CIS 4348-110, CRN 11383, Security Trends and Malware Analysis
Spring 2022
Texas A&M University-Central Texas

Instructor: Dinesh Reddy, Ph.D.
Office: FH 323G
Email: dreddy@tamuct.edu
Office Hours: TR 12:45-2 pm, 4:45-6 pm virtual (emails, calls, or video desktop sharing) (or by appointment)

Course Dates, Modality, and Location
Jan 18 – May 13. This is a classroom blended instructional method course. This course uses the A&M-Central Texas Canvas Learning Management System [https://tamuct.instructure.com]. I use Canvas to post course content, assignments, quizzes, exams, and to communicate any other announcements with the class. So please check Canvas regularly (on a daily basis) for updates.

Student-instructor interaction:
You may use the Canvas "inbox" feature or email me with your questions anytime as you would by attending the class and coming into my office. Your questions will be answered within 24 hours on weekdays and within 48 hours on weekends and holidays.

Emergency Warning System for Texas A&M University-Central Texas
SAFEZONE. SafeZone provides a public safety application that gives you the ability to call for help with the push of a button. It also provides Texas A&M University-Central Texas the ability to communicate emergency information quickly via push notifications, email, and text messages. All students automatically receive email and text messages via their myCT accounts.

Downloading SafeZone allows access to push notifications and enables you to connect directly for help through the app.

You can download SafeZone from the app store and use your myCT credentials to log in. If you would like more information, you can visit the SafeZone website [www.safezoneapp.com].

To register SafeZone on your phone, please follow these 3 easy steps*:*

1. Download the SafeZone App from your phone store using the link below:
    - iPhone/iPad: [https://apps.apple.com/app/safezone/id533054756]
    - Android Phone / Tablet [https://play.google.com/store/apps/details?id=com.criticalarc.safezoneapp]
2. Launch the app and enter your myCT email address (e.g. {name}@tamuct.edu)
3. Complete your profile and accept the terms of service

COURSE INFORMATION

Course Overview and description: This course analyzes and investigates security threats and ethical hacking methods. It will introduce students to modern malware analysis techniques through a detailed examination of malware, virus, and malicious code operation by examining case studies and hands-on interactive analysis of real world samples. The course will also examine in detail current trends in the threat environment and the most current attack exploits. Student will use a variety of methods to investigate current security threats and their mitigation. Topics include malware morphology, disassembly of malware, ethical hacking methods on systems including penetration, and trends in the threat-scape.

Student Learning Outcomes:

- Students will gain an understanding of hacker tools, techniques, and ethical hacking methods.
- Students will gain knowledge about penetration tests used to assess vulnerability of systems to current security incident trends including malware attacks.
- Students will gain an understanding of the following topics related to malware:
    - The malware concepts and technologies
    - The types of malware and how they are categorized
    - How malware protects itself from security products
    - The things that malware depends upon to operate
    - How to identify and remove malware on a Windows system
    - How to collect malware from different sources
    - How to perform static analysis of malware sample
    - How to perform dynamic analysis of malware sample
    - How to disassemble malware
    - How to use debugging techniques and tools for malware analysis

Required Reading and Textbook(s):

1. eBook on "Security Trends and Malware Analysis"
ISBN: 978-1-284-01407-5
Students will need to purchase an Access Code (by searching above ISBN on jblearning.com) in order to redeem their eBooks on the PUBLISH web site (http://publish.jblearning.com/ebooks).

2. Virtual lab access for "Security Trends and Malware Analysis"
ISBN: 978-1-284-19307-7
More details on purchase options will be provided in class and on Canvas.

3. Practical Malware Analysis - The Hands-On Guide to Dissecting Malicious Software
by Michael Sikorski and Andrew Honig
ISBN-13: 9781593272906

Supplemental Material

Additional required readings and optional readings will be posted on Canvas.

COURSE REQUIREMENTS

Exams

There will be three exams (two mid-terms and one final). Each exam is worth 100 points. Final exam will not be comprehensive. The exams can be conducted either paper-based or on canvas. Exams will be based on the textbook, and other readings posted on Canvas. It is assumed that you will read the assigned chapters and readings in advance. Make up exams are not typically given. The only acceptable excuses for missing an exam are circumstances clearly outside your control, such as illness, death in family, etc. If you miss an exam, notify me as soon as possible. I may require documentation of the circumstances.

