**University of Texas at Tyler**
**Soules College of Business**
**Department of Computer Science**
**COSC 4362 Cyber Security**

***Subject to Change***

## Course Information

**COSC 4362** Cyber Security Fall 2025
This is a fully online course. No in-person or zoom meetings.

## Instructor Contact

Instructor: Sara Memarian Esfahani
Office location: COB 315.04
Zoom Meeting ID: TBA
Office hours: Tuesdays and Thursdays 9:00 to 11:00, and 2-3 pm or on Zoom by appointment
Email: Use the Inbox in Canvas (MUST include COSC 4362 in the Subject Line)
Normally, I will reply to an email within 24 to 48 hours.
To ensure a quick response over the weekends, please email me no later than Friday mornings.
Occasionally I will be unable to respond within that time frame but will inform the class in advance.

## Communication Expectations

The most convenient way to communicate with the instructor is through the Inbox in Canvas. Download the mobile app for your convenience.

**Discussion Board Communication**

Please post general course or assignment questions to the General Course Questions & Answers Discussion Topic. Students are encouraged to respond to their fellow classmates' questions. I will read all discussion postings and add comments/suggestions/questions as necessary to keep the discussion on topic. Specific topic instructions on discussions are provided in the forums when needed.

**Canvas Notifications:**

Receive instant notifications about course events, such as submissions, discussion messages, and announcements through canvas. Assignments and all deliverables will be graded and returned no later than one week after the due date.

## About the Professor/Instructor

Welcome to COSC 4362 Cyber Security. I am Sara Memarian Esfahani, the instructor for this course. I am excited to have you in this course and look forward to learning more about you and your academic career goals while at UT Tyler. Together we will explore a variety of topics within security issues related to information and organizational assets and we will journey through this course together to do great things.

## Course Description

This course is designed to give students an understanding of computer security concepts. You are advised to pay careful attention to the class lectures and course exercises. Exam questions are based primarily on the material covered in class and are designed to test your understanding of the underlying concepts of computer security. It also covers information security management and much of the common Body of Knowledge of the CAMPTIA Security+ Certification Exam.

## Course Structure

This is a fully online course. No in-person or zoom meetings. All the course material will be delivered via Canvas. See the course schedule table at the end of this file and on Canvas.

**Course Objectives**

Upon successful completion of this course, you are expected to:

- Become familiar with the foundational concepts in security design.
- Become familiar with the principles of legal and ethical aspects of security design.
- Become familiar with principle of cryptography, various techniques and pros and cons of each method.
- Learn how to identify variety threats and attacks.
- Gain hands-on experience in a practical team-based project to implement your take aways of security principles.

**Course Topics**

**Domain 1: General Security Concepts**

1. Introduction to Cybersecurity & Security+ Certification
2. Core Security Principles: CIA & DAD Triads, Controls, Policies
3. Threat Landscape & Attack Vectors
4. Malware & Common Threats
5. Social Engineering & Human-Centric Attacks

---

**Domain 2: Threats, Vulnerabilities & Mitigations**

6. Vulnerability Management & Scanning
7. Penetration Testing & Red Team Concepts
8. Application Security & Secure Coding Practices
9. Endpoint Security & OS/IoT Hardening
10. Network Security: Secure Architecture, Segmentation & Zero Trust
11. Wireless and Mobile Security
12. Cryptography & PKI (Encryption, Hashing, Digital Signatures)

---

**Domain 3: Security Architecture**

13. Identity and Access Management (IAM)
14. Cloud & Virtualization Security
15. Security Monitoring, SIEM, and Logging
16. Security Automation & Scripting Basics

---

**Domain 4: Incident Response & Digital Forensics**

17. Incident Response Planning & Playbooks
18. Digital Forensics Fundamentals (Preservation, Collection, Chain of Custody)

---

**Domain 5: Governance, Risk & Compliance**

19. Risk Management & Business Continuity
20. Security Governance, Laws, Frameworks (e.g., NIST, ISO, GDPR)
21. Security Awareness, Training, and Personnel Management

### Required Materials

CompTIA Security+ Study Guide with over 500 Practice Test Questions: Exam SY0-701 (9th Edition)

Authors: Mike Chapple, David Seidl

ISBN: 978-1-394-21142-5

Link to purchase the book: https://www.wiley.com/en-us/CompTIA+Security%2B+Study+Guide+with+over+500+Practice+Test+Questions%3A+Exam+SY0-701%2C+9th+Edition-p-9781394211418

## Hardware & Software Requirements for course

- Personal Computer (PC)
- Lockdown Browser and Respondus Monitor
  - A working Webcam for Respondus Monitor (no exceptions). This camera may be on your laptop or an external camera. A working webcam is required to take all exams and some quizzes. This is non-negotiable.
  - Exams require the use of Respondus Lockdown Browser and Monitor. Therefore you need to download  Lockdown browser software (Links to an external site.)
  - Canvas. The course uses Canvas for communication between the instructor and students and among students.

