Carnegie Mellon University: Heinz College
95-889 Applied Threat Analysis (ATA)
Spring 2023 – Tuesday 630PM EST

Instructor Information:
Timur Snoke
tdsnoke@cmu.edu
Office Hours: by appointment

TA
Urvi Jere
uaj@andrew.cmu.edu
Office Hours: TBD

Email is the easiest and quickest form of communication. Please add 95-889 in the email 'Subject' line. I will get back to you with 24 hours.

Course Description
The role of Cyber Threat Analysts is to aggregate and fuse disparate data sources to provide actionable information to decision makers in industry as well as both the federal and civilian government. More and more these sectors are relying on analysts who have a deep understanding of the ecosystem and the risks contained therein to better understand the cyber threats that they are facing. This course seeks to provide a richer context and a basis for understanding the evolving nature of cyber threats. This class will discuss the relationship between vulnerabilities, exploits, and malware. In addition, this class will also explore the value of host based or network indicators and other indicators of compromise. Finally, we will discuss the continuum of threat actors and why sometimes the greatest threat is from within.

Objectives
- Analyze the vulnerability landscape, the acronym soup of threat identification and government regulations in practice.
- Explore the impacts of high-level threats to networks, systems, and applications.
- Assess exploit development and usage. Demonstrate knowledge of impacts of exploits upon operating systems, applications, and networks
- Discover, aggregate, and expand network indicators provided from analysis
- Understand the challenges of collection, interpretation, and making observations as an analyst
- Fuse all above data points in support of actionable threat intelligence reports by correlating facts and developing supporting analytics
- Communicate the threat landscape effectively for senior leadership and other decision makers

Bottom Line Up Front (BLUF):

- We will use Canvas. Please check it often. You will submit your assignments there, too.
- The TA is your first line of contact for all assignment questions. Go to them first and they will loop me in as appropriate.
- Course will be made up of assignments and a final project.
- If we are doing remote sessions for class, we will be using Zoom. You may be asked to turn on your camera. You can use a background filter if you have privacy concerns.
- All lectures will be recorded. The recorded lectures are not for you, but for future offerings of the course.
- Assignments will be posted following class
- By the end of the course, you will be able to demonstrate the ability to do data fusion of vulnerability, exploit, malware, and network data to profile threats and adversaries. You will also analyze malicious behavior, and synthesize output using open-source analysis tools
- You will practice effective communication in the form of analysis summaries and the written assignments.
- You are expected to effectively communicate with the instructors and others for both native and non-native English speakers.
- There will be ZERO cheating. We will punish any infraction to academic integrity to the full extent as outlined in our policies.

Course Management

Canvas will be the used to post lecture notes, class materials, assignments, and other information. The onus is on the student to check Canvas regularly for announcements, changes, and any other course information.

In some cases, readings, videos, or other media provided to support the class lectures on after class. Students are expected to read/watch/interact with the course material to engage in discussions on lecture days. The material provided in reading assignments will greatly help with leveling the learning curve for in class labs

The instructors can make changes to the lecture schedule at any time in an effort to best serve the student and the overall needs of the class. A new syllabus will be provided to the students for any changes.

Course Material

- Any reading will be provided to you as a PDF. No one book would fulfill the need of this course.
- Most of the work in this class will be using open-source tools and public resources, some of which have pay for use elements that are free for academics if registered with an academic email. I will leave the registration for those accounts up for the student's discretion.

Grading Scale
A rubric or instructions will be provided before a project or in-class lab. This class will follow the Heinz grading scale:

A+	98%	B+	88%	C+	78%
A	92%	B	82%	C	72%
A-	90%	B-	80%	C-	70%

Please note that this grading scale is **firm**; I will not add or deduct points individually to move students between letter grades at the end of the semester. The grade that you earn is the grade that you receive without exception. Students auditing the class for a pass/fail are responsible for turning in all assignments.

Course Outline
The Course schedule is preliminary and will be adjusted throughout the semester. Changes to the syllabus schedule will be uploaded to Canvas by the instructor. The course outline can become dynamic if we need to speed more time on a specific topic or material. Additionally, more material may be added if the instructor.

Week	Date	Topic
1	Mar 12	Intro & OSINT
2	March 19	Vulnerability Ecosystem – CVE, CWE, NVD Exploits – Intro, definition of exploit, where to find them
3	March 26	Networking Analysis – understanding system interconnections and analyzing traffic
4	Apr 2	Network Analysis – packet analysis
5	Apr 9	System Analysis – log analysis
6	Apr 16	Malware Analysis
7	April 23	Fusion of Results
8	May 2	Final Exam placeholder

Class Breakdown
- This will be a technical class. You will be challenged. It won't be impossible. You will succeed.
- For this class, we will be doing a lot of work in virtual machines and using Docker containers. You may use which ever Linux distro you are most comfortable using. I will be using Kali created by Offensive Security on VMware. You are responsible to troubleshoot your own problems with virtual machine software, the distro itself, and any tools within the distro.
- Assume all lab material we give you in class is malicious. Use a virtual machine environment that is not attached to the network when opening and analyzing the files. The password for any zip file is 'infected'. No quotes.

