George Mason University
Department of Electrical and Computer Engineering (ECE)
Digital Forensics and Cyber Analysis Program
DFOR/TCOM 663: Operations of Intrusion Detection for Forensics
Fall 2022

Course syllabus: ***This course syllabus is subject to revisions before and throughout the semester.***

Instructor

K. Hassan, Ph.D.
Email: khassan1@gmu.edu (preferred contact method)
Telephone: (703)592-8211
Office Hours: By appointment only, online meeting
Office Location: Engineering Building

Location & Time

DFOR/TCOM 663-001 Operation of Intrusion Detection for Forensic – CRN 77535/4
Location: Synchronous online. Online attendance required
Time: Thursdays 04:30 PM - 07:10 PM EST.

Textbooks (recommended)

Title: Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century

- Author: Ryan Trost
- Publisher: Addison-Wesley Professional
- Print ISBN-10: 0-321-59180-1

Additional Resources

1. Sanders, Chris and Smith, Jason. Applied Network Security Monitoring. Syngress, December 2013.
2. Collins, Michael S. Network Security Through Data Analysis. O'Reilly Media, 2014.
3. Bejtlich, Richard. The Tao of Network Security Monitoring: Beyond Intrusion Detection
4. Snort IDS User's Manual: http://manual.snort.org/
5. Zeek (Formerly Bro) IDS User's Manual: https://docs.zeek.org/en/master/

Course Description

663 Operations of Intrusion Detection for Forensics (3:3:0) Introduces students to network and computer intrusion detection and its relation to forensics. The class addresses intrusion detection architecture, system types, packet analysis, and products. It also presents advanced intrusion detection topics such as intrusion prevention and active response, decoy systems, alert correlation, data mining, and proactive forensics.

Course Objectives

At the conclusion of this course the student will have learned why and how intrusion detection systems are used and how they are applied in the forensics area. The student will also know how to implement an intrusion detection system, analyze packets, and construct signatures. The student will also have advanced knowledge of prevention and response technologies and other leading areas of research in intrusion detection and forensics.

Grading[1]

Raw scores may be adjusted to calculate final grades. Grades will be assessed on the following components:

IDS hands-on project assignments	55%
Participation/Attendance	5%
Midterm Exam: IDS research paper outline	15%
Final Exam: IDS research paper	25%

Below are the details of the course grade components:

Project Assignments:

In addition to the IDS research project, the following 5 computer forensic IDS related project exercises will be assigned throughout the semester. All assignments will be posted on the GMU course Blackboard.

1. **Project 1: Packet Forensic Analysis -** Project 1 assignment will contain practical exercises that will familiarize students with the IDS packet forensics using TCPDump and Wireshark network analyzers**.**
2. **Project 2: Snort IDS I** - Project 2 assignment will contain practical Snort IDS exercises that will familiarize students with intrusion forensic analysis using Snort Intrusion Detection System tool. In this assignment, students will learn and use existing Snort IDS Rules.
3. **Project 3: Snort IDS II** - Project 3 assignment will contain practical Snort IDS exercises that will familiarize students with intrusion forensic analysis using Snort Intrusion Detection System tool. In this assignment students, will configure and create new Snort IDS Rules.
4. **Project 4: Zeek (formerly Bro) IDS I-** Project 4 assignment will contain practical Bro IDS exercises that will familiarize students with packet forensic analysis using Bro Intrusion Detection System tool.
5. **Project 5: Zeek (formerly Bro) IDS II -** Project 5 assignment will contain practical Bro IDS exercises that will familiarize students with packet forensic analysis using Bro Intrusion Detection System tool. In this assignment, students will learn how to create and use Zeek IDS scripts.
6. **Project 6 (optional): Threat Simulator breach and attack simulation (BAS) platform project.** Project 6 assignment will be posted on the Blackboard, and it will contain practical exercises that will familiarize students with breach and attack simulation (BAS) using Keysight threat simulator tool.

Additional short hands-on assignments, questions, and quizzes: Additional short hands-on assignments, questions, and quizzes may be posted assigned and posted on the Blackboard. These short hands-on assignments, questions, and quizzes are designed to help students understand some of the key IDS packet analysis concepts in TCP/IP packets.

Va. Cyber Range (VaCR)

VaCR will be used during the semester if time permits. You will receive an email from the Va CR. Please log in and confirm your account to access the VaCR.

Assignments

All course assignments are due on the dates and times specified on the Blackboard assignment tap and they must be submitted on the Blackboard. Late assignment without prior approval from the professor will not be accepted after its due date and will receive zero grade.

[1] Homework assignment grade weights may be adjusted to calculate the final total homework grade percentage.

Class attendance and participation
Active participation/attendance required and is expected of all students. The class will discuss about recently published IDS related research articles.

Midterm Exam
Midterm exam will contain materials covered week 1 to 7. More information about the midterm exam will be provided during the midterm exam review session and will be posted on the Blackboard.

Final Exam
For the final exam, students will write a research paper about an IDS topic. More information about the final exam research paper will be provided during the class lectures and will be posted on the Blackboard.

