CFRS 663/TCOM 663 – Operations of Intrusion Detection for Forensics
Department of Electrical and Computer Engineering
George Mason University
Spring, 2015

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 Blackboard.

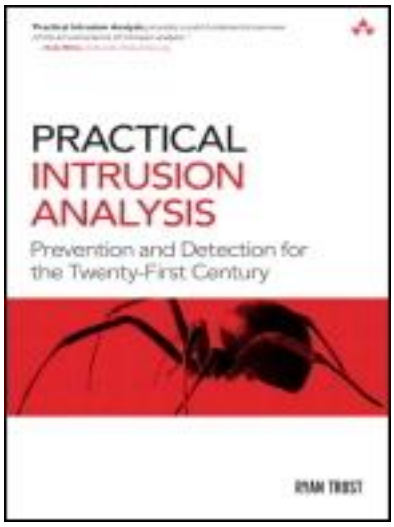
Instructor

Dr. K. Hassan
Email: khassan1@gmu.edu
Telephone: (703) 993-5528/1645
Office Hours: By appointment only
Office Location: Engineering Building, Room 3707

Location & Time

Operation of Intrusion Detection for Forensic – 11814 - CFRS 663-001
Operation of Intrusion Detection for Forensic – 11817 - TCOM 663-001
Location: Nguyen Engineering Building 4457
Time: Wednesday 4:30 PM.-07:10 PM.

Textbooks



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. Bace, Becky. *Intrusion Detection.* Sams. 1st edition. 1999.
2. Caswell, Brian, *Snort 2.1 Intrusion Detection*, Second Edition. Syngress. 2004.
3. Rehman, Rafeeq. *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID*. Prentice Hall. 2003.
4. Rash, Mike. *Intrusion Prevention and Active Response: Deploying Network and Host IPS*. Syngress. 2005.
5. Northcutt, Stephen. *Network Intrusion Detection*, 3rd Edition. New Riders. 2003.
6. Northcutt, Stephen. *Intrusion Signatures and Analysis.* New Riders. 2001.
7. Mohay, George. *Computer and Intrusion Forensics*. Artech House Publishers. 2003.
8. Marchette, David. *Computer Intrusion Detection and Network Monitoring: A Statistical Viewpoint.* Springer. 2001.
9. Kohlenberg, Toby *Snort IDS and IPS Toolkit*, Syngress, 2007
10. Archibald, Neil, et. al. *Nessus, Snort, & Ethereal Power Tools Customizing Open Source Security Applications* 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

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

Homework Assignments	55%
1 Mid Term Exam	20%
1 Final Exam:	20%

Attendance 5%

Homework Assignments*:
The following four IDS related forensic homework exercises will be assigned throughout the semester.

1. **Homework 1: Packet Forensic Analysis -** Homework 1 assignment will be posted on the Blackboard and it will contain practical exercises that will familiarize students with the IDS forensics using TCPDump and Wireshark network analyzers**.**

2. **Homework 2: Snort IDS** - Homework 2 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.

3. **Homework #3: Bro IDS -** Homework 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..

4. **Homework #4: IDS Log Analysis** - Homework 4 assignment will be posted on the Blackboard and it will contain practical IDS log analysis exercises that allows students to develop an automate IDS forensic log file analysis using software programming scripts.

5. **Homework #5: IDS Technical Specification Design -** Homework 5 assignment will be posted on the Blackboard and it will contain practical IDS Technical specification design that will allow students to develop and design practical IDS specifications for practical network.

   Additional short in-class hands-on assignments: Additional short hands-on assignments may be posted on the Blackboard. These hands-on assignments are designed to provide students some of the basic IDS packet analysis concepts.
   *Homework assignment grade weights may be adjusted to calculate the final total homework grade percentage**.**

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 be assessed a penalty of 10% of the assignment grade for each day or part there of it is late. No homework or hands-on assignment will be accepted after the third week.

Mid-term Exam
The mid-term exam will cover materials discussed in class from weeks 1 to 6.

Final Exam
The final exam will cover materials discussed in class from weeks 8 to 15. More information about the final exam will be provided after the midterm exam.

Schedule (Tentative)

Date	Week	Topic	Chapters
1/21	1	Course overview, network overview**,** TCP/IP review	1
1/28	2	Packet forensics analysis Part I: network monitoring and analysis tools and packet sniffing.	2
2/4	3	Packet forensics analysis Part II: Intrusion detection systems IDS groundwork.	3
2/11	4	Fundamentals of IDS Part I:	4
2/18	5	Fundamentals of IDS Part II: Introduction to Snort:	5
2/25	6	Network flows and anomaly detection IP data flows, NetFlow operational theory.	6
3/4	7	Midterm Exam (Covers week 1 – 6).	-
3/11	8	*Spring Recess (No Class)*	
3/18	9	Snort signatures analysis, wireless IDS/IPS	7
3/25	10	Bro IDS	8
4/1	11	Advanced Intrusion Detection and Intrusion Prevention Techniques	9
4/8	12	Intrusion detection current uses of geocoding,	10
4/15	***13***	Advanced IDS Methods for behavior analysis and proactive forensics visual data communications	11
4/22	14	IDS Technical Specification	-
4/29	15	Advanced IDS	-
5/6	16	Final Exam	-

This schedule is subject to revision before and throughout the semester. Make sure you always use the latest version that is available on the 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[1].

The 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/spring-2015/

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.

[1] Available at www.gmu.edu/catalog/apolicies/honor.html and related GMU Web pages.