ISA 564 / CS 499 Syllabus – Fall 2023

Course Catalog Description

Credits: 3 (NR)
Course Description (from GMU's course catalog, as listed for ISA 564):
Requires ISA 562, CS 531 or equivalent, or permission of instructor.

Provides hands-on experience in configuring and experimenting with commodity-networked systems and security software in a live laboratory environment, with the purpose of understanding real-world security threats. Takes both offensive and defensive approaches and exposes students to a variety of real-world attacks, including viruses, worms, rootkits, and botnets. Possible mitigation and defending mechanisms, such as firewalls and intrusion detection software, also covered. Offered by Computer Science. May not be repeated for credit.

Course Outcomes:
You will leave this course with the following skillsets, contingent on your level of effort:

- Hands-on experience with a breadth of security tools and analysis techniques.
- Deep understanding of the "cyber detection" problem and a portion of its solution space.
- An ability to construct, maintain, and operate the technical platforms needed to conduct contemporary cyber operations.
- A capability to troubleshoot and resolve technical issues in a computing environment.

These outcomes depend both on the tracked parts of the course and the level of effort a student chooses to put into it. You have a great opportunity to consume knowledge beyond the above course description and are encouraged to take advantage of that opportunity.

Required Prerequisites

- **THIS COURSE HAS STRICT TECHNOLOGY PREREQUISITES**:
    - **A laptop with an Intel-based CPU**, 8+ GB of RAM (16+ is ideal), and between 30 and 90+ GB of storage for running virtual machines. **You MUST have an Intel-based (or equivalent) CPU**, running a (Strongly Preferred) Windows operating system capable of running VMWare Workstation Pro 17.0, or a MAC (permitted for experienced users) capable of running VMWare fusion. Many of the components of the labs are compiled/tested only for Intel-based CPUs. **If you have an "Apple Silicon" CPU you will not be permitted to remain in the course**. Unfortunately, this requirement is immutable and there can be no exceptions.
        - MAC users are allowed in the course provided they accept that most MAC-specific troubleshooting will be left entirely in their hands. If you are such a user, it will be expected that you are experienced with your operating system and know how to configure it. I cannot offer comparable technical support for your operating system as I can for Linux and Windows.
        - These labs have been thoroughly tested with current versions of security tools, many of which run only on x86/x64 architectures.
        - Every student must have Administrator/Root-level permissions on the laptop they use.
    - **BOTH WIRED AND WIRELESS CAPABILITIES**. The course is composed of graded in-class exercises that require both wired and wireless network (ethernet) connectivity. WiFi-only laptops can meet this requirement with the purchase of a USB ethernet adapter.[1]

[1] For example : $10 : https://tinyurl.com/5n6zmjrr

- **25-50' Cat5+ Ethernet Cable**[2] (longer is better…please do not skimp on cable length, or you may not be able to sit where you need to sit in the room to reach power outlets, collaborate with lab partners, etc. I will not be able to ensure I have extra cables for students, so you will need your own to reliably participate in the classes exercises)

Additional Required Prerequisite(s):

- A willingness to research (for most, this means using Google, effectively, then reading documentation and forums posts) every error or problem they come across, put time into troubleshooting issues they experience, and learn from those issues so that they can avoid them in the future.
- A basic to intermediate level of technology literacy, to include but not limited to:
  - The ability and understanding required to connect to Wired and Wireless networks both at home and in class
  - Use USB devices and ports mounted to Windows and Linux
  - Use a web browser
  - User text editors within Linux and Windows
  - Navigate Windows and Linux CLIs and filesystems, identify and recover from hardware and software failures.
  - A working knowledge of the OSI model, particularly layers 2, 3, 4, and 7.
  - Record traffic captures in Wireshark and extract facts about headers and payloads of common protocols.
- An ability to independently solve their own technology problems. The lab environment, like real life, seldom survives a patch cycle unharmed, and installation documentation is often outdated when you need to use it. **You are expected to navigate user-specific problems on your own and understand how your own technology works. Any student that is unwilling to put in this time should take a different course.**
  - The student is the only person who knows the history of their hardware, and the efforts they put into driving it to a state where it no longer functions as intended. As a result, they are the most appropriate individuals to troubleshoot issues.
  - The professor is available and willing to help diagnose and resolve issues, however the student must exhaust their knowledge and efforts first before engaging them for support.

