THE GEORGE WASHINGTON UNIVERSITY
School of Engineering and Applied Science
Online Programs Office

Syllabus for
SEAS 8414-D3C
Analytical Tools for Cyber Analytics

Fall-2 2022

Instructor: Ravi Mallarapu
eMail: mravi@gwu.edu
Credit Hours: 3 credit hours
Course Website: On Blackboard
Class Time and Dates:

- Day and Time: Saturday, 9 am – 12 pm (Eastern)
- All Class Meeting Dates: October 22, 29; November 5, 12, 19; December 3, 10, 17; January 7, 14
- Attendance is normally expected at all sessions. If an absence from a class meeting is needed (due to family/medical or work-related emergency) students must contact the instructor in advance.
- Online classes are conducted via Zoom; Links are provided in Blackboard.
- Zoom link for Office Hours: https://gwu-edu.zoom.us/my/mallarapu

Weekly Discussion on Blackboard:

- At the beginning of the course, I will post an assignment prompt on the discussion board and you will be randomly assigned to a discussion group. Throughout the course there will be milestones that need to be met by each discussion group. You are responsible for spending at least one hour each week collaborating within your group, and individually posting a one-paragraph response on Blackboard discussion board for your discussion group to see. Response due by 1 pm, every Friday.

Office Hours: For 3 hours every week I will be available for drop-in office hours, as follows:

- Every Friday 6-9 PM ET

Bulletin Description of the Course:
Survey of analytical tools for analyzing cyber security data with particular attention to the use of data analytics procedures in supporting appropriate cyber security policy decisions.

Course Learning Objectives:
Upon completing the course, students will know how to:

1. Create protection, detection, and response controls to secure your corporate infrastructure.
2. Understand the landscape of various security tools and the importance of data analytics.
3. Leverage probabilities and statistics to understand how threat analytics tools operate.
4. Learn how Cloud security posture, access broker, and endpoint workload protection work.
5. Understand how to use frameworks, threat intelligence, and security graphs for security operations.

Required Textbook and Other Materials:

- Reference Textbook: None
- Other Material: None

Average Amount of Out-of-Class or Independent Learning Expected per Week:
Over 10 weeks, students will spend 3 hours per week in lecture, 1 hour per week in Blackboard discussion, and 6 hours in two exams given outside class hours (about 46 hours of guided instruction for the semester). Homework and other out-of-class work is estimated at around twice the classroom time (92 hours) for a total of about 138 hours of work.

Class Schedule and Assignments

Class	Topic/Activity	Assignment Due
1) Oct 22	**Week-1: Introduction to enterprise cybersecurity framework** In the first class, we will start an Internet company called GWU Secure Crypto Currency Services (gwuscc.com), which makes cryptocurrency recommendations based on personal and financial information. We will build and deploy the infrastructure in **AWS Cloud** (all the students are required to register for a free AWS account). We will work on identifying distinct types of cyber-attacks, attackers, and stages of attack relevant to gwuscc.com. We will explore frameworks such as **MITRE ATT&CK** and secure architectures such as **Zero Trust** to protect our start-up.	Discussion 1
2) Oct 29	**Week-2: Learn about data-centric security tools** We will build a data-centric risk management program for gwuscc.com. We will learn about the role of assets, vulnerabilities, threats, risks, and controls. We will leverage probability to develop a **risk management plan**. We will discuss how hashing, fingerprinting, and signature techniques are leveraged by data-centric security controls such as Data Leak Prevention **(DLP)** and Content Disarm and Reconstruction **(CDR)** for audit, prevention, detection, and forensics.	Discussion 2 HW 1
3) Nov 5	**Week-3: Introduction to endpoint security analytics tools** We will shift the focus from data to endpoint-centric security tools for gwuscc.com. We will cover: • Endpoint Detection and Response (**EDR**) • Endpoint Protection Platform (**EPP**) • EXtended Detection and Response (**XDR**) We will learn about how XDR leverages time-series **data** from system event logs and leverages **regression** for **predictive analytics**. We will tie how data and asset-centric security are essential for an enterprise cybersecurity program.	Discussion 3
4) Nov 12	**Week-4: Secure Cloud Computing tools** So far, we have built data and endpoint-centric security for gwuscc.com. In this class, we will learn about how to build secure cloud computing using the following tools: • Cloud Security Posture Management (**CSPM**) • Cloud Workload Protection Platform (**CWPP**) • Cloud Access Security Broker (**CASB**) For hands-on activities, we will limit exercises to native **AWS** cloud offerings.	Discussion 4 HW 2 RPNow Check Exam

