CS 4177 - Fall 2023

Software Vulnerabilities

This course focuses on security issues and their remediation through the use of hands-on, practical exercises. Students will learn of the potential risks that accompany the use of networks, devices, and systems by using cyber security tools and techniques to uncover and analyze their inner workings. Students will learn to apply defenses and mitigations to alleviate risks.

Instructor:

- Dr. Jaime C. Acosta
  Office: Prospect Hall Rm 120
  Email: jcacosta@utep.edu

Class location and time:

The course code for CS4177 is CRN 13896
Class will be held in Prospect Hall Rm 234 on Thursdays from 3:00pm to 4:20pm.

Course materials:

Students are required to bring a laptop to every class to complete assignments, tests, and the course project. If this is an issue, please notify the professor.

This course does not require the purchase of a textbook; all resource material will be posted on the course website and/or Blackboard.

Course Policies:

- Homework assignments are due at the beginning of the class, unless specified otherwise.
- Assignments may be discussed with others, but solutions must be designed, written, and tested by you or, in the case of group assignments, by your group.
- No make-up exams or assignments will be given except under extreme conditions.
- It is the student's responsibility to independently cover any material missed.

Learning Outcomes:

Level 3: Synthesis and Evaluation (Level 3 outcomes are those in which the students can apply the material in new situations. This is the highest level of mastery.) Upon successful completion of this course, students will be able to:

- Analyze an active security incident, create a plan, and respond using dynamic and static analysis methods to create decoders and signatures for various malware and malicious activities.
- Understand a recreate novel training exercises, built using publicly available vulnerability information and virtualization technologies; that demonstrates analysis, planning, and response using publicly available tools.

Level 2: Application and Analysis (Level 2 outcomes are those in which the student can apply the material in familiar situations, e.g., can work a problem of familiar structure with minor changes in the details.) Upon successful completion of this course, students will be able to:

- Become familiar with vulnerability analysis tools, including IDA Pro, Ghidra, and Dshell, and to understand under which circumstances they are best suited.
- Explain how adversaries can identify vulnerabilities and generate exploits for public and private software systems.
- Detect data exfiltration activities and conduct detailed analysis to describe the malignant logic and potential impacts.

Level 1: Knowledge and Comprehension (Level 1 outcomes are those in which the student has been exposed to the terms and concepts at a basic level and can supply basic definitions.) The material has been presented only at a superficial level. Upon successful completion of this course, students will be able to:

- Understand what constitutes a vulnerability at the system, network, and host level.
- Become aware of processes that are used to document and host vulnerability information as well as mitigations.
- General understanding of various security analysis tools that are used to identify vulnerabilities as well as mitigations

Grades:

Assignments	50%
Tests	20%
Project	30%

Final letter grades will be assigned as follows:

A = 90% through 100%
B = 80% through 89%
C = 70% through 79%
D = 60% through 69%
F = Less than 60%

Submission of late work:

Unless otherwise noted, homework assignments are due at the beginning of class. Late work will be accepted at most two days late, unless specified by the instructor, and will be marked down two letter grades. After two days the assignment will not be accepted.

Graduate Students:

If you are a graduate student, you will have to complete an additional assignment as part of your course grade. You will select, read, and present a research paper that focuses on cybersecurity vulnerabilities and mitigations.

Standards of Conduct and Academic Dishonesty

You are expected to conduct yourself in a professional and courteous manner, as prescribed by the UTEP Standards of Conduct: https://www.utep.edu/student-affairs/osccr/student-conduct/
Academic dishonesty includes but is not limited to cheating, plagiarism and collusion. Cheating may involve copying from or providing information to another student, possessing unauthorized materials during a test, or falsifying data (for example program outputs) in laboratory reports. Plagiarism occurs when someone represents the work or ideas of another person as his/her own. Collusion involves collaborating with another person to commit an academically dishonest act. Professors are required to - and will - report academic dishonesty and any other violation of the Standards of Conduct to the Dean of Students.

When in doubt, please ask. On exams you must submit your own work and you may not give or receive help. On assignments you must submit your own work. Submissions that are "identical" will be considered as a clear evidence of cheating.

Students Needing Special Accommodations

In accordance with the UTEP procedure, if you need accommodations for equal access in this course, please do the followings:

- Contact Center for Accommodations and Support Services (CASS) at cass@utep.edu or by phone at (915) 747-5148 to verify your eligibility.
- Contact me before or at the beginning of the first class to discuss your individual needs for accommodations, with an official letter of accommodation or other documents.

COVID-19 Precaution Statement

Please stay home if you have been diagnosed with COVID-19 or are experiencing COVID-19 symptoms. If you are feeling unwell, please let me know as soon as possible, so that we can work on appropriate accommodations. If you have tested positive for COVID-19, you are encouraged to report your results to covidaction@utep.edu, so that the Dean of Students Office can provide you with support and help with communication with your professors. The Student Health Center is equipped to provide COVID-19 testing.

Ethics and Security Vulnerabilities:

During this course, you will learn skills used by professional security evaluators to identify and remediate vulnerabilities. Tampering with systems and exploiting vulnerabilities without written consent has severe consequences including academic suspension and legal prosecution and could prevent you from ever working in your field of study.

In two words: **Act Responsibly!**

Schedule:

	Topics Covered	Assignments
Week 1	Course Introduction and Overview	
Week 2	Command and Control (C2) Malware Communications Analyses	A. Network and Memory Dumps
Week 3		B. Static Reverse Engineering
Week 4		C. Network Dissectors
Week 5	C2 Examination	
Week 6	Project Development - Part 1	D. Idea Development
Week 7	Cyber Sandbox Development	E. Environment Creation
Week 8		F. Embedding/Testing Vulnerabilities
Week 9	Project Development - Part 2	G. Technology Identification
Week 10	Forensic Analysis using Dynamic Reverse Engineering	H. High- to Low-Level Source Code Analysis
Week 11		I. Passcodes Extraction
Week 12	Dynamic SRE Examination	
Week 13	Ransomware Analysis	J. WannaCry Analysis and Kill Switch
Week 14		K. WannaCry Key Recovery
Week 15	Project Demonstrations	