Lab Assignments

Labs are designed for students to have hands on experiences on the topics covered in this course. All lab work should be completed via virtual lab environment that accompanies the required textbook. Instructions on what to submit for each lab will be posted on Canvas. You will be asked to prepare a lab report with your observations and screenshots. All lab reports must be submitted before the end of the day (11:59 PM) on the due date mentioned in the course schedule. Late submissions will not be accepted for full points and will attract 10% deduction for each day that it is late. Each lab assignment is worth 25 points.

Quizzes

There will be ten quizzes (multiple choice, true/false) that are designed to test the general understanding of the topics covered in the course. The quizzes can be conducted either paper-based or on Canvas. Late submissions will not be accepted. Each quiz is worth 20 points.

Project Report

There will be a project based on the concepts learned in this course. The project may be a combination of items such as a malware analysis case, essay questions, lab work, etc. The project deliverables will include a professionally written project report on findings. The project report must be submitted before the end of the day (11:59 PM) on the due date mentioned in the course schedule. Late submissions will not be accepted for full points and will attract 10% deduction for each day that it is late. Project report is worth 150 points.

Project Presentation

Each student will be required to present a topic (either individual or in a group). Students will select and explore a current topic/trend in this course. More details on the presentation topics,

presentation schedule, and grading rubrics (used for assessing the presentations) will be announced in class and uploaded on Canvas. Late presentations will not be scheduled. Presentation is worth 100 points.

Grading Criteria:

Course Requirement	Points	Weightage
Two Mid-Term Exams (100 points each)	200	20%
Final Exam	100	10%
Ten Lab Assignments (25 points each)	250	25%
Ten Quizzes (20 points each)	200	20%
Project Report	150	15%
Project Presentation	100	10%
Total	**1000**	**100%**

Final letter grade distribution will be as per the following scale:

Letter Grade	Point Range
A	900 and above
B	800-899
C	700-799
D	600-699
F	599 and below

Posting of Grades

All students' grade will be posted on the Canvas Grade book, and students can monitor their progress on Canvas grade book. Students can expect to see their grades within two weeks of the closing of class tests, exams, and assignments. Students are expected to visit Canvas course webpage regularly to get any update regarding this course.

COURSE OUTLINE AND CALENDAR

Course Schedule* ** (* This schedule provides a general plan. Deviations may be necessary) (** Readings for each week will be posted on Canvas)

Week	Date	Readings	Due
1	1/18	Syllabus, eBook Ch 1 – Hacking: The Next Generation	
	1/20	eBook Ch 1 – Continued	Quiz 1
2	1/25	eBook Ch 2 - Footprinting Tools	
	1/27	eBook Ch 2 – Continued	Quiz 2
3	2/1	eBook Ch 3 – Port Scanning	Lab Assignment 1
	2/3	eBook Ch 3 - Continued	Quiz 3
4	2/8	eBook Ch 4 - Enumeration & Computer System Hacking	Lab Assignment 2
	2/10	eBook Ch 4 – Continued	Quiz 4
5	2/15	Exam 1 Review	Lab Assignment 3
	2/17	Exam 1	Exam 1
6	2/22	eBook Ch 5 - Malware	Lab Assignment 4
	2/24	eBook Ch 5 – Continued	Quiz 5
7	3/1	PMA Ch 0 – Malware Analysis Primer	Lab Assignment 5
	3/3	PMA Ch 1 – Basic Static Techniques	Quiz 6
8	3/8	PMA Ch 2 – Malware Analysis in Virtual Machines	Lab Assignment 6
	3/10	PMA Ch 3 – Basic Dynamic Analysis	Quiz 7
9	3/15	S P R I N G B R E A K	
	3/17	S P R I N G B R E A K	
10	3/22	PMA Ch 4 - A Crash Course in x86 Disassembly	Lab Assignment 7
	3/24	PMA Ch 4 – Continued	Quiz 8
11	3/29	Exam 2 Review	
	3/31	Exam 2	Exam 2
12	4/5	PMA Ch 5 – IDA Pro	Lab Assignment 8
	4/7	PMA Ch 5 - Continued	Quiz 9
13	4/12	PMA Ch 6 – Recognizing C Code Constructs in Assembly	Lab Assignment 9
	4/14	PMA Ch 6 - Continued	Quiz 10
14	4/19	PMA Ch 7 – Analyzing Malicious Windows Programs	Lab Assignment 10
	4/21	PMA Ch 7 – Continued	
15	4/26	PMA Ch 8 – Debugging (Intro to OllyDbg & WinDbg)	Project Report
	4/28	Project Presentations	
16	5/3	Project Presentations	
	5/5	Final Exam Review	
17	5/10	Final Exam	Final Exam