5) Nov 19	**Week-5: Code-centric security analytics tools** Since the data, servers, and infrastructure is secured, we will learn how to ensure the gwuscc.com code and supply-chain components are secure. We will cover the following tools: • Static Application Security Testing (**SAST**) • Dynamic Application Security Testing (**DAST**) • Software Composition Analysis (**SCA**) In order to understand how to interpret the results from these tools, you will be introduced to the concept of **expectations** and **variance**.	Discussion 5 Midterm Exam
6) Dec 3	**Week-6: Web-centric security tools** Now that we have established how to validate code security, we will cover how to secure the software application deployed in production. We will cover OWASP and the following tools: • Web Application Firewall (**WAF**) • Web Application Proxy (**WAP**) This class is primarily hands-on. You will be equipped with the basic skills required to perform web penetration testing. This class will use **Docker**, **Kali Linux**, and **ZAP Proxy**.	Discussion 6 HW 3
7) Dec 10	**Week-7: Log-centric detection analytics tools** Now that we have covered all the prevention controls for securing gwuscc.com, we will focus on detection engineering using log-centric tools. • Security Information and Event Management (**SIEM**) • Security Orchestration, Automation, and Response (**SOAR**) • Root Cause Analysis (**RCA**) for	Discussion 7
8) Dec 17	**Week-8: User security analytics tools** This lecture will shift the focus from digital assets to human beings. We will understand the role of motivation, indicators of compromise (**IOC**), and person of interest (**POI**) from gwuscc.com user and employee perspective. cover the following tools: • Identity and Access Management (**IAM**) • User and Entity Behavior Analytics (**UEBA**) • Insider Threat Detection Platform (**InTP**) In order to understand the operation of tools, we will learn about conditional probability and the Bayes theorem.	Discussion 8 HW 4

9) Jan 7	**Week-9: Advanced persistent threat analytics tools** This lecture will shift our focus from traditional cyber-attacks to targeted attacks. We will learn about the following frameworks and simulators to reinforce our understanding. • **MITRE ATT&CK** and **Shield** tools • **Kill chain** and Diamond Model • **ATP** Simulator and Caldera	Discussion 9
10) Jan 14	**Week-10: Collaborative security analytics tools** We will wrap-up the course with hands-on exposure to the tools in from the following collaborative security category: • Security Threat Intelligence (**STI**) • Threat hunting • Security Intelligence Graphs (**SIG**)	Discussion 10 HW 5 Final Exam
Midterm exam will be available from Saturday, Nov. 19, 8 pm ET, through Monday, Nov. 21, 8 pm ET.		
Final exam will be available from Saturday, Jan. 14, 8 pm ET, through Monday, Jan. 16, 8 pm ET.		

How Student Performance Will Be Evaluated on Assignments & Other Course Assessments:
There will be five homework assignments and weekly discussion topics for a total of 25% of the class grade. They will be discussed in class with students, when assigned. For all assignments, the requirements are to submit on-time and will be graded accordingly based on correctness and completeness.

Please see appendix for details of homework assignments and discussions.
No extra credit assignments will be available.

