1University of Texas at Tyler
Soules College of Business
Department of Computer Science
CSCI 4362-5362 Ethical Hacking

Subject to Change

Course Information

CSCI 4362-5362 Ethical Hacking Fall 2024
Class Meetings will be in-person on Tuesdays 17:30-18:50, COB 211
Please note that all Thursday classes are online via Zoom, unless otherwise mentioned.

Instructor Contact

Instructor: Sara Memarian Esfahani
Office location: COB 315.04
Zoom Meeting ID: TBA
Office hours: Tuesdays and Thursdays 12:00 to 14:00 or on Zoom by appointment
Email: Use the Inbox in Canvas (MUST include **CSCI 4362-5362** Ethical Hacking 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 **CSCI 4362-5362** Ethical Hacking. 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 class is designed to provide students an insight into the current security scenario and increasing hacking attempts on various information systems. The goal of ethical hacking and countermeasures is to help organizations take preemptive measures against malicious attacks by attacking their own system while staying within legal limits.

Course Structure

This course is a Hybrid course that lasts 15 weeks (1 semester). See the course schedule table at the end of this file and on Canvas.

Course Objectives

Students who successfully complete this class will be able to do the following:

1. Assess the ethical and legal requirements of security assessment and penetration testing and determine a strategy to comply with these requirements.
2. Analyze different phases of hacking and recommend a strategy to use ethical hacking for assessing the security of various components of an information system.
3. Compare and contrast different hacking techniques and analyze the legal implications of hacking.
4. Examine different vulnerabilities, threats, and attacks to information systems and recommend the countermeasures.
5. Analyze cryptography algorithms and encryption techniques and design the implementation strategies for securing information.
6. Compare and contrast various network security assessment and hacking tools. 7. Assess various network security techniques and tools and then implement an appropriate level of information security controls based on evidence, information, and research.

Course Topics

1. Introduction to Ethical Hacking
2. Footprinting and Reconnaissance
3. Scanning Networks
4. Enumeration
5. Vulnerability Analysis
6. System Hacking
7. Malware Threats
8. Sniffing
9. Social Engineering
10. Denial-of-Service
11. Session Hijacking
12. Evading IDS, Firewalls, and Honeypots
13. Hacking Web Servers
14. Hacking Web Applications
15. SQL Injection
16. Hacking Wireless Networks
17. Hacking Mobile Platforms
18. Hacking IoT and OT (Operational Technology)
19. Cloud Computing
20. Cryptography

Required Materials

- Lab access purchase from EC-council. More information will be provided in the class during the introductory session.

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. All the students are expected to come to class with questions.

Team Projects: Each student will participate in a systems analysis and Security design project as a team member. The objective of the project is to give students hands-on experience of security analysis and through such in-depth analysis and research, the teams will present their findings and offer mitigation strategies, simulating a somehow actual consultancy role in the cybersecurity landscape.

Team: Each team will consist of up to 5 members. It is the responsibility of individual students to find colleagues to work with as a team. Once a team is formed, each member has obligation to stay and function as a productive team member until the completion of the project. Any disputes, conflicts, and problems within a team must first be resolved among the members.
Each team will elect a team leader who will be responsible for coordinating various project tasks and communicating with the instructor. You may also elect or assign different titles to team members, reflecting different duties and specializations. The performance of a team will always be graded as a single unit. However, individual members will receive an adjusted grade at the end of the semester, which reflects the level of contribution as assessed by peers.

EXAMS: There will be three 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.

CLASS QUIZZES, ATTENDANCE, AND PARTICIPATION

Regular and punctual attendance for the full class period is expected. Attendance will be recorded. You must attend the entire class to avoid being recorded absent. Any student whose absences exceed the equivalent of two weeks of the class without proper notice may be dropped by the instructor with a WF for nonattendance.
You are expected to come to class prepared. That means you will need to read the assigned chapters and other materials before coming to class and be fully prepared to actively engage in discuss with the class. Friday classes will occur via zoom, and are focused on the review of the week, it can be in a form of pop-up quiz or Q&A.

If you find that there is no grade recorded for submitted work, or if you want to dispute a grade, you must send your instructor an email about the problem NO LATER THAN 2 DAYS after the submission date.

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.

No.	Assessment	Points per Item	Total Points	Details
1	Course Discussion Threads	10 threads x 4 pts	40 pts	There are 10 discussion threads (each worth 4 pts).
2	Assignments from Reading	20 assignments x 4 pts	80 pts	There are 20 assignments from reading (each assignment is worth 4 pts).
3	Lab Assignments	20 labs x 4 pts	80 pts	There are 20 lab assignments (each worth 4 pts).
4	Course Quizzes	50 questions x 1 pt	50 pts	There are 50 quiz questions (each worth 1 pt).

No.	Assessment	Points per Item	Total Points	Details
5	Research Project	1 project x 50 pts	50 pts	There is 1 research project (worth 50 pts).
6	Midterm Exam	1 exam x 100 pts	100 pts	Midterm exam worth 100 pts.
7	Final Exam	1 exam x 100 pts	100 pts	There is 1 final exam (worth 100 pts).