Important University Dates:

January 18, 2022	Classes Begin for Spring Semester
January 20, 2022	Deadline for Add, Drop, and Late Registration for 16- and First 8-Week Classes
January 25, 2022	Deadline to Drop First 8-Week Classes with No Record
February 1, 2022	Deadline for Teacher Education Program Applications
February 2, 2022	Deadline to Drop 16-Week Classes with No Record
February 25, 2022	Deadline to Drop First 8-Week Classes with a Quit (Q) or Withdraw (W)
March 11, 2022	Classes end for 1st 8-Weeks Session
March 15, 2022	Deadline for Clinical Teaching/Practicum Applications
March 15, 2022	Deadline for Faculty Submission of First 8-Week Final Class Grades (due by 3pm)
March 14-18, 2022	Spring Break (No Classes - Administrative Offices Open)
March 21, 2022	Class Schedule Published for Summer Semester
March 21, 2022	Add, Drop, and Late Registration Begins for Second 8-Week Classes $25 Fee assessed for late registrants
March 21, 2022	Classes Begin for Second 8-Week Session
March 23, 2022	Deadline for Add, Drop, and Late Registration for Second 8-Week Classes
March 25, 2022	Deadline for Spring Graduation Application for Ceremony Participation
March 28, 2022	Deadline to Drop Second 8-Week Classes with No Record
April 1, 2022	Deadline for GRE/GMAT Scores to Graduate School Office
April 1, 2022	Deadline for School Counselor Program Applications

April 4, 2022	Registration Opens for Summer Semester
April 8, 2022	Deadline to Drop 16-Week Classes with a Quit (Q) or Withdraw (W)
April 16, 2022	Deadline for Final Committee-Edited Theses with Committee Approval Signatures for Spring Semester to Graduate School Office
April 29, 2022	Deadline to drop Second 8-week Classes with a Quit (Q) or Withdraw (W).
May 13, 2022	Deadline to Withdraw from the University for 16- and Second 8-Week Classes
May 13, 2022	Spring Semester Ends

TECHNOLOGY REQUIREMENTS AND SUPPORT

Technology Requirements

This course will use the A&M-Central Texas Instructure Canvas learning management system. **We strongly recommend the latest versions of Chrome or Firefox browsers. Canvas no longer supports any version of Internet Explorer.**

Logon to A&M-Central Texas Canvas [https://tamuct.instructure.com/] or access Canvas through the TAMUCT Online link in myCT [https://tamuct.onecampus.com/]. You will log in through our Microsoft portal.

Username: Your MyCT email address. Password: Your MyCT password

Canvas Support

Use the Canvas Help link, located at the bottom of the left-hand menu, for issues with Canvas. You can select "Chat with Canvas Support," submit a support request through "Report a Problem," or call the Canvas support line: 1-844-757-0953.

For issues related to course content and requirements, contact your instructor.

Online Proctored Testing

A&M-Central Texas uses Proctorio for online identity verification and proctored testing. This service is provided at no direct cost to students. If the course requires identity verification or proctored testing, the technology requirements are: Any computer meeting the minimum computing requirements, plus web camera, speaker, and microphone (or headset). Proctorio also requires the Chrome web browser with their custom plug in.

Other Technology Support

For log-in problems, students should contact Help Desk Central, 24 hours a day, 7 days a week

Email: helpdesk@tamu.edu
Phone: (254) 519-5466

Web Chat: [http://hdc.tamu.edu]
Please let the support technician know you are an A&M-Central Texas student.

UNIVERSITY RESOURCES, PROCEDURES, AND GUIDELINES

Drop Policy

If you discover that you need to drop this class, you must complete the Drop Request Dynamic Form through Warrior Web.

[https://dynamicforms.ngwebsolutions.com/casAuthentication.ashx?InstID=eaed95b9-f2be-45f3-a37d-46928168bc10&targetUrl=https%3A%2F%2Fdynamicforms.ngwebsolutions.com%2FSubmit%2FForm%2FStart%2F53b8369e-0502-4f36-be43-f02a4202f612].