The bullets above represent the bulk of the deficiencies in student skillsets when working through this course. **You *can* develop these skillsets during this course, but only if you put in the requisite effort to do so, and that requires you to "put in work[3]". This is often a significant hurdle for students who are new to this area**.

[2] For example: $6 : https://tinyurl.com/2y8tw4cr

[3] Sometimes, a lot of work.

Strongly Recommended Prerequisite(s):

- A thorough understanding of how HTTP/S, SSH, DHCP, DNS, NAT and TCP/IP protocols work and what they look like when seen over Ethernet. Ideally you have taken (and performed well in) a networking course in the past.
- Experience in using Wireshark to (quickly) analyze network traffic.
- Experience with examining and understanding Windows event logs and Sysmon.
- Familiarity with VMWare and experience with creating and managing virtual machines and virtual networking.
- Installing, configuring, and troubleshooting Ubuntu and Kali Linux, Windows 10 and Windows Server.
- Non-trivial experience developing scripts in Python.
- Working knowledge of PowerShell and Linux Shell scripting (bash)

This course includes an initial lab that functions as a "gear check" and orientation. This particular lab will contain test elements and may take slightly longer to complete than typical labs in the course, however it exists to give you an opportunity to decide if this course is "for you" while you still have time to drop it and find another to take if needed. **Please complete this initial lab as soon as possible after its release so that you do not trap yourself in a course you are not ready for or forfeit tuition if you need to withdraw/risk academic probation if you fail.**

Administrative Info

Class Times: TBD, TBD – TBD (**Be on time**. The start times of in-class exercises may not allow for announcements and instruction to be repeated for latecomers. If you arrive late on exercise days, you will most likely perform poorly as the professor and GTA will be busy with students already underway.

Location: TBD
Instructor: Dr Paul Seymer
Email: pseymer@gmu.edu

- Note: University policy requires that communications about the course be conducted only over university-controlled mechanisms. The above email address is the best and only method to correspond with me during this course outside of class.

Office Hours: Weekly class time (as there is no formal lecture), or by appointment (preferably before class, but online via Teams through a scheduled appointment)

Graduate Teaching Assistant / Office Hours: TBD
Undergraduate Teaching Assistant / Office Hours: TBD

Note: Please bring your Mason ID card with you each time you attend class. In addition to providing proof of who you are, it lists your G number so that you do not need to remember it. If you do not have a Mason ID (keeping in mind that university policy requires you to have one), info can be found here: https://masonid.gmu.edu/about-mason-id/

Note: The most reliable and consistent way to ask questions and get extra help is to use the Bb forums. This allows us to share the outcomes from one student's problems with the entire class, however, please use university email to contact me for confidential questions or see me after class.

Note: It is a policy violation to disclose student grades to anyone other than the student, so please refrain from having grade-specific discussions in front of other students.

Note: You are not permitted, per university policy, to communicate with the Professor or GTA on any non-University controlled system. This includes using personal mobile numbers or tracking people[4] on social media and "accidentally" running into them outside of class[5]. You have adequate opportunities for support during this course, and 11th hour urgency due from your perspective is only just that.

FYSA: I am an adjunct professor here at GMU. I do not work for the university on a full-time basis, and I do not have a dedicated office on campus. Please keep your emails appropriate and course-related, and I will reply to them as often and as quickly as I can.

Course Composition (Summary, tl;dr)

Final Grade[6] = 40% Lab Submission + 55% In-Class Exercises + 5% Forum discussions.

- **Lab Submission** – Each lab topic will have an accompanying lab assignment. Students will perform the lab, place requested content into a lab report template, save it as a PDF, and submit it through blackboard. *Labs are the primary conduit for students to learn.*

- **In-Class Exercises** – In class exercises are aimed at assessing how well a student learned during the lab, and how successful they are at synthesizing solutions to expanded problems that overlap the lab topics. These consume 1.5 hours during their scheduled classes, and present nontrivial problems that students will work on solving either in pairs or by themselves (as indicated prior to the exercise). The technology and tools used during exercises is cumulative, requiring that students assemble a reliable set of skills over time. *In-Class exercises are intended to be the primary grading method in the course.* Students will undoubtedly learn during these exercises; however, the expectation is that students will come prepared and ready to demonstrate what they know. Preparation instructions will be posted prior to the exercise. Failure to adequately prepare for these exercises will almost certainly render them impossible to complete in the time allotted, eventually resulting in failure of the course.