- **60% of Grade**: There will be multiple homework assignments throughout the mini. Assume every week.
- **40% Final:** Paper or Presentation. Final details will be provided by week 4.

Academic Integrity

We have zero tolerance for academic integrity violations, and especially at the graduate level, the University does too. We encourage you to read and understand the University Policy on Academic Integrity to help guide your choices. The high-level definition of academic integrity is as follows: You may not copy any part of a solution to a problem that was written by another student. You may not develop a solution with another student. You may not copy from any other unauthorized source, including those found on the Internet. You may not look at another student's solution, even if you have completed your own. You may not give or show your solution to another student, nor knowingly leave your solution where another student could see it. That is: helping another student cheat *is also cheating.*

To illustrate, here are some examples of inappropriate behavior:

- Copying, retyping, or referring to, files or parts of files (e.g., source code, written text, or unit tests) from another person or source (whether in final or draft form, regardless of the permissions on the associated files) while producing your own. This is true even if your version includes modifications.
- Getting help that you do not fully understand, and from someone whom you do not acknowledge on your solution.
- Coaching or providing help to another step-by-step without them understanding your help.
- Writing, using, or submitting a program that attempts to alter or erase grading information or otherwise compromise security of course resources.
- Lying to course staff.
- Giving copies of your work to others or allowing someone else to copy or refer to your code or written assignment to produce their own, either in draft or final form. *This includes making your work publicly available in a way that other students (current or future) can access your solutions, even by accident.* Beware the privacy settings on your open-source accounts!
- The use of assistive technologies like ChatGPT is discouraged for classroom activities or assignments, unless directed to do so and its usage is cited with all prompts used.

If any of your work contains any statement that was not written by you, you must put it in quotes and cite the source. If you are paraphrasing an idea, you read elsewhere, you must acknowledge the source. Using existing material without proper citation is plagiarism, a form of cheating. If there is any question about whether the material is permitted, you must get permission in advance. It is *not* considered cheating to discuss and clarify vague points in the assignments, lectures, lecture notes; to give help or receive help in using the computer tools, systems, compilers, debuggers, profilers, or other facilities; or to discuss ideas at a very high level, without referring to or producing code.

Any violation of this policy is cheating. The *absolute minimum* penalty for cheating (including plagiarism) will be a zero grade for the whole assignment. Cheating incidents will also be reported

through University channels, with possible additional disciplinary action (see the above-linked University Policy on Academic Integrity).

Accommodations for Individuals with Disabilities
If you have a disability and have an accommodations letter from the Disability Resources office, we encourage you to discuss your accommodations and needs with us as early in the semester as possible. We will work with you to ensure that accommodations are provided as appropriate. If you suspect that you may have a disability and would benefit from accommodations but are not yet registered with the Office of Disability Resources, we encourage you to contact them at access@andrew.cmu.edu.

Course modality and COVID-19 policies

Our class is designated as in-person expectation. This means that attendance in the classroom on a regular basis is expected. In order to attend class in person, we expect that all students will abide by all behaviors indicated on CMU's Covid-19 Updates webpage. The class recording is not a substitute for attending class. If you are ill or experience exceptional circumstances, contact the course faculty to discuss getting access to lecture is warranted. This will be decided on a case-by-case basis.

Attendance
Your attendance and participation in class is critical to getting the most out of this class. Classes are designed to be interactive and often are most successful when they draw on challenges faced by students. We will be performing in class activities to evaluate students throughout the semester.

Extensions and Rescheduling Exams
Extensions and rescheduled exams will *only* be provided in the dire circumstances. These will be evaluated on a case-by-case basis and will require documentation. We will only consider regrading if notified within 24 hours in writing (email preferred) of receiving an assessment. The student should explain why they thought the grade is inaccurate within the email.

Late Assignments
Students will be submitting all assignments through Canvas. Any late assignments timestamped after the expected due date provided by the instructor ***will result in a zero.*** If Canvas is down, students *must* provide the assignment via email to the instructor and TA before the due date.

Group Work
There may be some group work in this class. Groups will be no larger than 3 students and will be chosen by the professors.

Success in This Class
I understand that many of you are coming from different backgrounds and experiences. I appreciate this heterogeneous mixture, as it allows ideas to flow, and provides a great basis for in class discussion! You will be successful in this class if you take the time to understand the assigned readings, participate in class discussions and activities, identify when you are not understanding a

topic, and communicate effectively with your peers and the instructors. The instructors are here to facilitate your learning, not impede it.