS NETWORKS**
    a. Understanding Wireless Technology
    b. Understanding Wireless Network Standards
    c. Understanding Authentication
    d. Understanding Wardriving
    e. Understanding Wireless Hacking
12. **MODULE 12. CRYPTOGRAPHY**
    a. Understanding Cryptography Basics
    b. Understanding Symmetric and Asymmetric Algorithms
    c. Understanding Public Key Infrastructure
    d. Understanding Cryptography Attacks
    e. Understanding Password Cracking
13. **MODULE 13. NETWORK PROTECTION SYSTEMS**
    a. Using Network Protection Systems
    b. Protecting with Firewalls
    c. Protecting with Intrusion Detection and Prevention Systems
    d. Using Honeypots

## Grade Scale

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

## Course Evaluation

Final grades will be calculated according to the following criteria:

| | |
|---|---|
| Labs | 30% |
| Practice Questions | 10% |
| Tests | 30% |
| Final Exam | 30% |

## Course Requirements

1. Demonstrate proficiency through hands-on labs as assigned.
2. Completion of Study Guides as assigned.

## Course Policies

1. No food, drinks, or use of tobacco products in class.
2. Electronic devices not being used for the class, such as phones and headphones, must be turned off while in class. Any device usage during class may result in a deduction of points on an assignment or test.
3. Do not bring children to class.
4. Certification: If s student passes the certification test that is associated with this class you will receive an "A" on the final exam and credit for 25% of your labs. If you have missed a previous test you must still take the final exam to substitute for that grade.
5. 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.
6. If you wish to drop a course, the student is responsible for initiating and completing the drop process. If you stop coming to class and fail to drop the course, you will earn an 'F' in the course.
7. Tools: Return all tools and/or software to their designated place.
8. A grade of 'C' or better must be earned in this course for credit toward degree requirement:
9. Additional course policies, as defined by the individual course instructor, will be outlined in the course addendum and provided by the instructor.

## 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) 839-2018. You may also visit the online resource at Special Populations - Lamar Institute of Technology (lit.edu).

## Technical Requirements (for courses using Blackboard)

The latest technical requirements, including hardware, compatible browsers, operating systems, software, Java, etc. can be found online at:

https://help.blackboard.com/Learn/Student/Getting_Started/Browser_Support/Browser_Checker.

A functional broadband internet connection, such as DSL, cable, or Wi-Fi is necessary to maximize the use of the online technology and resources.

## 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 log in 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.

For more information: https://www.lit.edu/student-success/starfish

## 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 or obtained in print upon request at the Student Services Office. Please note that the online version of the LIT Catalog and Student Handbook supersedes all other versions of the same document.

## Certification Requirement

CNTT 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)