The University of Texas at Tyler
Soules College of Business
Computer Science Department

CSCI 5363.060 – Malware Reverse Engineering
Spring Term 2025

Course Syllabus

Instructor Contact Information:

Name: Dr. Tim Nix
Office: COB 315.12
E-mail: tnix@uttyler.edu

***Course Description*:** This course provides an introduction to reverse engineering and malware analysis. Tools and techniques for safely examining a suspected malware executable in order to determine its capabilities will be used.

Prerequisite: None.

Required Textbook:

- *Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly; Author: Dennis Andriesse; Publisher: No Starch Press; December 2018; ISBN: 978-1593279127*

Selected Topics:

- Understanding x86 assembly and binaries (Week 01)
- The ELF and PE file formats (Week 02)
- Building a binary loader and basic binary analysis (Week 03)
- Disassembly, binary analysis, and code injection (Week 04)
- Customizing disassembly and binary instrumentation (Week 05)
- Dynamic taint analysis (Week 06)
- Symbolic execution (Week 07)

Grading Policy:

Reading Quizzes	30%
Homework Assignments	20%
Midterm Exam	20%
Final Exam	30%
Total:	**100%**

Office Hours: Emails will be answered within 24 hours Monday – Thursday. Emails received before 12:00 PM on Friday will be answered within 24 hours. Emails received after 12:00 PM on Friday will be answered the following Monday. If more help is needed than can be provided via email, then please request a Zoom meeting.

Course Mode: Course will be asynchronous, meaning that there are no scheduled lecture times. All assignments, including exams will be made available for a duration of time (typically, one week) in which it must be completed.

Grading Rubric:

Letter Grade	Assigned Score (s)	Definition
A	$90\ \% \leq s$	Mastery
B	$80\ \% \leq s < 90\ \%$	Good Understanding
C	$70\ \% \leq s < 80\ \%$	Adequate
D	$65\ \% \leq s < 70\ \%$	Probably Failed to Demonstrate
F	$s < 65\ \%$	Definitely Failed to Demonstrate

Reading Quizzes: Each week, a reading selection will be assigned along with a corresponding reading quiz. You will have one week from the assignment of the reading quiz until it is due. Reading quizzes are made available on each Sunday at 12:00 AM and due at 11:59 PM on the following Sunday; thus, you have 8 days to complete the reading quiz. You can take the reading quiz at any time during those 8 days as long as it is completed before the due date/time. However, once you begin the reading quiz, you will only have 90 minutes to complete it. There is a reading quiz each week (total of 7) and they constitute 30% of the overall course grade.

Homework Assignments: Homework assignments will focus on practical skills and applications. You will have one week from the assignment of the homework assignment until it is due. Homework assignments are made available on Sunday at 12:00 AM and due at 11:59 PM on the following Sunday; thus, you have 8 days to complete it. There will be, at most, one homework assignment per week (there will not be a homework assignment every week). Homework assignments are worth 20% of the overall course grade.

Exams: There will be one mid-term exam and a final exam. Both exams are comprehensive. The midterm exam will be given during Week 4 and the final exam will be given during Week 7. Each exam will be made available on Sunday at 12:00 AM and due at 11:59 PM on the following Sunday of its assigned week; thus, you have 8 days to complete the exam. You can take the exam at any time during those 8 days as long as it is completed before the due date/time. However, once you begin the exam, you will only have 120 minutes to complete it. The mid-term exam is worth 20% of the overall course grade and the final exam is worth 30% of the overall course grade.

Tentative Topic Schedule:

Week	Topic
Jan 12 – Jan 19	x86 Assembly Language / C Compilation / Anatomy of a Binary
Jan 19 – Jan 26	The ELF Format / The PE Format
Jan 26 – Feb 02	Binary Loading / Basic Binary Analysis
Feb 02 – Feb 09	Disassembly / Analysis Methods / Code Injection Techniques
Feb 09 – Feb 16	Custom Disassembly / Binary Instrumentation
Feb 16 – Feb 23	Dynamic Taint Analysis
Feb 23 – Mar 02	Symbolic Execution

Late Policies: All homework assignments are due on the date/time specified in the assignment. Assignments will not be accepted after that time. Any assignment submitted late will receive a grade of zero.

Any assignment submitted late will receive a grade of zero.