- **Forum Discussions** – To earn full credit, you will need to post something useful or *be part of a discussion that is useful on <u>each</u> <u>and</u> <u>every</u> lab forum*. This used to be an extra credit portion for the course, however most students for some unknown reason chose not to participate. It is now a mandatory, but small, part of each student's grade.

---

[4] Electronic countersurveillance should not be assumed to be part of a professor's daily duties, regardless of the nature of course material or perceived (lack of) boundaries set by some students :-\

[5] Yes, this has happened, and it is entirely inappropriate, policy violating, and frankly...creepy.

[6] You are advised to continuously computer your grade using what is posted in Blackboard, so you may understand your performance. When assignments and exercises are graded, their scores are posted to Blackboard, and computing your ongoing grade is a trivial computation with this formula. Tracking your performance is your responsibility, as is noticing poor performance and initiating improvements (prior to the end of the semester, when it is too late to effect change).

Be advised: You are responsible for the impact of all technology problems you create or encounter to any activity performed in this course. Keep this in mind, and ensure you put the required time into learning about, maintaining, and troubleshooting your hardware and software platforms. Hard lessons are often learned when this time is not put in.

Course Composition (Detail)

- **Course Lab Assignments (Lab Submissions): 40%**
    - All deliverables must be submitted by the due date/time listed in the Blackboard assignment. Late submissions will **not** be accepted (full stop).
    - Lab submissions are the primary vehicle that you will use to learn. In-class exercises will immediately expose gaps in knowledge that you should have gained during these lab assignments and penalized accordingly, so work hard to prepare.
    - All lab assignments are individual assignments. You may not share work with other students. You are permitted to discuss lab assignments with other students, **however, be advised**: Students who immediately turn to their classmates for guidance on every step of every assignment without adequately absorbing the knowledge they need to pass the other portions of the class will not pass this course. You are NOT to turn these assignments into group projects.
    - We will not grade late labs. Do not bother asking, the answer is always No. You have 2 weeks to execute each lab, which gives you ample time to mitigate unforeseen life circumstances if you start early and/or meet with the instructor. We will do our best to help you mitigate these an a fair and reasonable way. The course schedule, however, does not lend itself to allowing for "make-up work". If you experience significant hardship during the semester, there are limits to what a professor can do to help you mitigate these. In these cases, you should consult your advisor or degree program office for withdrawal options (but speak to me first to get a quick assessment of the situation). Do not suffer unnecessarily if there are mitigation options at your disposal.
        - There may be opportunities to submit additional labs or perform unscheduled exercises for replacement credit, however these only occur when there are class-wide patterns that require them. These should not be assumed to occur, so please do not rely on them.
    - You will submit results from each lab as a report. You will be given a Word template for this report. **You must use this template when submitting lab deliverables**. **Each lab report submission must be a single PDF file** (save out the .doc as a PDF prior to submitting). Failure to do this will forfeit all points for the lab.
    - Lab scoring will be a composition of the material content of the lab, as well as your attention to detail while following all instructions (formatting or otherwise). This tends to follow an 80% material content, 20% formatting rules, however this is influenced by how far into the semester the assignment is given (i.e., formatting problems are penalized less on the first assignment, strongly penalized on later ones).

      You will start at full "formatting" credit and work downwards for each of the following penalties:
        - Names, Lab indicators, or TOCs that are inaccurate.
        - Section numbers do not match the assignment: Task 4,1, Task 4.2,etc.
        - Irrelevant content (not related to the current lab).
        - Translation or other "treasure hunting" activities that make grading take longer than it should be.