This course will also utilize **Professor Messer's CompTIA Security+ (SY0-701) YouTube videos** as a supplemental learning resource. These videos are concise, well-aligned with the certification objectives, and are freely available. Students are strongly encouraged to watch the relevant videos each week to reinforce lecture topics and exam preparation.

You can access the full playlist here: https://www.youtube.com/@professormesser
*(Note: This is not a required material but is highly recommended for success on the Security+ certification exam.)*

## COURSE REQUIREMENTS AND GRADING:

Your grade will be determined based on your performance on the activities identified below. No make-up for exams, simulations, or homework will be given. It is highly likely that "extra-credit work" will be assigned to individuals as a replacement for, or in addition to, these components. All points will show up in Canvas. Be sure to review the grading schema below to determine your letter grade.

**Individual Assignments**: Weekly reading of the assigned chapter for each week. Also each week there will be lab assignments that are designed for you to gain hands on experience.

Lab assignments are free, browser-based, and designed for beginner to intermediate learners. The 3 main online labs that we will use in this class are:

- TryHackMe
- LabEx
- Cybrary

**Lab Platforms Access**: Students are required to create free accounts on the mentioned platforms in order to complete hands-on lab assignments throughout the semester:

Please ensure you register using your full name and keep login credentials secure. You will receive specific lab instructions and links during each week of the course.

## EXAMS:

There will be two exams during the semester. You will be tested on all material assigned or taught in this course which includes class slides, quizzes, videos, etc. Respondus Lockdown Browser & Monitor is required to take all exams which require a webcam feature. Instructions are posted on canvas.

** Students who pass CompTIA Security+ by semester's end can earn up to +5% extra credit or replace the final exam score.

**GRADE CRITERIA:** All course work is always due at 11:59 p.m., unless otherwise noted. If you have not finished your projects, submit whatever you have completed. You will earn credit for what you complete.

| **Assignments (Subject to change)** | **Points Possible (Approx.)** |
|---|---|
| Class Quizzes (12) | 240 |
| Lab Assignments (12) | 240 |
| Discussion Participation (12) | 120 |
| Midterm Exam | 150 |
| Final Exam | 200 |
| Weekly Progress / Canvas Check-ins | 50 |
| CompTIA Security+ Certified | Waives Final exam |
| **Total Points Possible with no extra credit** | **1000** |

| **Total Points (%)** | **Letter Grade** |
|---|---|
| 900 & above | A |
| 800 - 899 | B |
| 700 - 799 | C |
| 600 - 699 | D |
| 599 & below | F |

*Schedule (subject to change)*
*All Assignments are Due by Friday 11:59 p.m. unless otherwise noted*

| **Week** | **Date** | **Topic / Reading** | **CompTIA Security+ Domain** | **Assignments and Quizzes** |
|---|---|---|---|---|
| Week 1 | Aug 25-29 | Introduction to Cybersecurity & CIA Triad<br>Reading: Chapter 1 | Domain 1: General Security Concepts | • Understanding the Syllabus<br>• Introduce Yourself<br>• TryHackMe: Pre-Security (Lab) |
| Week 2 | Sep 1-5 | Threat Actors & Common Attacks<br>Reading: Chapter 2 | Domain 2: Threats & Vulnerabilities | • TryHackMe: Threats & Attacks,<br>• LabEx: Phishing |
| Week 3 | Sep 8-12 | Social Engineering & Malware<br>Reading: Chapter 3 & 4 | Domain 2 (continued) | • TryHackMe: Social Engineering,<br>• LabEx: Malware |
| Week 4 | Sep 15-19 | Secure Network Architecture<br>Reading: Chapter 12 | Domain 3: Security Architecture | • TryHackMe: Network Security,<br>• LabEx: Segmentation |
| Week 5 | Sep 22-26 | Secure Protocols & Wireless Security<br>Reading: Chapter 12 & 13 | Domain 3 (continued) | • TryHackMe: Wi-Fi Hacking Fundamentals,<br>• LabEx: Secure Protocols |
| Week 6 | Sep 29-3 | Identity & Access Management (IAM)<br>Reading: Chapter 8 | Domain 3 (continued) | • TryHackMe: IAM,<br>• LabEx: RBAC |
| Week 7 | Oct 6-10 | Midterm Review Exam | Review Chapters: 1–4, 8, 12–13 | • Lockdown Browser Required |