	Quality Points Earned	Comments
A	4.0	Superior Attainment of Course Outcomes
B	3.0	Good Attainment of Course Outcomes
C	2.0	Acceptable Attainment of Course Outcomes
D	1.0	Poor Attainment of Course Outcomes
F	0.0	Nonattainment of Course Outcomes

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

Week	Modules Covered	Objectives	Assessments
Week 1	Introduction	Overview of the syllabus, course objectives, expectations, and assessments. Introduction to Ethical Hacking concepts. Discussion on ethical and legal implications of hacking.	None
Week 2	Module 01: Introduction to Ethical Hacking Module 02: Footprinting and Reconnaissance	1. Assess the ethical and legal requirements of security assessment and penetration testing. 2. Analyze different phases of hacking. 3. Compare and contrast different hacking techniques. 4. Examine vulnerabilities and recommend countermeasures.	- Discussion Thread: Importance of competitive intelligence (4 pts) - Readings: Chapters 1 & 2 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 3	Module 03: Scanning Networks Module 04: Enumeration	1. Analyze different phases of hacking. 2. Compare and contrast hacking techniques. 3. Examine vulnerabilities and recommend countermeasures.	- Discussion Thread: OS banner grabbing and target system OS identification (4 pts) - Readings: Chapters 3 & 4 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 4	Module 05: Vulnerability Analysis	1. Assess ethical and legal requirements. 2. Analyze hacking phases. 3. Compare hacking techniques.	- Discussion Thread: Steganography methods comparison (4 pts) - Readings: Chapter 5 (8 pts)

Week	Modules Covered	Objectives	Assessments
	Module 06: System Hacking	4. Examine vulnerabilities and recommend countermeasures.	- Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 5	Module 07: Malware Threats Module 08: Sniffing	1. Analyze hacking phases. 2. Compare hacking techniques. 3. Examine vulnerabilities and recommend countermeasures. 4. Compare network security tools.	- Discussion Thread: Countermeasures for malware threats (4 pts) - Readings: Chapters 2 & 3 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 6	Module 09: Social Engineering Module 10: Denial-of-Service	1. Compare hacking techniques. 2. Examine vulnerabilities and recommend countermeasures. 3. Compare network security tools. 4. Assess security techniques and implement controls.	- Discussion Thread: Countermeasures for social engineering (4 pts) - Readings: Chapters 4 & 5 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 7	Module 11: Session Hijacking Module 12: Evading IDS, Firewalls, and Honeypots	1. Assess ethical and legal requirements. 2. Compare hacking techniques. 3. Examine vulnerabilities and recommend countermeasures.	- Discussion Thread: Role of honeypots (4 pts) - Readings: Chapters 1 & 2 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 8	**Midterm Exam**	Covers Modules 1-12.	Midterm Exam (100 pts)
Week 9	Module 13: Hacking Web Servers Module 14: Hacking Web Applications	1. Compare hacking techniques. 2. Examine vulnerabilities and recommend countermeasures.	- Discussion Thread: Methodology for web server attacks (4 pts) - Readings: Chapters 3 & 4 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 10	Module 15: SQL Injection Module 16: Hacking Wireless Networks	1. Compare hacking techniques. 2. Examine vulnerabilities and recommend countermeasures. 3. Analyze cryptography and encryption techniques.	- Discussion Thread: Consequences of SQL injection (4 pts) - Readings: Chapter 5 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 11	Module 17: Hacking Mobile Platforms Module 18: Hacking IoT and OT	1. Examine vulnerabilities and recommend countermeasures. 2. Compare network security tools. 3. Assess security techniques and implement controls.	- Discussion Thread: Securing mobile phones (4 pts) - Readings: Chapters 2 & 3 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)

Week	Modules Covered	Objectives	Assessments
Week 12	Module 19: Cloud Computing Module 20: Cryptography	1. Compare hacking techniques. 2. Examine vulnerabilities and recommend countermeasures. 3. Analyze cryptography and encryption techniques.	- Discussion Thread: Serverless computing vs. containers (4 pts) - Readings: Chapters 4 & 5 (8 pts) - Lab Assignments: 2 Labs (8 pts) - Quiz: 5 Questions (5 pts)
Week 13	**Review and Recap**	Review all modules and key concepts in preparation for the final exam.	None
Week 14	**Project Work**	In-depth analysis and project presentations on specific ethical hacking techniques.	Project Presentations
Week 15	**Final Exam**	Comprehensive exam covering all course material (100 pts).	Final Exam (100 pts)

Code of Conduct and Ethics

Academic integrity must be exhibited in your academic work, methods and conduct. Course work for which you receive an individual grade must be your original, individual effort. If any evidence exists of copying, cheating, or any other forms of academic dishonesty on all, or part, of your graded course work, you (and any others involved) will be awarded a ZERO for that work. Sharing files also counts as academic dishonesty. A second incident will result in a grade of an "F" in this course and a recommendation for further action by the office of the Vice President for Student Development.

A few key points to remember:

I would like to point out some of the activities we have sanctioned (awarded "F" grade and sometimes even more, removed from dean's list, merit list etc.). I want to share this so that you know that we careintegrity of the degree you receive from UT Tyler.

1. In one of the semesters, some exams were conducted using Respondus lockdown browser and video monitoring. However, some students took advantage of a loophole and had help from resources outside the screen and camera. Our instructors viewed 120 hours of video recording and found a group of students involved in a coordinated plagiarism. All were sanctioned, with some losing even scholarships!
2. In one instance, a student outsourced all his assignments to a person outside this country. The assignments were flagged for abnormal activities and with the help of some technology providers we were able to trace the IP address. The student was sanctioned (awarded a "F" grade in the course))
3. In multiple instances, students have had to borrow a laptop from another student in the course and posted something as them because they had not logged out of Canvas. This is considered misconduct on the part of both students. DO NOT give another student access to your UTTyler accounts.

Almost exams and quizzes have multiple versions, and the numbers and options are different. So, if you use your peer – the chance of choosing the wrong answer is extremely high. In worst cases (it has happened in some instances), the student would have used the numbers and details.

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.