- You have misalignment in section numbering, tables of contents, appendix, etc. You are not expected to produce a work of art for your submission, but you should be precise in your formatting (as indicated in the report).
- You leave submission instructions, currently in the template, in the lab report when you submit (ignoring the many indications in that template to remove-after-reading)
- Your solution's text is hard to read.
- Your screenshots are illegible (lab assignments are clear on what needs to be viewable)
- Other "no-no's" mentioned in the submission template.

Please be clear and concise with your answers, and do not assume that "shot gunning" many answers will result in points given. **In the event there are more explicit answers than what was asked for or if deciphering your submission emulates a treasure hunt and consultation of stars or a crystal ball to understand, we will often choose the least correct answer and grade accordingly**.

- The lab assignments are meant to be straightforward…I will never be deceptive in the assignments. You should not be deceptive in your solutions. **Note: Failure to submit a PDF will result in 0 points for the entire lab (as mentioned excessively in the lab template)**

- **In-Class Individual lab demonstrations (In-class exercises): 55%**

  - Students will need to present their Mason ID (physical or electronic) to be permitted to remain in class for the exercise.
  - These activities are where you show and prove what you learned in the lab assignment.
  - During some classes (per syllabus), students will be required to demonstrate lab-related activities to the instructor. Preparatory instructions will be posted (typically in the corresponding lab); however, you are expected to synthesis what you learn in the lab assignments into successes in the exercises. I will not inform students of what to expect other than the prep instructions. If you are not in attendance for that class period, you will not earn credit for that exercise.
  - Technically focused activities aimed at measuring how well you are adapting to the technology space you are working in and how successful you will be at dealing with inevitable technical problems you *will* experience in future activities will be included in these in-class exercises. Topics will be released in advance so that you can practice and prepare.
  - These exercises are very demanding and short on time, so you will be expected to know the material and how to use it prior to attendance. This will not be the time to figure out how the labs worked or fill in skill gaps. This is an examination phase, and not an instructional one.
  - **Rules for Lab Exercise Partners and Groups** – Typically, working in groups in undergraduate and graduate school is a mixture of positive and negative experiences. Students who are prepared often must work to compensate for those that are not prepared. To mitigate this, lab exercises will be individual unless specified on the assignment. There are two caveats to exercises that a group-based: One, a student may choose to continue to work alone. Students who wish to work alone will need to inform the professor at or near the beginning of the semester. This will prevent churn or undo pre-class planning. Two, all students will need to demonstrate a minimal level of

competence in the course and your individual technology platforms before being allowed to group with other students. This competence will be measured during the first lab and in-class exercise and will be adjusted at the Professor's discretion throughout the semester based on on-going student grades and participation. Lab groups will be assigned by the Professor and will change from week to week. Assigned groups will be posted at the beginning of the class period that contains an exercise.
    - Regardless of group status, students are not permitted to communicate with any other humans outside of their assigned group until after the exercise is over.

- **Class Forum participation: 5%**
    - Each lab will have a corresponding Forum thread. You are advised to use these often, however you are required to use each of them at least once per lab to share topic relevant information. Content needs to remain specific to the lab's content and topics.
        - Forums will be locked and graded at corresponding lab submission time.
        - You are free and encouraged to initiate questions or respond to content with additional questions but be advised:
            - Off-topic or inappropriate content will not earn credit (and will annoy the professor, who may remove you from the forums entirely, regardless of its criticality to your final grade)
            - You will need to make a positive contribution to each lab to earn credit by providing questions, answers, or substantive discussion. The professor reserves the right to decide the definition of "positive contribution" means on an on-going basis, however given the volume of work in this course it is expected that the effort needed for participation in these discussions will be trivial (and a matter of course)
        - I will use the following as grading guidance for this:
            - 1% - Viable content for a single lab forum.
            - 2% - Viable content for >1/4 of all lab forums.
            - 3% - Viable content for >1/2 of all lab forums.
            - 4% - Viable content for >3/4 of all lab forums.
            - 5% - Viable content for every lab forum.
        - You are permitted to transpose important class discussions and notes into the class forums if you wish to meet this requirement.