| | | | | |
|---|---|---|---|---|
| Week 8 | Oct 13-17 | Endpoint Security & Device Hardening<br>Reading: Chapter 11 | Domain 3 (continued) | • TryHackMe: Endpoint Protection,<br>• LabEx: Nmap test lab |
| Week 9 | Oct 20-24 | Cloud Security & Shared Responsibility<br>Reading: Chapter 10 | Domain 3 (continued) | • TryHackMe: Intro to Cloud Security,<br>• LabEx: Cloud Security Basics |
| Week 10 | Oct 27-31 | Security Monitoring & SIEM<br>Reading: Chapter 14 | Domain 4 | • TryHackMe: SOC Level 1,<br>• LabEx: Log Analysis Tools |
| Week 11 | Nov 3-7 | Incident Response & Digital Forensics<br>Reading: Chapter 14 & 15 | Domain 4 (continued) | • TryHackMe: Incident Response,<br>• LabEx: Forensics Basics |
| Week 12 | Nov 10-14 | Risk Management & Business Continuity<br>Reading: Chapter 17 | Domain 5 | • TryHackMe: Risk Management,<br>• LabEx: BIA/DRP Lab |
| Week 13 | Nov 17-21 | Security Governance, Laws & Frameworks<br>Reading: Chapter 16 | Domain 5 (continued) | • Cybrary: Compliance & Frameworks |
| Week 14 | 24-28 | Thanksgiving- Holiday | - | No Class Meeting |
| Week 15 | Dec 1-5 | Final Review & Certification Prep | All Domains | • Mock Exam, Self-Check |
| Week 16 | Dec 10 | Final Exam<br>Cumulative | All Domains | • Security+ Proof of certification |

## UT Tyler Student Resources

- UT Tyler Writing Center: Provides support for writing assignments and skill development. Contact: (903) 565-5995 | writingcenter@uttyler.edu
- UT Tyler Tutoring Center: Offers tutoring across various subjects to support academic success. Contact: (903) 565-5964 | tutoring@uttyler.edu
- Mathematics Learning Center (RBN 4021): An open-access computer lab for math students with tutors available to assist in early-career math courses.
- UT Tyler Counseling Center: Provides confidential counseling and support services for students. Contact: (903) 566-7254

## Code of Conduct and Ethics

Disciplinary actions may be taken against any student involved in academic dishonesty, which includes but is not limited to cheating, plagiarism, collusion, or submitting work that is wholly or partially the work of another person. Engaging in any act intended to provide an unfair academic advantage or attempting such actions is prohibited.

Cheating includes but is not limited to:

- Copying from another student's test or assignment.
- Using unauthorized materials during a test.
- Failing to follow instructions given by the test administrator.
- Possessing unauthorized materials, such as notes or textbooks, during an exam.
- Stealing, buying, or soliciting test materials or answers.

- Collaborating with or seeking help from others during a test without permission.
- Discussing exam content with students who have yet to take the test.
- Revealing exam questions when instructed to keep them confidential.
- Substituting for another person in a test or coursework.
- Offering money or coercing others to obtain test materials.
- Falsifying research data, lab results, or academic work for credit.
- Damaging or misplacing university property to gain academic advantage.
- Providing false information, such as grades or achievements, for personal gain or to harm others.
- Plagiarism includes but is not limited to:
    - Using someone else's work without proper citation and presenting it as your own.
    - Buying, receiving, or obtaining academic work and submitting it for credit.
- Collusion includes but is not limited to:
    - Collaborating with others on assignments without authorization.
    - Working with others to violate academic integrity policies.
- All submitted written work will be subject to plagiarism detection software review.

The instructor will post both UNOFFICIAL grade reports using Canvas.

**THREE BEFORE ME RULE**: If you have any issues or questions about assignments, class policies and schedules, etc. and want to speak with me (the Professor), please remember the three before me rule as stated in the next sentence. You must have attempted at least three options before you come to me. For example: TA, tutor, grader, etc. You must tell me what you tried and the results, including screen prints of errors or printed error messages

I have read and understood the contents of this course syllabus and agree to abide by its terms and expectations.

Name:------------------------- Date:-------------------- Sign:----------------------