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

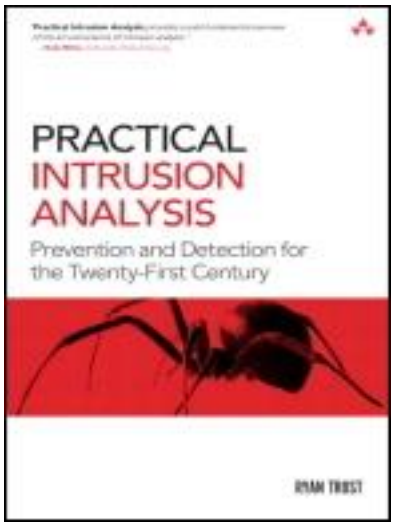
Instructor

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 – 75140 - CFRS 663-001
Operation of Intrusion Detection for Forensic – 75141 - TCOM 663-001
Location: Nguyen Engineering Building 5358
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. Snort IDS User's Manual: http://manual.snort.org/
2. Bro IDS User's Manual: https://www.bro.org/sphinx/index.html
3. Scarfone, Karen and Mell, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS), National Institute of Standards and Technology, Gaithersburg. 2007.
4. Caswell, Brian, *Snort 2.1 Intrusion Detection*, Second Edition. Syngress. 2004.
5. Rehman, Rafeeq. *Intrusion Detection with SNORT: Advanced IDS Techniques Using SNORT, Apache, MySQL, PHP, and ACID*. Prentice Hall. 2003.
6. Rash, Mike. *Intrusion Prevention and Active Response: Deploying Network and Host IPS*. Syngress. 2005.
7. Northcutt, Stephen. *Network Intrusion Detection*, 3rd Edition. New Riders. 2003.
8. Northcutt, Stephen. *Intrusion Signatures and Analysis.* New Riders. 2001.
9. Mohay, George. *Computer and Intrusion Forensics*. Artech House Publishers. 2003.
10. Kohlenberg, Toby *Snort IDS and IPS Toolkit*, Syngress, 2007
11. 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[1]

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

Hands-on and homework Assignments	40%
Research paper investigation and analysis	30%

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

1 Mid Term Exam	15%
1 Final Exam:	15%

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 packet forensics using TCPDump and Wireshark network analyzers**.**

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

4. **Homework #4: 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..

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

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.

Final Exam
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.

Course Schedule (Subject to Change)

Date	Week	Topic	Chapters	Assignments
02-Sep	1	Intrusion detection systems (IDS) overview, network overview**,** TCP/IP review	1	Read Ch. 1 Configure VMware and Snort
09-Sep	2	IDS packet forensics analysis Part I: network monitoring and analysis tools and packet sniffing.	2	Read Ch. 2 **TCPdump Assignment due at 11:59pm**
16-Sep	3	IDS packet forensics analysis Part II: IDS groundwork.	3/4	Read Ch. 3 and 4 Research Paper 1 due at 11:59pm
23-Sep	4	Fundamentals of IDS Part I: Introduction to Snort:	3/4	Read Ch. 3 and 4
30-Sep	5	Fundamentals of IDS Part II: Proactive intrusion Prevention, attack modeling and simulation	5	Read Ch. 5 **Snort I Assignment is due at 11:59pm**
07-Oct	6	Network flows and anomaly detection IP data flows, NetFlow operational theory.	6	Read Ch. 6
14-Oct	7	**Midterm Exam:** (Covers week 1 – 6).	-	-
21-Oct	8	Snort signatures analysis, Web Application Firewalls, Wireless IDS/IPS	7/8	Read Ch. 7, 8
28-Oct	9	Bro IDS, Physical Intrusion Detection for IT	9	Configure Bro IDS, Read Ch. 9, **Snort II (Signature writing) Assignment is due at 4:30pm**
04-Nov	10	Bro IDS	-	Read Bro IDS on https://www.bro.org/ Configure Bro, ELSA, Security Onion
11-Nov	11	Advanced IDS: Geospatial Intrusion detection	10	Read Ch. 10 **Bro Assignment due at 11:59pm**
18-Nov	12	IDS and visual data Communications	11	Read Ch. 11

25-Nov	13	Thanksgiving Recess (No Class)		
02-Dec	14	Advanced IDS Methods for behavior analysis and proactive forensics visual data communications	-	Research Paper 2 due at 11:59pm
09-Dec	15	Advanced IDS: Latest research analysis	-	**Log Analysis assignment due at 11:59pm**
06-May	16	Final Exam in-class (covers week 9 – 15).	-	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/fall-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.