Academic Dishonesty: Representation of other's work as your own will not be tolerated and this includes AI-generated content. Cheating on examinations, quizzes, and homework and the false representation of work will be interpreted as academic dishonesty. Academic dishonesty will be subject to disciplinary action as outlined by the UT Tyler Student Guide on Conduct and Discipline.

Evidence of academic dishonesty will result in automatic failure of the course.

AI is not permitted in this course at all: I expect all work students submit for this course to be their own. Doing your own work, without human or artificial intelligence assistance, is best for your efforts in mastering course learning objectives. For this course, I expressly forbid using ChatGPT or any other artificial intelligence (AI) tools for any stages of the work process, including brainstorming. Deviations from these guidelines will be considered a violation of UT Tyler's Honor Code and academic honesty values.

EXPECTATIONS OF STUDENTS:

- **Take ownership of your learning.** You are solely responsible for how much you get out of this course. It is not my responsibility to spoon-feed knowledge to you, but rather to guide you along your developmental path. I hope that this course will challenge you. Deep learning happens when you struggle and succeed.

- **Seek my help early if you feel lost.** If you are doing the readings, and attempting the assignments, and yet you still feel lost, do not convince yourself that things will get better on their own or that you will catch up this weekend. This course, like most others, builds on itself throughout the semester. Contact me before the feelings of confusion compound.

COURSE PARTICIPATION:

If you have not turned-on notifications, I highly recommend you do. Look on the right-hand side of the class home page and you will see a notification button. Click on it and make sure notifications are turned on. To be successful in this online class, you need to be engaged with the materials. You should sign into Canvas several times a week and real all announcements and emails.

TECHNOLOGY STATEMENT:

To be successful om this online course you will need regular access to a computer and a stable Internet connection. While mobile devices are great for checking your grades or watching a video, relying on them as your primary method for taking an online course is not a good idea. Internet or computer issues are not a valid excuse for late or missing assignments.

If you have any problems accessing Canvas, or any other technical issues, contact the 24/7 Canvas Support (you need to be logged into Canvas to access it). You can also contact UT Tyler IT Support at itsupport@uttyler.edu.

UNIVERSITY POLICIES

UT Tyler Honor Code – Every member of the UT Tyler community joins together to embrace: Honor and integrity that will not allow me to lie, cheat, or steal, nor to accept the actions of those who do.

Student Standards of Academic Conduct – Disciplinary proceedings may be initiated against any student who engages in scholastic dishonesty, including, but not limited to, cheating, plagiarism, collusion, the submission for credit of any work or materials that are attributable in whole or in part to another person, taking

an examination for another person, any act designed to give unfair advantage to a student or the attempt to commit such acts.

“Cheating” includes, but is not limited to:

- copying from another student’s test paper or homework assignment;
- using, during a test, materials not authorized by the person giving the test;
- failure to comply with instructions given by the person administering the test;
- using, buying, stealing, transporting, or soliciting in whole or part the contents of an unadministered test, test key, homework solution, or computer program;
- collaborating with or seeking aid from another student during a test or other assignment without authority;
- discussing the contents of an examination with another student who will take the examination;
- divulging the contents of an examination, for the purpose of preserving questions for use by another, when the instructors has designated that the examination is not to be removed from the examination room or not to be returned or to be kept by the student;
- substituting for another person, or permitting another person to substitute for oneself to take a course, a test, or any course-related assignment;
- paying or offering money or other valuable thing to, or coercing another person to obtain an unadministered test, test key, homework solution, or computer program or information about an unadministered test, test key, home solution or computer program;
- falsifying any academic work offered for credit;
- taking, keeping, misplacing, or damaging the property of The University of Texas at Tyler, or of another person, if the student knows or reasonably should know that an unfair academic advantage would be gained by such conduct;
- misrepresenting facts, including providing false grades or resumes, for the purpose of obtaining an academic or financial benefit or injuring another student academically or financially; and
- use of any AI-generated content.

Unless otherwise specified, all work submitted for a grade must be completed by yourself. You are not to submit another person’s work and claim it as your own. Plagiarism and/or collusion will result in disciplinary actions. To spare yourself accusations of plagiarism:

1. Do not show another student a copy of your work before it has been graded. The penalties for permitting your work to be copied are the same as the penalties for copying someone else’s work.
2. Do not leave printouts of your work where other students may pick them up.