Additional guidance: Some additional comments that will help you pass this course (which have sunk past students who failed to consume such guidance):

- You are responsible for learning what is needed to perform these labs. Other students are not in class solely to provide technical support to other students…but they may choose to do so. Please give them the option of saying "No, thank you" first. If you are turned away by your classmates, consider spending more time working through the lab yourself.

- Often, there will be at least 2 labs "out" at any one time…however **it is expected that you read and understand lab as soon as it is posted**, and that you will not wait until the last-minute work through them. Panicked 11th hour inquiries are extremely risky and should not be relied on[7]. You will run into "life events" that impact your submissions, however there are no

[7] Additionally, they are only successful at frustrating the professor. The answer is almost always "No."

exceptions to the late lab submission policy, and it is not feasible to supply make-up opportunities. This is the main motivation for the large amount of allotted time for each lab…so that you can plan for the potential impacts from external events[8]. Hard lessons are learned in this class. You are advised to try to forgo those lessons.

- You are strongly advised to develop an ability to troubleshoot your individual technical problems with infrastructure and laptop hardware as quickly as possible. I will attempt to aid students with this, but there is a limit to the amount of time available. You are also the best equipped expert at how your own technology functions (i.e., I am not looking you're your shoulder to record the 40 things you tried that broke your VM in the first place). Please dedicate necessary time to labs or consider taking a different graduate course in the event you do not possess or cannot quickly develop this skillset.
    - Note: Copying other people's labs or other violations of GMU's Academic Integrity policies are not an acceptable coping strategy for a skillset gap. You must put time into the course to do well. Ignoring this rule will result in poor performance in the demo portions, so doing so will only successfully create new problems for you.

- **Most Importantly: Read the lab instructions carefully (and immediately when they are assigned, so you do not leave the classroom without first obtaining test data, files, etc. that might be needed)** and submit all required elements (and only those required elements). We cannot give partial credit to labs (or parts of labs) that are not submitted. In past semesters, this has been the single most contributing factor to low lab grades. Before submitting, review your lab reports to ensure they contain what is being asked for in the assignment, and remove non-relevant content (e.g., my assignments are literal…if I didn't ask for it, you don't need to include it).

- **If this is your last semester at GMU (i.e., you are graduating) you are advised to work hard to ensure you pass this course and do indeed graduate**. If you do not meet the requirements in the course, you will fail the course, regardless of how close to graduation you are. Your past course performance is tangential to how you are graded in this one. Please do not put yourself in a situation where you risk your graduation by assuming your professors will pass you to meet a graduation deadline. I cannot, have not, and will not make accommodations for a student's graduation schedule or probationary status, and no degree of assertiveness and upward pressure will change my approach[9].

[8] I cannot prevent students from procrastinating, however I can and will most certainly penalize them for not meeting this standard.

[9] Apologies for the tone, and the need to put this in a syllabus, however…

Plagiarism/Cheating:

Unless otherwise stated by the professor, all assignments must be completed and submitted individually; however, you are encouraged to share lessons learned and lead discussions on the class forums for all work including these assignments. Outside of these guidelines, this course will adhere strictly to the Mason Honor Code[10]. Suspected violations will be submitted to the Office of Academic Integrity (OAI). The consequences for violating the honor code at the graduate level are very severe. I take this seriously, and students are advised to do the same.

Use of NLP-driven AI Technologies:
I do not ban the use of external technologies and data sources in the course, however I would recommend that students do not use them. I can provide more through explanations of the perils of this technology and it's use in this course during an in-class lecture, however it should be known that current student use of this technology is resulting in a decrease in learning quality and lower exercise scores. Offloading the learning process from the student is the least desired outcome of taking a college course, so its use here is frankly a waste of a student's tuition (but again, I do not ban its use. The decision is left in the hands of the student)

Class Recording:
Please refrain from recording the course in any way, without explicit written permission from the instructor. As this semester's class is F2F, I do not plan to record any material. Do not take photographs of anything (or anyone) during class, and do not distribute the course material under any circumstances.

