COSC 5325-01/02 Operating System Security
Spring 2018

Instructor

Qingzhong Liu, Associate Professor, Department of Computer Science, Sam Houston State University
Office: AB1-216D Email: liu@shsu.edu Phone: (936) 294-3569

Course Description

This course will provide the rationale and necessity for a full range of security concepts and techniques and how to apply them to operating systems. The course will cover methodologies for the analysis of operating system security and forensic techniques, as well as the identification of best practices in the administration, testing and security for operating systems. Operating systems hacking behaviors will be exposed and penetration testing will be introduced in this class too.

Course Outline

- Introduction digital/cyber forensics
- Collecting and analyzing volatile data
- Windows memory analysis
- Registry analysis
- File analysis
- Executable File Analysis
- Rootkits and Rootkit Detection
- Timeline and application analysis
- Linux forensics
- Macintosh forensics
- Mobile forensics

IDEA Objective

Based on the Individual Development & Educational Assessment (IDEA), at the end of this course the ideal student should be able to present the following essential and important objectives:

1. **Gaining factual knowledge (terminology, classifications, methods, trends) regarding operating systems forensics and security**
2. **Learning to apply course materials/tools to analyze operating systems forensics and security.**

ABET Computing Educational Outcomes

Based on ABET computing educational outcomes, at the end of this course the ideal student should be able to present the following abilities (ABET outcome b, e, and i):

1. Analyze a problem, and identify and define the computing requirements appropriate to its solution;
2. An understanding of professional, ethical, legal, security and social issues and responsibilities;
3. Use current techniques, skills, and tools necessary for computing practice.

Textbooks

Books Reqested/Recommended	Author(s)	ISBN	Year	Publisher
Windows Forensic Analysis DVD Toolkit, 2nd Edition (XP, requested)	**Harlan Carvey**	**9781597494229**	**2009**	**Syngress**
System Forensics, Investigation, and Response, Third Edition	Chuck Easttom	9781284121841	2019	JBlearning
Operating System Forensics	Ric Messier	9780128019498	2015	Syngress
Windows Forensics Cookbook	Skulkin and Courcier	9781784390495	2017	Packt

Grading

Your grades will be determined according to the following:

Homework and hands-on assignments	50%
Exams	15%
Project	35%
Total	**100%**

Course letter grades will be assigned according to the following:

Total	Grade
>= 90%	A
80% <= TOTAL < 90%	B
70% <= TOTAL < 80%	C
60% <= TOTAL < 70%	D
TOTAL < 60%	F

Assignments
These are practical exercises aiming to help student understand the course material better (labs may be assigned as some homeworks). Details of lab instructions and requirements will be posted later on course website.

Project and Collaboration
Two or three students make a group (one student a group is allowable) and work on any topic in operating systems forensics or networking security at your interest. You may utilize the resources on the internet but must have your own findings/progress. All groups are requested to submit a report including the objective, backgrounds, methodology and results, and make a presentation on your project in the week before the final. All homework assignments must be completed by each student individually. Each team project must be completed by the members of the team only.

Late Policy
Penalty for late work is 10% of the worth per calendar day late, unless an extension has been granted in advance.

Academic Dishonesty
All students are expected to engage in all academic pursuits in a manner that is above reproach. Students are expected to maintain complete honesty and integrity in the academic experiences both in and out of the classroom. Any student found guilty of dishonesty in any phase of academic work will be subject to disciplinary action. The University and its official representatives may initiate disciplinary proceedings against a student accused of any form of academic dishonesty including, but not limited to, cheating on an examination or other academic work which is to be submitted, plagiarism, collusion and the abuse of resource materials.
Students should be aware, specifically, that the instructor reviews all programming assignments and exercises for evidence of collaborative work. While it is sometimes appropriate and encouraged for students to discuss concepts and ideas, it is never permissible to collaboratively work on coded examples, to share or swap completed or partially completed programming assignments. In addition it is not permitted for students to use code examples provided by the instructor without appropriate documentation/ citation of the use of that code.

Classroom Conduct
Students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. Cellular telephones and pagers must be turned off before class begins. Students are prohibited from eating in class, using tobacco products, making offensive remarks, reading newspapers, sleeping, talking at inappropriate times, wearing inappropriate clothing, or engaging in any other form of distraction. Inappropriate behavior in the classroom shall result in a directive to leave class. Students who are especially disruptive also may be reported to the Dean of Students for disciplinary action in accordance with university policy.

Americans with Disabilities Act
Students with disabilities covered by the Americans with Disabilities Act should go to the Counseling Center and Services for Students with Disabilities (SSD) in a timely manner to obtain the documentation required. Students are responsible for initiating the process of documenting the need for an accommodation under the ADA act.

Religious Observance
University policy allows for student to observe religious holy days, including travel time associated with visiting a holy site, without penalty. If you intend to miss class as a result of the observance of a religious holy day or as a result of the necessary traveling time required for religious observance, such an absence will not be penalized so long as you have notified the instructor in writing of the dates and times of class sessions that are missed. The deadline for notification is the 12 class day. Students absent from class as a result of religious observance are required to submit any due assignments immediately on their return to the classroom. Makeup tests and quizzes will also be provided on return to the class.