Exams:
- There will be a mid-term and a final exam, administered on Blackboard outside the class meeting time.
- There is a mandatory practice exam designed to make sure that your computer is compatible with RPNow and you have no IT issues accessing the midterm/final exam. It will take 5 minutes and you must complete it before end of Week 4. Failure to do so will prevent you from accessing the midterm exam and you will receive a grade of zero on your midterm.
- Both exams are closed book. Only calculators native to the PC or Mac as well as Excel may be used.
- Each exam is designed to be completed in 2.5 hours, with a 3-hour window to take it in.
- You are permitted to bring a single, 8.5"x11", reference sheet (front and back) to each exam, any format.
- **The exams are available for 48 hours. The mid-term will be released at 8 pm Eastern on Saturday,** Nov. 19 **and is due the following Monday, 8 pm Eastern. The final exam will be available at 8 pm eastern on Saturday,** Jan. 14**, the last week of classes and should completed and submitted no later than 8 pm on the following Monday. Please note the system allows you to start the exam as late as 7:59pm Eastern on the day it is due; however, our IT support ends at 8pm Eastern. Therefore, we strongly recommend that you start the exam prior to 5pm Eastern on the day it is due.**
    - Students are highly encouraged to take the exam early
    - Exams are proctored by Remote Proctor Now, which records the examinee's webcam, audio, and desktop. Certified reviewers confirm that the student adheres to the institution's and the faculty member's policies. Information about RPNow can be found at the following link: https://seasonline.gwu.edu/useful_links/
    - Contact Mark Griffith at seasonline@gwu.edu (202-422-2806) and copy instructor email regarding issues related to the exam in RPNow and/or Blackboard

Grading:

GW's grading system for graduate students is: ***A,*** Excellent; ***B,*** Good; ***C,*** Satisfactory; ***F,*** Fail; other grades that may be assigned are ***A–, B+, B–, C+,*** **C-**. In this course, grades are determined by weighted average values and based on a standard curve relative to the class average:

Homework, totaling:	20%
Discussion Board	5%
Exam 1	35%
Exam 2	40%

Withdrawals:

- Students may drop from courses through the day after the second class meeting without any academic or financial penalty. After that time, students may withdraw through the day after the eighth class meeting and will receive a designation of "W" and are responsible for full tuition.

Incomplete

- Students who cannot complete a course due to deployment overseas/called to active military duty/death in the immediate family/debilitating illness may seek an incomplete with proper documentation.

University Policy on Observance of Religious Holidays: Students should notify faculty during the first week of the semester of their intention to be absent from class on their day(s) of religious observance. See https://registrar.gwu.edu/university-policies#holidays

Student Disability Support Services (DSS) 202-994-8250: Students needing an accommodation based on the potential impact of a disability should contact Disability Support Services. See https://disabilitysupport.gwu.edu/.

Student Mental Health Services 202-994-5300: GW offers 24/7 assistance and referral for students needing crisis and emergency mental consultations, confidential assessment, and counseling services. See https://counselingcenter.gwu.edu/.

SEAS Online Programs Office Policies: https://seasonline.gwu.edu/about-us/policies-procedures-masters/

Emergencies: In case of emergency, students will be notified on Blackboard.

Course recordings: As part of the educational support for students, we provide downloadable recordings of each class session to be used exclusively by registered students in that particular class for their own private use. These recordings are available for the duration of the course and should only be used by registered students. *Releasing these recordings is strictly prohibited*.

SEAS Online Labs: Students can remotely access most computer labs of the School of Engineering and Applied Science and work with a variety of engineering design and analysis software packages. See https://www.seas.gwu.edu/remote-access-labs

Academic Integrity Code: Academic dishonesty is defined as cheating of any kind, including misrepresenting one's own work, taking credit for the work of others without crediting them and without appropriate authorization, and fabricating information. All academic work is subject to GW University and SEAS Online Programs policy and may be scrutinized electronically. For more information, see https://studentconduct.gwu.edu/.

Student Guidelines for "Remote Proctor Now" (RPNow)

RPNow is used with all online exams:

- Students must establish identity following the procedures outlined in the RPNow User Guide.
- Students are responsible for testing the functionality of the system well in advance of the remote-proctored exams in their courses so that any troubleshooting required can be accomplished. Check with your exam sponsor/faculty member for practice exams.