Course Text: There is no required text for this course, as most of this material changes rapidly over short periods of time (sometimes within a semester). We will rely heavily on Instructor-provided guidance and online tutorials/documentation. Should students have monies to "burn", they may want to obtain *Computer Security*, 2nd Edition. Matt Bishop. ISBN-13 978-0321712332

[10] https://oai.gmu.edu/mason-honor-code/

Guidance for Recommendation Letters, GTA/RA opportunities, Research Opportunities

Each semester I get a few dozen emails, mostly from current or recent students asking for recommendation letters, or jobs as a GTA/UTA or RA. As an adjunct professor, I don't have a budget here at GMU. Email spam has become so untenable, that I need to post guidance in my course syllabi addressing this (and I apologize for the tone here as well, but I want to leave no confusion):

- **Please refrain from asking for letters, or job referrals unless you work on a project with or for me outside of degree coursework.** The volume and unprofessional nature of these requests is often so high that I almost always delete them without consideration, so the contents of your sales pitch are immediately lost. Attendance in my class is not a sufficient qualifier for a letter or referral as I am not given sufficient exposure to you or your work from which to base a recommendation on. It is also:
    - …rude to ask for, and rude to assume a professor would do so. It's even more rude if you ask more than once, and extremely rude if you don't take no for an answer.
    - Sending "follow up" emails asking for something that no one agreed to participate in will absolutely produce an outcome other than the one you wanted.
- **I do not recruit for my employer, and most students are not eligible to work there in the first place. It is not appropriate for me to recruit for an external employer during paid work for the university. Please do not ask me for a referral.**
    - You may, of course, ask about the industry in general or solicit advice, however, please respect this boundary.
- **If you have research interests that overlap mine, and you are ****genuinely***** interested in collaborating to produce a research product, you will need to talk to me in person and prepare a thirty second elevator speech. I am happy to talk through research ideas and areas, but only if you are prepared to have that conversation.** Otherwise, you should work with your full-time faculty advisor. Research is a learned process and I teach on a limited part-time basis, so I am not able to be a student's first instructor in the formal research process.

I understand that you may have been given advice on how to capitalize on an assertive nature, but aggressive behaviors from students seldom result in a positive outcome in academia. **You are expected to cultivate a sufficient understanding of how to communicate with professors effectively and appropriately. Keep that in mind when deciding how to communicate with faculty.**

Tentative Course Schedule

Day	Topic	Out (7:00pm)	Due (4:00pm)
08/21	Lab 0 – Initial VM Build and "Gear-Check." Exposure to exercise environment	Lab 0	
08/28	Lab 1 – Host Monitoring and Analysis In-Class Demo Exercise 0	Lab 1 Demo 0	Lab 0
09/04	University Holiday (No Class)		
09/05	Last day to Drop with 100% Tuition Refund		
09/11	Lab 2 – SIEM and Log Management In-Class Demo Exercise 1	Lab 2 Demo 1	Lab 1
09/18	Lab 3 – Network Monitoring and Analysis	Lab 3	
09/25	Lab 4 – Command and Control (C^2) and Exfil In-Class Demo Exercise 2	Lab 4 Demo 2	Lab 2
10/02	Lab 5 Anti-Virus , VirusTotal and Malicious Docs In-Class Demo Exercise 3	Lab 5 Demo 3	Lab 3
10/09	Fall Break (No Class)		
10/10	In-Class Demo Exercise 4 -Fall Break Make-up class-	Demo 4	Lab 4
10/16	Lab 6 – Targeted Network Monitoring with Zeek	Lab 6	
10/23	Lab 7 - Exploitation and Penetration Testing I In-Class Demo Exercise 5 (Working Session)	Lab 7 Demo 5	Lab 5
10/30	In-Class Demo Exercise 6 (Labs 5,6)	Demo 6	Lab 6
11/06	Lab 8 - Exploitation and Penetration Testing II In-Class Demo Exercise 7 (Working Session)	Lab 8 Demo 7	Lab 7
11/13	In-Class Demo Exercise 8 (Lab 7 focused)	Demo 8	
11/20	Experimental Lab "N" (Optional) In-Class Demo Exercise 9 (Working Session)	Lab "N" Demo 9	Lab 8
11/27	In-Class Demo Exercise 10 (Lab 8 focused) - Last day of in-person class -	Demo 10	
11/30			Lab N
12/14	Final Grades Due in Patriotweb		
12/16	Degree Conferral Date		