CFRS 663/TCOM 663 – Operations of Intrusion Detection for Forensics
Department of Electrical and Computer Engineering
George Mason University
Fall, 2013

Course Syllabus Revised: August 19, 2013.

Instructor

Dr. Kafi Hassan
Email: khassan1@gmu.edu
Telephone: (703) 592-8211
Office Hours: By email, phone or by appointment only
Office Location: Engineering Building, Room 3707

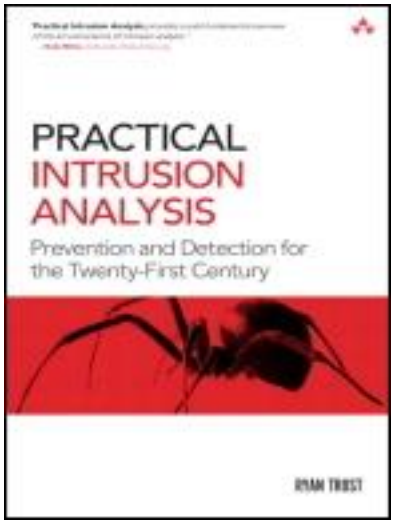
Teaching Assisting

TBD
Email: TBD
Telephone: TBD
Office Hours: TBD
Office Location: TBD

Location & Time

Operation of Intrusion Detection for Forensic – 72057 - CFRS 663-001
Operation of Intrusion Detection for Forensic – 70141 - TCOM 663-001
Location: Nguyen Engineering Building 1505
Time: Wednesday 7:20 PM.-10:00 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:

4 Homework Assignments (15% each):	60%
Mid Term Exam	20%
Final Exam	20%

Grading components are outlined in the following sections:

Homework Assignments:

The following four forensic IDS related homework exercises will be assigned throughout the semester.

1. **Homework 1: TCPDump/Wireshark -** Homework 1 assignment will be posted on the Blackboard and it will contain practical exercises that will familiarize you with the IDS forensics using TCPDump/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 you with forensic analysis using Snort Intrusion Detection System tool.
3. **Homework #3: IDS Log Analysis** - Homework 3 assignment will be posted on the Blackboard and it will contain practical IDS log analysis exercises that allows you to analyze IDS forensic logs file using software programming scripts.
4. **Homework #4: Bro IDS -** Homework 4 assignment will be posted on the Blackboard and it will contain practical Bro IDS exercises that will familiarize you with forensic analysis using Bro Intrusion Detection System tool.

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 25% of the assignment grade for each week 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 be take home exam and will cover materials discussed in class from weeks 1 to 6. Midterm exam will be released one week before its due date. No collaborations are authorized.

Final Exam

Each student should pick a research paper with a focus on intrusion detection systems for forensics and write a response/critique of the paper. Do not just repeat what the authors say, think about what they are saying and what they are possibly missing. Your critique should include the following:

1. A summary of what was done.
2. What are the central contributions of the paper?
3. A summary of related work.
4. What are the principal shortcomings of the technical content of the paper?
5. Other advantages and disadvantages of the technique.
6. Future research that may be done in the addressed area.

This is an individual assignment. You are required to complete it on your own without assistance of anyone.

1. Papers must be 5-10 pages in length.
2. Papers may be accessed through the IEEE or ACM Digital Library accessible through GMU or other search engines.
3. You will present your findings and analysis in class.
4. The final paper is due on presentation day and must be submitted on the Blackboard before its due date.

Schedule

Date	Week	Topic	Chapters	Assignments
28 Aug.	1	Course overview, Network Overview**,** TCP/IP review	1	
4 Sept.	2	Packet Analysis Part 1: Monitoring Network-Analysis Tools and Packet Sniffing.	2	
11 Sept.	3	Packet Analysis Part 2: Intrusion Detection Systems IDS.	3	HW 1 due
18 Sept.	4	Fundamentals of IDS Part 1: Introduction to Snort:	4	
25 Sept.	5	Fundamentals of IDS Part 2: Proactive Intrusion Prevention and Response via Attack Graphs Topological Vulnerability.	5	HW 2 due
02 Oct.	6	Network Flows and Anomaly Detection IP Data Flows NetFlow Operational Theory,	6	
09 Oct.	7	Midterm Exam (Covers week 1 – 6).	-	
16 Oct.	8	Snort Signatures and Analysis. Web application Firewalls and web threat overview.	7	
23 Oct.	9	Wireless IDS/IPS	8	HW 3 due
30 Oct.	10	Physical Intrusion Detection for IT, origins of Physical Security, Advanced Intrusion Detection and Intrusion Prevention Techniques	9	
06 Nov.	11	Intrusion Detection Current Uses of Geocoding, Alert Correlation for Incident and Forensic Analysis	10	HW 4 due
13 Nov.	12	Visual Data Communications Introduction to Visualization, Advanced IDS Methods for Behavior Analysis and Proactive Forensics	11	
20 Nov.	***13***	Advanced IDS	-	
27 Nov.	14	***Thanksgiving Recess (No Class)***	-	
04 Dec	15	Final Research Paper Presentation	-	
11 Dec.	16	Final Research Paper Presentation	-	

This schedule is subject to revision before and throughout the course.

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:
For complete GMU key dates, refer to the official GMU Registrar Website at:
http://registrar.gmu.edu/calendars/2013fall/
Make sure that you understand and know all important dates listed on the official GMU Registrar Calendars Website.

Religious Holidays and Observations
Information regarding the calendar of religious holidays and observations for 2011-2015 academic year is available on the GMU Student Life Website: http://ulife.gmu.edu/calendar/religious-holiday-calendar/.
Please 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.