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.

Class Time
Online

Instructor Information
Christopher Shaw
Adjunct Lecturer, CS Dept.
cshaw@uttyler.edu

Office Hours
Virtual Office Hours: 8:30AM – 10:00AM; Wednesday
8:30AM – 10:00AM; Friday

Textbook Information
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

Course Objective
- Understanding x86 assembly and binaries
- The ELF and PE file formats
- Binary loader and basic binary analysis
- Disassembly, binary analysis, and code injection
- Customizing disassembly and binary instrumentation
- Dynamic taint analysis
- Symbolic execution

Computer Account Access
Students will need a Patriot account and password for computer access. This information can be found at https://www.uttyler.edu/ccs

Course Documents and Slides
This class will use Canvas for course documents, slides, quizzes and other class-related materials. Students are encouraged to check the website frequently during the course of the semester to keep up to date about course activity.

Course Grading

Course evaluation will be based on the following:

Grading Policy:

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

Grading Scale

A	85.0 points or more
B	70.0 to 84.999 points
C	55.0 to 69.999 points
D	40.0 to 54.999 points
F	39.999 points or less

Course Policies

1. ***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. Once you begin the reading quiz, you will only have 90 minutes to complete it. There is a reading quiz each week (total of 13) and they constitute 30% of the overall course grade.

2. ***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. 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.

3. ***Exams:*** There will be one mid-term exam and a final exam. Both exams are comprehensive. The midterm exam will be given during Week 8 and the final exam will be given during Week 15. 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. Exams are designed to measure the student's knowledge of the material as well as their ability to use these skills in an efficient manner. Examinations may consist of multiple-choice questions or application problems.

4. Make-up exams will be granted at the discretion of the instructor. Make-ups will be given only under extremely unusual circumstances, will be different from exams given during the regular class time and may be penalized up to 50% of the grade. *Permission for a makeup exam must be obtained* ***PRIOR*** *to the regular exam and must include written documentation of the student's absence.*

5. Missed Classes, Tests/Quizzes and Assignments – Students who miss class are responsible for getting missed materials and lecture information on their own time from their peers. Any tests/quizzes and/or assignments due during the student's documented absence will be due by 5pm of the day of their return with no penalty.

6. UT Tyler is committed to exploring and using artificial intelligence (AI) tools as appropriate for the discipline and task undertaken. We encourage discussing AI tools' ethical, societal, philosophical, and disciplinary implications. All uses of AI should be acknowledged as this aligns

with our commitment to honor and integrity, as noted in UT Tyler's Honor Code. Faculty and students must not use protected information, data, or copyrighted materials when using any AI tool. Additionally, users should be aware that AI tools rely on predictive models to generate content that may appear correct but is sometimes shown to be incomplete, inaccurate, taken without attribution from other sources, and/or biased. Consequently, an AI tool should not be considered a substitute for traditional approaches to research. You are ultimately responsible for the quality and content of the information you submit. Misusing AI tools that violate the guidelines specified for this course is considered a breach of academic integrity. The student will be subject to disciplinary actions as outlined in UT Tyler's Academic Integrity Policy. Refer to the About This Course section of the UT Tyler Syllabus Module for specific information on appropriate use of AI in your course(s).

Tentative Course Schedule and Assignments

Date	Concept	Assignments	Quiz
Jan 12-16	Introduction		
Jan 20-23	Anatomy of a Binary		Ch. 1
Jan 26-30	The ELF Format		Ch. 2
Feb 2-6	The PE Format	Ch. 3 Assignment	Ch. 3
Feb 9-13	Building a Binary Loader Using libbfd		Ch. 4
Feb 16-20	Basic Binary Analysis in Linux	Ch. 5 Assignment	Ch. 5
Feb 23-27	Disassembly and Binary Analysis Fundamentals		Ch. 6
Mar 2-6	Simple Code Injection Techniques for ELF & Mid-Term Exam		Ch. 7
Mar 9-13	SPRING BREAK!!!		
Mar 16-20	Customizing Disassembly	Ch. 8 Assignment	Ch. 8
Mar 23-27	Binary Instrumentation		Ch. 9
Mar 30-Apr 3	Principles of Dynamic Taint Analysis		Ch. 10
Apr 6-10	Practical Dynamic Taint Analysis with libdft	Ch. 11 Assignment	Ch. 11
Apr 13-17	Principles of Symbolic Execution		Ch. 12
Apr 20-24	Practical Symbolic Execution with Triton		Ch. 13
Apr 27-May 1	Final Exam		