CS 4177

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.

Course Content:

Website: https://cssrvlab01.utep.edu/Classes/cs4177/ (VPN-access only)
Blackboard (through my.utep.edu)

Office Hours:

T 1pm-2pm on Zoom

Instructor:

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

Class location and time:

The course code for CS4177 is CRN 26431.
Class will be held virtually on Zoom on Thursdays from 4:30pm to 5:50pm.

Course materials:

Students are required to bring a laptop to every class.

This course does not require the purchase of a textbook; all resource material will be posted on the course website. Some of the material from this course will derive from the following books:

- Eldad Eilam, *Reversing: Secrets of Reverse Engineering*. Wiley, 2005.
- Stuart McClure, Joel Scambray, George Kurtz, *Hacking Exposed 7: Network Security Secrets and Solutions, Seventh Edition*. McGraw-Hill Osborne Media, 2012
- Michael Sikorski and Andrew Honig, *Practical Malware Analysis*. No Starch Press, 2012.

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.

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:

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.

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 assignments you must submit your own work. Submissions that are "identical" will be considered as a clear evidence of cheating.

Students with Disabilities

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 915-747-5148 or at CASS@utep.edu to verify your eligibility.
- Contact me at the start of the semester to discuss your individual needs for accommodations, with an official letter of accommodation or other documents.

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!**

Tentative Schedule: (may change as the semester progresses)

Decoding Malware Communication
• Uncovering malware communications (Wireshark and Volatility) • Reversing the encoding scheme (Ghidra) • Building a decoder (Dshell) • Test
Sandboxes and Innovation exercises
• Environment development (Kali Linux, Ubuntu, Metasploitable) • Project planning
Dynamic Reversing
• Create and reverse your own binary (IDA Pro) • Recover passcodes (IDA Pro debugger) • Automated reversing (Angr) • Test
Process Analysis
• Ransomware analysis and mitigation • Ransomware key recovery • Password security and deep memory analysis
Projects
• Presentations • Walkthroughs • Reports