Faculty cannot drop students; this is always the responsibility of the student. The Registrar's Office will provide a deadline on the Academic Calendar for which the form must be completed. Once you submit the completed form to the Registrar's Office, you must go into Warrior Web and confirm that you are no longer enrolled. If you still show as enrolled, FOLLOW-UP with the Registrar's Office immediately. You are to attend class until the procedure is complete to avoid penalty for absence. Should you miss the drop deadline or fail to follow the procedure, you will receive an F in the course, which may affect your financial aid and/or VA educational benefits.

Academic Integrity

Texas A&M University-Central Texas values the integrity of the academic enterprise and strives for the highest standards of academic conduct. A&M-Central Texas expects its students, faculty, and staff to support the adherence to high standards of personal and scholarly conduct to preserve the honor and integrity of the creative community. Any deviation by students from this expectation may result in a failing grade for the assignment and potentially a failing grade for the course. All academic misconduct concerns will be referred to the Office of Student Conduct. When in doubt on collaboration, citation, or any issue, please contact your instructor before taking a course of action.

For more information regarding the Student Conduct process, [https://www.tamuct.edu/student-affairs/student-conduct.html].

If you know of potential honor violations by other students, you may submit a report, [https://cm.maxient.com/reportingform.php?TAMUCentralTexas&layout_id=0].

Academic Accommodations

At Texas A&M University-Central Texas, we value an inclusive learning environment where every student has an equal chance to succeed and has the right to a barrier-free education. The Warrior Center for Student Success, Equity and Inclusion is responsible for ensuring that students with a disability receive equal access to the university's programs, services and activities. If you believe you have a disability requiring reasonable accommodations, please contact the Office of Access and Inclusion, WH-212; or call (254) 501-5836. Any information you provide is private and confidential and will be treated as such.

For more information, please visit our Access & Inclusion Canvas page (log-in required) [https://tamuct.instructure.com/courses/717]

Important information for Pregnant and/or Parenting Students

Texas A&M University-Central Texas supports students who are pregnant and/or parenting. In accordance with requirements of Title IX and related guidance from US Department of Education's Office of Civil Rights, the Dean of Student Affairs' Office can assist students who are pregnant and/or parenting in seeking accommodations related to pregnancy and/or parenting. Students should seek out assistance as early in the pregnancy as possible. For more information, please visit Student Affairs [https://www.tamuct.edu/student-affairs/pregnant-and-parenting-students.html]. Students may also contact the institution's Title IX Coordinator. If you would like to read more about these requirements and guidelines online, please visit the website [http://www2.ed.gov/about/offices/list/ocr/docs/pregnancy.pdf].

Title IX of the Education Amendments Act of 1972 prohibits discrimination on the basis of sex and gender–including pregnancy, parenting, and all related conditions. A&M-Central Texas is able to provide flexible and individualized reasonable accommodation to pregnant and parenting students. All pregnant and parenting students should contact the Associate Dean in the Division of Student Affairs at (254) 501-5909 to seek out assistance. Students may also contact the University's Title IX Coordinator.

Tutoring

Tutoring is available to all A&M-Central Texas students, both virtually and in-person. Student success coaching is available online upon request.

If you have a question, are interested in becoming a tutor, or in need of success coaching contact the Warrior Center for Student Success, Equity and Inclusion at (254) 501-5836, visit the Warrior Center at 212 Warrior Hall, or by emailing WarriorCenter@tamuct.edu.

To schedule tutoring sessions and view tutor availability, please visit Tutor Matching Services [https://tutormatchingservice.com/TAMUCT] or visit the Tutoring Center in 111 Warrior Hall.

Chat live with a remote tutor 24/7 for almost any subject from on your computer! Tutor.com is an online tutoring platform that enables A&M-Central Texas students to log in and receive online tutoring support at no additional cost. This tool provides tutoring in over 40 subject areas except writing support. Access Tutor.com through Canvas.