Review the RPNow video tutorial streaming recording link at:
https://youtu.be/wboTIkLpNaM

Test Environment Requirements

The online test environment should mimic the in-class test environment, and conform to the following:

Test Area

- Sit at a clean desk or table (not on a bed or couch).
- Ensure that lighting in the room is bright enough to be considered "daylight" quality. Overhead lighting is preferred; however, if overhead is not possible, the source of light should not be behind you.
- Clear the desk or table of all materials: Students can have a single sheet of 8.5 x 11 inch paper with handwritten or typed notes on the front and back only
- Use one computer monitor only; dual monitors are not permitted.
- Have no writing on desk or walls or any notes or writing saved as your computer desktop background.
- You must completely scan the room and testing area when prompted. For students with fixed desktops webcams, you must use a mirror to scan test area.
- No software other than RPNow and Blackboard should be open unless permitted by the instructor.
- Close all other programs and/or windows on the testing computer before logging in to the proctored test environment.
- Do not have a radio or television playing in the background.
- Do not talk to anyone else—you may not communicate with others by any means.
- No other persons except the test-taker is permitted in the room during testing.
- If a calculator is required, you may use the calculator that comes with the Mac or the Windows operating system only. No calculators will be allowed in the testing area.

Behavior

- Dress as if in a public setting
- You will be allowed to take a brief bathroom break during the exam. You should not leave the room for any other reason during the exam. Do not take the computer into another room to finish testing (exam must be completed in the same room as the "Exam Environment View").
- No headsets, ear plugs, or similar audio devices are permitted
- Cell phones are not permitted in the exam room. The only exception is if a student needs to contact RPNow at the beginning of an exam. Once reconnected students will be required to remove the cell phone from the environment.
- Your entire face must be visible throughout the exam. Being out of camera view is considered an exam violation. You should check the thumbnail at the top of the screen to confirm.
- Your ID photo should be readable if not you may be contacted via email by RPNow to resend your ID photo. Failure to comply is considered a violation.

Policy Violation Consequences

- Exams
    - **Minor Violations** – radio/TV in the background, someone enters the room, sitting on a couch, any part of face out of camera view briefly (less than 5 minutes in total), second monitor (off) on the desk, improper lighting, incomplete room scan, using headphones, wearing hats, sunglasses, etc.
        - If you are flagged for a minor violation, you receive a warning for the first offense. Students who commit minor violations after being warned will be penalized 10% on the exam. Subsequent minor violations could result in referral to the office of academic integrity. Minor violations will be counted cumulatively across the entire program.
    - **Major Violations** - browsing the web, using the phone or other devices, using additional screens, any part of face out of camera view (more than 5 min), communicating with another individual by any means.
        - If you are flagged for a major violation you will receive a 20% reduction on the exam and may be referred to the office of academic integrity.
- Homework and other written material
    - Written work must comply with the Academic Integrity Policy of the George Washington University policy. Any plagiarized material will receive a grade of 0.

Appendix: Homework Assignments and Discussions

HW Assignment	Description
HW 1	Design a start-up infrastructure for running a web service with sensitive data. We will discuss various frameworks and security controls you could use during the class.
HW 2	Design a client-server infrastructure leveraging data and endpoint security controls. We will go through the reference environments during the class.
HW 3	Design AWS-based application development environment with code and web security controls learned during the class. HW requires hands-on AWS experiences, which we will go through in class.
HW 4	Design data analytics dashboard using security data source. You will be using Splunk for this homework.
HW 5	Design a corporate infrastructure involving network, data, endpoint, code, web, and insider security controls.

Discussion Board	Description
Discussion 1	Summary of cybersecurity tools understanding and experience
Discussion 2	Summary of cybersecurity frameworks. I will post the related research papers.
Discussion 3	Summary of data security controls, known issues, and future developments
Discussion 4	Summary of endpoint security controls, similarities, and future
Discussion 5	Summary of cloud security controls and role of CSA and NIST
Discussion 6	Summary of commercial and open-source code analysis tools
Discussion 7	Summary of defensive and offensive web application security tools
Discussion 8	Summary of log analytics, correlation, and the role of machine learning
Discussion 9	Summary of insider threat detection, entity resolution, and social intelligence
Discussion 10	Summary of APT detection frameworks and the role of nation-state actors