Department of Computer Science
Sam Houston State University

COSC 5330 Malware (Fall 2024)

COURSE DESCRIPTION:

Students are provided an in-depth approach to the identification and deconstruction of malicious software, including static and dynamic analyses, malware deconstruction, and rootkit elimination. The course requires the use of virtual machines to isolate live malware samples, and access to a high-speed internet connection.

Prerequisite: none.

Credits: 3 semester hours
Lecture: Online

Course Designation as Required, Elective, or Selected Elective: Required

INSTRUCTOR:

Mr. Kirk Burns
Office: Online
Email: lib_kab@shsu.edu
Phone: 936.689.1103
Website: https://profiles.shsu.edu/lib_kab

REQUIRED TEXTBOOKS:

Practical Malware Analysis
ISBN: **978-1593272906**

Learning Malware Analysis
ISBN: 9781788392501

RECOMMENDED TEXTBOOKS:

Malware Data Science: Attack Detection and Attribution
ISBN: 9781593278595

OTHER TOOLS

- Hypervisor, VirtualBox recommended (**REQUIRED)**
- High quality Internet capabilities. If you are running less than 50 Mbps you may experience problems.
- A modern (64 bit) home computer (desktop or laptop).
- Windows and Linux virtual machines. Either the VMs or an ISO so you can create the VMs will be provided.

COURSE OUTCOMES:

- Understand the internal structures, and functions of the most common forms of malware
- Develop a Virtual Malware Lab
- Forensically examine systems for malware
- Apply appropriate commercial and open-source tools for the defense of systems and networks against malware

COURSE SCHEDULE:

Will be posted in Blackboard with due dates and topic to be covered per week

COURSE REQUIREMENTS:

SHSU E-mails:
Students are required to check SHSU E-mails regularly as announcement and reminders will be sent to SHSU e-mails. Student personal email addresses will NOT be used for class communication.

Assignments:
Assignments will be a combination of weekly activities, grand challenges and a portfolio. Late submissions will **NOT** be accepted without a verifiable university approved reason. Graded homework with the instructor's comments will be uploaded on Blackboard usually within a week from the due date, and students are required to request correction(s) on grading within a week after each grade's posting. Make sure and check your grades regularly to meet these timelines.

Attendance:
In accordance with University Policy, regular attendance is required, and your attendance will be seriously monitored. For an online class the attendance will be monitored by access of Blackboard. You are responsible for all material covered in every class, regardless of whether you attended or not. It is your responsibility to obtain notes, assignments, etc., from fellow class members if you miss a class.

GRADING CRITERIA:

13 weekly activities @ 50 points each = 650
4 grand challenges @ 150 points each = 600
1 Semester Portfolio @ 250 points = 250

Grade

A	> 1349
B	1200 - 1349
C	1050 - 1199
F	< 1050

There are no exams in this course.

Course Topics:

- Techniques for the Lay Person. The Virtual Malware Lab
- Dynamic Analysis I
- X86 Architecture. Code Disassembly
- IDA Pro. Assembly C
- Windows API. The Registry. Tracking Active Malware
- Debugging. OLLYDBG
- Kernel Debugging. WINDBG
- Malware Behavior
- Data Encoding
- Anti-Disassembly
- Anti-Debugging

NOTES: When working on the assignments and ground challenges you should use the following procedure:

- Attempt each question in the labs on your own. If you get stuck you should refer to the model answers in the text. There are no points lost for getting stuck or not understanding the labs. You lose points by not attempting the labs, not turning labs in on time, and not taking a self-motivated approach to meeting the

requirements. So be honest about when you get stuck. Identify where the problem occurred, then identify how the model answers helped and what new insight and understanding you achieved by referring to those answers.

- Attempt each Grand Challenge on your own. There are going to be points where you have to ask for help. You don't lose points for asking for help. You lose points by NOT asking for help, by avoiding the problem because you find it difficult or time consuming. Sometimes the instructor will give leading or deliberately oblique clues in an attempt to get you on the right path without giving you all the answers.
- You are dealing with **MALWARE**, **SOMETIMES LIVE REAL WORLD MALWARE**. You should practice safe analysis. This means the following
    - Never have a live internet connection during an analysis.
    - If you need a network (because you are looking for malware network activity) then setup a virtual network in our VM Farm sandbox. You'll be given instructions on how to access and setup your VM's.
    - Never move malware from a sandbox to a live system.
    - If you value your computer system, always backup before attempting any analysis. This is true of your physical system and also of any VM's you create.
- Even if a lab is centered on a particular technique, you should always follow the same procedure. Do a complete analysis including basic static and dynamic analysis, followed by advanced techniques that you need. You should strive to develop a standard systematic approach and report your findings in a standard professional format.

The portfolio is an aggregation of all the labs in the course. Together with final versions of the grand challenges. Each lab and grand challenge should be updated to take into account feedback from the instructor. If you miss a lab you are still at liberty to include it in the portfolio if you get it done at a later point.

RULES OF CONDUCT:

During online class sessions, students will refrain from behavior in the classroom that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. **Please turn off or mute your *cellular phone* before class begins**. **Inappropriate behavior in the classroom shall result in, minimally, being reported to the Dean of Students for disciplinary action in accordance with university policy**.

BLACKBOARD CONDUCT:

Students will refrain from behavior in Blackboard that intentionally or unintentionally disrupts the learning process and, thus, impedes the mission of the university. Inappropriate behavior in the classroom shall result in, minimally, a directive to leave class or being reported to the Dean of Students for disciplinary action in accordance with university policy

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.

No cheating on an examination or assignments is allowed. A score of zero will be given to the student if such a case occurred.

OTHER ADMINISTRATIVE MATTERS:

Americans with Disabilities Act: It is the policy of Sam Houston State University that individuals otherwise qualified shall not be excluded, solely by reason of their disability, from participation in any academic program of the university. Further, they shall not be denied the benefits of these programs nor shall they be subjected to discrimination. Students with disabilities that might affect their academic performance should register with the Office of Services for Students with Disabilities located in the Lee Drain Annex (telephone 936-294-3512, TDD 936-294-3786, and e-mail disability@shsu.edu). They should then make arrangements with their individual instructors so that appropriate

strategies can be considered and helpful procedures can be developed to ensure that participation and achievement opportunities are not impaired. SHSU adheres to all applicable federal, state, and local laws, regulations, and guidelines with respect to providing reasonable accommodations for students with disabilities. If you have a disability that may affect adversely your work in this class, then I encourage you to register with the SHSU Services for Students with Disabilities and to talk with me about how I can best help you. All disclosures of disabilities will be kept strictly confidential. NOTE: No accommodation can be made until you register with the Services for Students with Disabilities. For a complete listing of the university policy, see: http://www.shsu.edu/dept/academic-affairs/documents/aps/students/811006.pdf.

Religious Holidays:
An institution of higher education shall excuse a student from attending classes or other required activities, including examinations, for the observance of a religious holy day, including travel for that purpose. A student whose absence is excused under this subsection may not be penalized for that absence and shall be allowed to take an examination or complete an assignment from which the student is excused within a reasonable time after the absence.

Other:
The instructor reserves the right to modify the schedule of assignments as needed.