

**CFRS 663/TCOM 663 – Operations of Intrusion Detection for Forensics**  
**Department of Electrical and Computer Engineering**  
**George Mason University**  
**Fall, 2017**

Course Syllabus Rev. 1.

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

**Instructor**

**Dr. K. Hassan**

Email: [khassan1@gmu.edu](mailto:khassan1@gmu.edu)

Telephone: (703)592-8211. (703) 993-5528.

Office Hours: By appointment only

Office Location: Engineering Building, Room 3707

**Location & Time**

Operation of Intrusion Detection for Forensic – 73279 - CFRS 663-001

Operation of Intrusion Detection for Forensic – 73280 - 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<sup>1</sup>**

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

Hands-on and homework Assignments	60%
1 Mid-Term Exam	20%
1 Final Exam	20%

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.

---

<sup>1</sup> 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 provide students some of the basic IDS packet analysis concepts.

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.

### **Mid-term Exam**

Mid-term exam will cover materials discussed in class from weeks 1 to 6. More information about the midterm exam will be provided during the class lectures.

### **Final Exam**

Final exam will cover materials discussed in class from weeks 9 to 15. More information about the final exam will be provided after the midterm exam.

### **Course Schedule (tentative)**

<b>Date</b>	<b>Week</b>	<b>Topic</b>	<b>Assignments</b>
30-Aug	1	Intrusion detection systems (IDS) overview, network overview, TCP/IP review	Read Ch. 1. Configure VMware and Snort
6-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
13-Sep	3	IDS essentials: IDS packet forensics analysis.	Read Ch. 3. TCPdump Assignment due at 11:59pm

20-Sep	4	Fundamentals of signature based IDS: Introduction to Snort:	Read Ch. 4
27-Sep	5	Fundamentals of signature based IDS: Snort signature analysis	Read Ch. 5. Snort Assignment I is due at 11:59pm
4-Oct	6	Mobile IDS/IPS	Read Ch. 6
11-Oct	7	Midterm Exam: in-class (Covers week 1 – 6).	
18-Oct	8	Fundamentals of anomaly based IDS: Introduction to Bro IDS	Configure Bro, ELSA, and Security Onion.
25-Oct	9	Fundamentals of anomaly based IDS: Bro IDS analysis	Configure Bro, ELSA, and Security Onion.
1-Nov	10	Bro IDS analysis	
8-Nov	11	Bro IDS scripts	Bro Assignment due at 11:59pm
15-Nov	12	Bro IDS in-class hands-on exercises	
22-Nov	13	<b>Spring Break Recess</b>	<b>(No Class)</b>
29-Nov	14	Log analysis project will be performed in-class.	Log Analysis project assignment is due at 11:59pm
6-Dec	15	Final research paper preparations	
13-Dec	16	Final Exam-in-class. Final research paper presentations for ALL students.	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**

Students are required to be familiar and comply with the requirements of the GMU Honor Code:

<http://oai.gmu.edu/the-mason-honor-code-2/>

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 are a student with disability and you need academic accommodations, please see me and contact the Office of Disability Services (ODS) at 993-2474. All academic accommodations must be arranged through the ODS.

## **Key Dates:**

Important GMU calendar dates are published on the GMU registrar website:

<http://registrar.gmu.edu/calendars/fall-2017/>

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.

---