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

Course Syllabus Revised: Jan 11, 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 5358

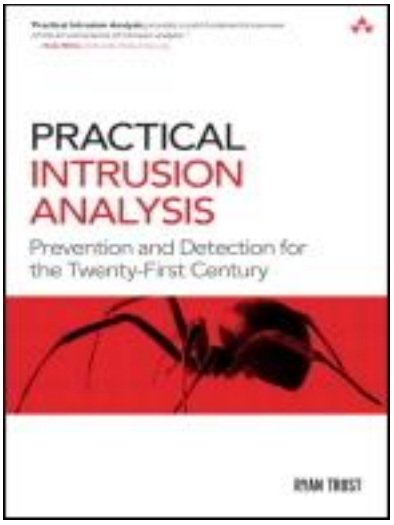
Teaching Assisting

TBD

Location & Time

Operation of Intrusion Detection for Forensic - 12415 - CFRS 663-001
Operation of Intrusion Detection for Forensic - 12419 - TCOM 663-001
Location: Nguyen Engineering Building 5358
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:	10%
Practical IDS Exercises Assignments:	35%

Mid Term Exam	25%
Final Exam:	30%

Grading components are outlined in the following sections:

Practical IDS Exercise Assignments:

Three practical IDS forensic exercises will be assigned throughout the semester.

1. **Hands-on Exercise 1: TCPDump/Wireshark -** Hands-on Exercise 1 will be posted on the Blackboard and it will contain practical exercises that will familiarize you with the TCPDump and Wireshark network analyzers**.** ***This hands-on exercise is due before class on Feb. 13.***

2. **Hands-on Exercise #2: Snort IDS** - Hands-on Exercise 2 will be posted on the Blackboard and it will contain practical Snort IDS exercises that will familiarize you with the Snort Intrusion Detection System. ***This hands-on exercise is due before class on Feb. 27.***
3.
4. **Hands-on Exercise #3: Snort IDS:** - Hands-on Exercise 3 will be posted on the Blackboard and it will contain practical Snort IDS exercises that will familiarize you with the Snort Intrusion Detection System. ***This hands-on exercise is due before class on March 27.***
5.
6. **Hands-on Exercise #4: Bro IDS:** - Hands-on Exercise 4 will be posted on the Blackboard and it will contain practical Bro IDS exercises that will familiarize you with the Snort Intrusion Detection System. ***This hands-on exercise is due before class on April 24.***
7.
8. **Hands-on Exercise #5: IDS Log Analysis** - Hands-on Exercise 3 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. ***This hands-on exercise is due before class on May 07.***
9.

Homework Assignments:

1. **Homework 1 -** This home work will be posted on the Blackboard website and must be submitted *by Jan. 30 at 4:30PM.*
2. **Homework 2 –** This home work will be posted on the Blackboard website and must be submitted *by April 10 at 4:30PM.*

All homework and hands-on exercise 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.

Midterm exam

The midterm exam will be in-class exam and will cover materials discussed in class from week 1 to 6.

Final Exam

The Final exam will be in-class exam and will cover materials discussed in class from week 7 to 16.

Schedule

Date	Week	Topic	Chapters	Assignments
23 Jan.	1	Course overview and Network Overview, TCP/IP review	1	
30 Jan.	2	Packet Analysis Part 1: Monitoring Network-Analysis Tools and Packet Sniffing.	2	HW 1 due
06 Feb.	3	Packet Analysis Part 2: Intrusion Detection Systems IDS Groundwork,	3	
13 Feb.	4	Fundamentals of IDS Part 1: Lifecycle of Vulnerability.	4	Hands-on Exercise 1 due
20 Feb.	5	Fundamentals of IDS Part 2: Proactive Intrusion Prevention and Response via Attack Graphs Topological Vulnerability.	5	
27 Feb.	6	Network Flows and Anomaly Detection IP Data Flows NetFlow Operational Theory, Introduction to Snort:	6	Hands-on Exercise 2 due
6 March	7	In-class Midterm Exam (Covers week 1 – 6).	-	
13 Mar.	8	**Spring Break**		
20 Mar.	9	Snort Signatures and Analysis. Web application Firewalls and web threat overview.	7	
27 Mar.	10	Wireless IDS/IPS	8	Hands-on Exercise 3 due
03 Apr.	11	Physical Intrusion Detection for IT, origins of Physical Security, Advanced Intrusion Detection and Intrusion Prevention Techniques	9	
10 Apr.		Intrusion Detection Current Uses of Geocoding, Alert Correlation for Incident and Forensic Analysis	10	HW 2 due
17 Apr.	12	Visual Data Communications Introduction to Visualization,	11	
24 Apr.	***13***	Advanced IDS Methods for Behavior Analysis and Proactive Forensics	*12*	Hands-on Exercise 4 due
01 May	14	Advanced IDS	-	
07 May	15	Advanced IDS	-	Hands-on Exercise 5 due
15 May.	16	In-class Final Exam (Covers week 7 –16)	-	

This schedule is subject to revision before the start of the semester and throughout the semester.

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 *:

January 1 Day of Week	*Tuesday*
Martin Luther King Day (no classes)	Mon Jan 21
First day of classes; last day to submit Domicile Reclassification Application; Payment Due Date; full semester waitlists removed	Tue Jan 22
Summer 2013 Graduation Intent Available via Patriot Web	Mon Jan 28
Last day to add classes—all individualized section forms due **Last day to drop with no tuition penalty**	Tues Jan 29
Last day to drop with a 33% tuition penalty	Tues Feb 12
Final Drop Deadline (67% tuition penalty)	Fri Feb 22
Last day to file your Spring 2013 Graduation Intent	Fri Feb 22
Immunization Record Deadline	Fri Mar 1
Midterm progress reporting period (100-200 level classes)—grades available via Patriot Web	Mon Feb 18 - Fri Mar 22
Selective Withdrawal Period (undergraduate students only)	Mon Feb 25 - Fri Mar 29
Spring Break	Mon Mar 11 - Sun Mar 17
Incomplete work from Fall 2012 due to instructor**	Fri Mar 29
Incomplete grade changes from Fall 2012 due to registrar**	Fri Apr 5
Dissertation/Thesis Deadline**	Fri May 3
Last day of classes	Mon May 6
Reading Days*	Tue May 7
Exam Period (beginning at 7:30 a.m.)	Wed May 8 - Wed May 14
Commencement and Degree Conferral Date	May 18, 2013

* These Key Dates are http://registrar.gmu.edu/calendars/2013Spring.html 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 year is available on the GMU Student Life Website: http://ulife.gmu.edu/religious_calendar.php.
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.