CFRS 663/TCOM 663 – Operations of Intrusion Detection for Forensics
Department of Electrical and Computer Engineering (ECE)
George Mason University
Fall, 2018

Course Syllabus Rev. 1.
This Course Syllabus is subject to revision before and throughout the semester. Make sure you always use the latest version available on the GMU Blackboard website for the CFRS/TCOM 663 course.

Instructor

K. Hassan, Ph.D.
Email: khassan1@gmu.edu (preferred contact method)
Telephone: (703)592-8211. (703) 993-5528.
Office Hours: By appointment only
Office Location: Engineering Building, Room 4457

Location & Time

Operation of Intrusion Detection for Forensic – 72818 - CFRS 663-001
Operation of Intrusion Detection for Forensic – 72819 - TCOM 663-001
Location: Innovation Hall 129
Time: Wednesday 07:20 PM - 10:00 PM.

Textbooks (recommended)

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

- **Author:** Ryan Trost
- **Publisher:** Addison-Wesley Professional
- **Pub. Date:** June 24, 2009
- **Print ISBN-10:** 0-321-59180-1
- **Print ISBN-13:** 978-0-321-59180-7
- **Web ISBN-10:** 0-321-59189-5
- **Web ISBN-13:** 978-0-321-59189-0

Additional Resources:

1. Sanders, Chris and Smith, Jason. Applied Network Security Monitoring. Syngress, December 2013.
2. Koziol, Jack. Intrusion Detection with Snort. Sam's publishing, 2003.
3. Collins, Michael S. Network Security Through Data Analysis. O'Reilly Media, 2014.
4. Snort IDS User's Manual: http://manual.snort.org/
5. Bro IDS User's Manual: https://www.bro.org/sphinx/index.html
6. Scarfone, Karen and Mell, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology, Gaithersburg. 2007.
7. Caswell, Brian, *Snort 2.1 Intrusion Detection*, Second Edition. Syngress. 2004.
8. Rehman, Rafeeq. *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID*. Prentice Hall. 2003.

9. Rash, Mike. *Intrusion Prevention and Active Response: Deploying Network and Host IPS*. Syngress. 2005.

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.

Prerequisites

TCOM 509, 529, and a working knowledge of computer programming.

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:

Hands-on and homework Assignments	60%
Class attendance and participation	10%
Final Exam	30%

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.

1. **Project 1: Packet Forensic Analysis -** Project 1 assignment will be posted on the Blackboard and it 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 be posted on the Blackboard and it will contain practical Snort IDS exercises that will familiarize students with intrusion forensic analysis using Snort Intrusion Detection System tool.

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

3. **Project 3: Snort IDS II -** Project 3 assignment will be posted on the Blackboard and it will contain practical Snort IDS exercises that will familiarize students with forensic analysis using Snort Intrusion Detection System tool. In this assignments students will configure and create Snort IDS Rules.

4. **Project 4: Bro IDS -** Project 3 assignment will be posted on the Blackboard and it will contain practical Bro IDS exercises that will familiarize students with packet forensic analysis using Bro Intrusion Detection System tool..

5. **Project 5: IDS Log Analysis** - Project 5 assignment will be posted on the Blackboard and it will contain practical IDS log analysis exercises that allows students to solve and develop an automated IDS forensic log file analysis using programming scripting skills.

Additional short in-class hands-on assignments: Additional short hands-on assignments will be posted on the Blackboard. These hands-on assignments are designed to help students some of the basic IDS packet analysis concepts in TCP/IP packets.

All homework assignments are due on the dates and times defined on the Blackboard assignment tap and they must be submitted on the Blackboard. Late assignments will not be accepted by the Blackboard after its due date.

Class attendance and participation

Active participation/attendance is expected of all students. For more information about the class Participation and attendance, see the class participation and attendance rubric posted on the GMU Blackboard link for the CFRS/TCOM 663 course, under the syllabus tap.

Final Exam

For the final exam, students will write a research paper about IDS and how it is used in computer forensics. More information about the final exam research paper will be posted on the Blackboard.

Course Schedule (tentative)

Date	Week	Topic	Assignments
29-Aug	1	Intrusion detection systems (IDS) overview, network overview and TCP/IP review.	Read Ch. 1. Configure VMware and Snort
5-Sep	2	IDS packet forensics analysis: Network monitoring, network analysis tools and packet sniffing.	Read Ch. 2. Configure VMware and Snort due at 11:59PM
12-Sep	3	IDS fundamentals: IDS packet forensics analysis.	Read Ch. 3.

			TCPdump/WireShark Assignment due at 11:59pm
19-Sep	4	Fundamentals of signature based IDS: Introduction to Snort:	Read Ch. 4
26-Sep	5	Fundamentals of signature based IDS: Snort signature analysis	Read Ch. 5. Snort Assignment I is due on 09/30 at 11:59pm
3-Oct	6	IDS Sensors	Read Ch. 6 and 7
10-Oct	7	Mobile IDS/IPS	Read Chapter 8. Snort Assignment II is due at 11:59pm
17-Oct	8	Fundamentals of anomaly-based IDS: Introduction to Bro IDS	Configure Bro, ELSA, and Security Onion.
24-Oct	9	Bro IDS analysis	
31-Oct	10	Bro IDS scripts	Bro Assignment due at 11:59pm
7-Nov	11	Bro IDS scripts	
14-Nov	12	Bro IDS in-class hands-on exercises	
21-Nov	*13*	*Thanksgiving Recess*	*(No Class)*
28-Nov	14	Log analysis project will be performed in-class.	Log Analysis project assignment is due at 11:59pm
5-Dec	15	Advanced IDS and new IDS applications	
12-Dec	16	Final Exam-in-class. Final research paper presentations for all students. 7:30 pm – 10:15 pm	Final Project Presentations, Final Paper due at 11:59pm

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 CFRS/TCOM 663 course Blackboard.

Call 703-993-1000 for recorded information on campus closings (*e.g.* due to weather).

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 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:
http://registrar.gmu.edu/calendars/fall-2018/

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 for 2011-2015 academic years 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.