Tentative Course Schedule (subject to changes)

Date	Week	Topic	Reading Assignments	Assignment due
25-Aug	1	Intrusion detection systems (IDS) overview, network overview and TCP/IP review.	Install/Configure VMware, TCDump, WireShark, and snort tools. Read chapter 1	
1-Sep	2	IDS packet forensics analysis: Network monitoring and tools	Read chapter 2	
08-Sep	3	IDS fundamentals: IDS packet forensics analysis.	Read chapter 3	Project 1 TCPDump
15-Sep	4	Fundamentals of signature-based IDS: Introduction to Snort:	Read chapter 4	
22-Sep	5	Fundamentals of signature-based IDS: Snort signature analysis	Read chapter 5	Project 2 Snort IDS I
29-Sep	6	IDS Sensors and Mobile IDS/IPS	Read chapter 6	Final research paper IDS topic selection
06-Oct	7	Snort IDS rules analysis – Midterm Exam review	Read chapter 7/8	Project 3 Snort IDS II
13-Oct	8	**Midterm Exam**		Research paper outline & references
20-Oct	9	Fundamentals of anomaly-based IDS: Introduction to Zeek IDS	Install and Configure Zeek IDS	
27-Oct	10	Zeek IDS analysis Zeek IDS scripts	Read Zeek docs.	Project 4 Zeek IDS I
03-Nov	11	Zeek IDS	Read chapter 10	
10-Nov	12	Advanced IDS	Read chapter 11	
17-Nov	*13*	IDS Log analysis		Project 5 Zeek IDS II
24-Nov	14	*Thanksgiving Recess*	No class	
01-Dec	15	Final research paper presentation PowerPoint summary		Final research paper presentation PowerPoint - summary
08-Dec	16	**Final Exam**		Final Research paper due

This schedule is subject to revision before and throughout the semester. Make sure you always use the latest version that is posted on the GMU DFOR/TCOM 663 course Blackboard.
Call 703-993-1000 for recorded information on campus closings (*e.g.,* due to weather)

Basic Course Technology Requirements:
Activities and assignments in this course will regularly use the Blackboard learning system, available at https://mymason.gmu.edu. Students are required to have regular, reliable access to a computer with an

updated operating system and a stable broadband Internet connection. Hands-on projects in this course will require students to use the following software:

- Free student license VMware workstation Pro 16.x software available at GMU https://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?cmi_mnuMain=16a020b5-ed3c-df11-b4ab-0030487d8897&ws=57245579-6f24-de11-a497-0030485a8df0&vsro=8
- Free WireShark available at https://www.wireshark.org/
- Free Snort IDS available at https://www.snort.org/
- Free Zeek (formerly Bro) IDS available at https://www.snort.org/
- Free trial Keysight threat Simulator available at https://www.keysight.com/us/en/products/network-security/breach-defense/threat-simulator.html

Attendance Policy

Students are expected to attend each class, to complete any required preparatory work (including assigned reading) and to participate actively in lectures, discussions, and exercises. As members of the academic community, all students are expected to contribute regardless of their proficiency with the subject matter.

Students are expected to make prior arrangements with instructor if they know in advance that they will miss any class and to consult with the instructor if they miss any class without prior notice.

Departmental policy requires students to take exams at the scheduled time and place, unless there are truly compelling circumstances supported by appropriate documentation. Except in such circumstances, failure to attend a scheduled exam may result in a grade of zero (0) for that exam.

Communications

Communication on issues relating to the individual student should be conducted using email or telephone. Email is the preferred method – for urgent messages, you should also attempt to contact the instructor via telephone. Email messages from the instructor to all class members will be sent to students' GMU email addresses – if you use another email account as your primary address, you should forward your GMU email to that account.

Lecture slides are complements to the lecture process, not substitutes for it. Access to lecture slides will be provided as a courtesy to students provided acceptable attendance is maintained.

Honor Code

The integrity of the University community is affected by the individual choices made by each of us. Mason has an Honor Code with clear guidelines regarding academic integrity. Three fundamental and rather simple principles to follow at all times are that: (1) all work submitted be your own; (2) when using the work or ideas of others, including fellow students, give full credit through accurate citations; and (3) if you are uncertain about the ground rules on a particular assignment, ask for clarification. No grade is important enough to justify academic misconduct. Plagiarism means using the exact words, opinions, or factual information from another person without giving the person credit. Writers give credit through accepted documentation styles, such as parenthetical citation, footnotes, or endnotes. Paraphrased material must also be cited, using IEEE reference format. A simple listing of books or articles is not sufficient. Plagiarism is the equivalent of intellectual robbery and cannot be tolerated in the academic setting. If you have any doubts about what constitutes plagiarism, please see me.

Students are required to be familiar and comply with the requirements of the GMU Honor Code: https://oai.gmu.edu/mason-honor-code/. The GMU Honor Code will be strictly enforced in this course. All assessable work is to be completed by the individual student. Students must **NOT** collaborate on the project reports or presentation without explicit prior permission from the instructor.

Office of Disability Services

If you have a documented learning disability or other condition that may affect academic performance, you should:

1. Make sure this documentation is on file with Disability Services (SUB I, Rm. 4205; 993-2474; http://ds.gmu.edu) to determine the accommodations you need; and
2. Talk with me to discuss your accommodation needs.

If you are a student with a disability and you need academic accommodations, please see me and contact Disability Services at email ods@gmu.edu or call 703.993.2474, http://ds.gmu.edu. All academic accommodations must be arranged through Disability Services.

Important Dates:

Important GMU calendar dates are published on the GMU registrar website:
https://registrar.gmu.edu/calendars/fall_2022/
Make sure that you check and verify on the official GMU Registrar Web page for updated and latest date information.

Religious Holidays and Observations

Information regarding the calendar of religious holidays and observations is available on the GMU Student Life Website:
http://ulife.gmu.edu/calendar/religious-holiday-calendar/
Let me know in advance if you will have any difficulty with the course assignment schedule.