State-Mandated Course Drop Policy – Students may withdraw (drop) from this course using the Withdrawal Portal. Withdrawing (dropping) this course can impact your Financial Aid, Scholarships, Veteran Benefits, Exemptions, Waivers, International Student Status, housing, and degree progress. Please speak with your instructors, consider your options, speak with your advisor, and visit the One-Stop Service Center (STE 230) or email enroll@uttyler.edu to get a complete review of your student account and the possible impacts to withdrawing. We want you to make an informed decision. UT Tyler faculty and staff are here for you and often can provide additional support options or assistance. Make sure to carefully read the implications for withdrawing from a course and the instructions on using the Withdrawal portal.

Incomplete Grade Policy: If a student, because of extenuating circumstances, is unable to complete all of the requirements for a course by the end of the semester, then the instructor may recommend an Incomplete (I) for the course. The "I" may be assigned in place of a grade *only when all of the following conditions are met:* (a)

the student has been making satisfactory progress in the course; (b) the student is unable to complete all coursework or final exam due to unusual circumstances that are beyond personal control and are acceptable to the instructor, and (c) the student presents these reasons before the time that the final grade roster is due. The semester credit hours for an Incomplete will not be used to calculate the grade point average.

The student and the instructor must submit an Incomplete Form detailing the work required and the time by which the work must be completed to their respective department chair or college dean for approval. The time limit established must not exceed one year. Should the student fail to meet all of the work for the course within the time limit, then the instructor may assign zeros to the unfinished work, compute the course average for the student, and assign the appropriate grade. If a grade has yet to be assigned within one year, then the Incomplete will be changed to an F, or NC. If the course was initially taken under the CR/NC grading basis, this may adversely affect the student's academic standing.

Grade Appeal Policy: Disputes regarding grades must be initiated within sixty (60) days from the date of receiving the final course grade by filing a Grade Appeal Form with the instructor who assigned the grade. A grade appeal should be used when the student thinks the final course grade awarded does not reflect the grades earned on assessments or follow the grading scale as documented in the syllabus. The student should provide the rationale for the grade appeal and attach supporting document about the grades earned. The form should be sent via email to the faculty member who assigned the grade. The faculty member reviews the rationale and supporting documentation and completes the instruction section of the form. The instructor should return the form to the student, even if a grade change is made at this level. If the student is not satisfied with the decision, the student may appeal in writing to the Chairperson of the department from which the grade was issued. In situations where there is an allegation of capricious grading, discrimination, or unlawful actions, appeals may go beyond the Chairperson to the Dean or the Dean's designee of the college from which the grade was issued, with that decision being final. The Grade Appeal form is found in the Registrar's Form Library.

Disability/Accessibility Services: In accordance with Section 504 of the Rehabilitation Act, Americans with Disabilities Act (ADA) and the ADA Amendments Act (ADAAA), the University of Texas at Tyler offers accommodations to students with learning, physical, and/or psychological disabilities. If you have a disability, including a non-visible diagnosis such as a learning disorder, chronic illness, TBI, PTSD, ADHD, or a history of modifications or accommodations in a previous educational environment, you are encouraged to visit https://hood.accessiblelearning.com/UTTyler/ and fill out the New Student application. The Student Accessibility and Resources (SAR) office will contact you when your application has been submitted and an appointment with the Assistant Director Student Accessibility and Resources/ADA Coordinator. For more information, including filling out an application for services, please visit the SAR webpage at https://www.uttyler.edu/disability-services, the SAR office located in the Robert Muntz Library, LIB 460, email saroffice@uttyler.edu, or call 903.566.7079."

Military Affiliated Students: UT Tyler honors the service and sacrifices of our military-affiliated students. If you are a student who is a veteran, on active duty, in the reserves or National Guard, or a military spouse or dependent, please stay in contact with your faculty member if any aspect of your present or prior service or family situation makes it difficult for you to fulfill the requirements of a course or creates disruption in your academic progress. It is important to make your faculty member aware of any complications as far in advance as possible. Your faculty member is willing to work with you and, if needed, put you in contact with university staff who are trained to assist you. The Military and Veterans Success Center (MVSC) has campus resources for military-affiliated students. The MVSC can be reached at MVSC@uttyler.edu or via phone at 903.565.5972.

Students on an F-1 Visa: To remain in compliance with Federal Regulations requirements, only one online course can count toward your full-time enrollment. Students are expected to be fully engaged and meet all requirements for the online course.

FERPA: UT Tyler follows the Family Educational Rights and Privacy Act (FERPA) as noted in University Policy 5.2.3. The course instructor will follow all requirements to protect your confidential information.