University Writing Center

University Writing Center: Located in Warrior Hall 416, the University Writing Center (UWC) at Texas A&M University–Central Texas (A&M–Central Texas) is a free service open to all A&M–Central Texas students. For the Spring 2022 semester, the hours of operation are from 10:00 a.m.-5:00 p.m. Monday thru Thursday in Warrior Hall 416 (with online tutoring available every hour as well) with satellite hours available online only Monday thru Thursday from 6:00-9:00 p.m. and Saturday 12:00-3:00 p.m.

Tutors are prepared to help writers of all levels and abilities at any stage of the writing process. While tutors will not write, edit, or grade papers, they will assist students in developing more effective composing practices. By providing a practice audience for students' ideas and writing, our tutors highlight the ways in which they read and interpret students' texts, offering guidance and support throughout the various stages of the writing process. In addition, students may work independently in the UWC by checking out a laptop that runs the Microsoft Office suite and connects to WIFI, or by consulting our resources on writing, including all of the relevant style guides. Whether you need help brainstorming ideas, organizing an essay, proofreading, understanding proper citation practices, or just want a quiet place to work, the UWC is here to help!

Students may arrange a one-to-one session with a trained and experienced writing tutor by making an appointment via WCOnline [https://tamuct.mywconline.com/]. In addition, you can email Dr. Bruce Bowles Jr. at bruce.bowles@tamuct.edu if you have any questions about the UWC, need any assistance with scheduling, or would like to schedule a recurring appointment with your favorite tutor by making an appointment via WCOnline [https://tamuct.mywconline.com/]. In addition, you can email Dr. Bruce Bowles Jr. at bruce.bowles@tamuct.edu if you have any questions about the UWC, need any assistance with scheduling, or would like to schedule a recurring appointment with your favorite tutor.

University Library

The University Library provides many services in support of research across campus and at a distance. We offer over 200 electronic databases containing approximately 400,000 eBooks and 82,000 journals, in addition to the 96,000 items in our print collection, which can be mailed to students who live more than 50 miles from campus. Research guides for each subject taught at A&M-Central Texas are available through our website to help students navigate these resources. On campus, the library offers technology including cameras, laptops, microphones, webcams, and digital sound recorders.

Research assistance from a librarian is also available 24 hours a day through our online chat service, and at the reference desk when the library is open. Research sessions can be scheduled for more comprehensive assistance, and may take place virtually through WebEx, Microsoft Teams or in-person at the library. Schedule an appointment here [https://tamuct.libcal.com/appointments/?g=6956]. Assistance may cover many topics, including how to find articles in peer-reviewed journals, how to cite resources, and how to piece together research for written assignments.

Our 27,000-square-foot facility on the A&M-Central Texas main campus includes student lounges, private study rooms, group work spaces, computer labs, family areas suitable for all ages, and many other features. Services such as interlibrary loan, TexShare, binding, and laminating are available. The library frequently offers workshops, tours, readings, and other events. For more information, please visit our Library website [http://tamuct.libguides.com/index].

OPTIONAL POLICY STATEMENTS

A Note about Sexual Violence at A&M-Central Texas

Sexual violence is a serious safety, social justice, and public health issue. The university offers support for anyone struggling with these issues. University faculty are mandated reporters, so if someone discloses that they were sexually assaulted (or a victim of Domestic/Dating Violence or Stalking) while a student at TAMUCT, faculty members are required to inform the Title IX Office. If you want to discuss any of these issues confidentially, you can do so through Student Wellness and Counseling (254-501-5955) located on the second floor of Warrior Hall (207L).

Sexual violence can occur on our campus because predators often feel emboldened, and victims often feel silenced or shamed. It is incumbent on ALL of us to find ways to actively create environments that tell predators we don't agree with their behaviors and tell survivors we will support them. Your actions matter. Don't be a bystander; be an agent of change. For additional information on campus policy and resources visit the Title IX webpage [https://www.tamuct.edu/compliance/titleix.html].

Behavioral Intervention

Texas A&M University-Central Texas cares about the safety, health, and well-being of its students, faculty, staff, and community. If you are aware of individuals for whom you have a concern, please make a referral to the Behavioral Intervention Team. Referring your concern shows you care. You can complete the referral online [https://cm.maxient.com/reportingform.php?TAMUCentralTexas&layout_id=2].

Anonymous referrals are accepted. Please see the Behavioral Intervention Team website for more information [https://www.tamuct.edu/bit]. If a person's behavior poses an imminent threat to you or another, contact 911 or A&M-Central Texas University Police at 254-501-5805.
