TCOM 663 Sec 001 – Intrusion Detection and Forensics
Department of Electrical and Computer Engineering
George Mason University
Fall, 2008

Syllabus  2008-06-02

Administrative Information

Instructor:
Dr. Aleksandar Lazarevich

Email:  alazarev@gmu.edu [subject=GMU-TCOM662-Sec/001_Your name]
Phone:  703-393-2247
Office hours:  By appointment

Teaching Assistant
UNK

Day/time of class: Tuesday 4:30 - 7:10

Location:  Innovation Hall, Room 330

Class section: 001

Email:  ???@gmu.edu [subject=IT221-001...]
Phone:  703-993-???
Office hours:  see mason.gmu.edu/~???

Course Description

663 Operations of Intrusion Detection and Forensics (3:3:0) Prerequisites: TCOM 509 and 529 and a working knowledge of computer programming. Introduces students to network and computer intrusion detection and its relation to forensics. It 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.

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.

Textbooks

No required textbook. Reading will be assigned from various Internet sites and published research papers.

Grading

Raw scores may be adjusted to calculate final grades.

Grades will be assessed on the following components:

- Homework: 30%
- Mid-term: 30%
- Final Paper: 40%

These components are outlined in the following sections.

Homework

**Homework 1** - Research 3 open source/free intrusion detection products and 3 commercial intrusion detection products. Write 200 words on each product that summarizes how the product operates, the type of attacks it can detect, how you would use this product in your architecture, and any other pertinent information about the product. Because we will be discussing it in class, do not include Snort as one of your products. This is an individual homework please remember the honor code.

This homework is due before class on Sept. 16.

Please bring 2 copies and be prepared to share your findings with the class in an informal setting.

**Homework 2** –

1. (1 point) Write a Snort rule that will alert on TCP traffic exiting the 10.0.1.0/24 network with the content "proprietary". I do not care where the traffic is going or what ports it is
using. When Snort creates the alert it should read "Proprietary information leaving!"

2. (1 point) Write a Snort rule that will log any TCP traffic entering into the 192.168.100.0/24 and 10.2.2.0/24 networks with destination ports 1 through 1024. I do not care about the source IP addresses or source ports. When Snort logs the traffic it should read "Incoming to low ports".

3. (1 point) Write a Snort rule that will alert on UDP traffic entering the 192.168.10.0/24 network that contains the content "cgi-bin" anywhere between the 5th byte offset to the 25th byte offset. The alert should trigger on both lowercase and uppercase content. I do not care about the source ports or destination ports. When Snort creates the alert it should read "UDP CGI exploit".

4. (1 point) Why would someone use a Snort Pass rule?

5. (1 point) Explain 3 ways to improve Snort's performance.

6. (1 point) In the Steg_IDS Local.rules file, what does the "flags: AP;" rule option do?

For the next 2 questions you will need to read the following paper:

The paper may be downloaded from http://discovery.csc.ncsu.edu/pubs/tissec04.pdf.

7. (2 points) How do the methods presented in the paper help to further the state of the art in intrusion detection?

8. (2 points) How do you think these methods could assist with intrusion forensics?

This homework is due by class time on Nov. 4.

**Homework 3** – Prepare and present a short presentation on your research paper topic. This will be around 5-10 minutes. You may prepare Powerpoint slides with talking points or figures if you wish. However, no more than 3 slides due to time limit. In your presentation please address the following:

1. Summarize the topic of the research.
2. How is this research advancing the science of intrusion detection? What makes this research so great?
3. Any other interesting information about this research.
You will not have time to go into the details of the methodology or testing of the research, so just hit the highlights. Please prepare a 1-2 page write-up of your presentation to hand in before class time.

This homework is due in class on Nov. 18. If you have a prior commitment and will not be in class on Nov. 18, please discuss with me.

Late reports will be assessed a penalty of 25% of the assignment grade for each week or part there of it is late. No homework will be accepted after the third week.

**Mid-term exams**

The mid-term exam will be conducted during class time in Week 7 and will cover material discussed in Weeks 1-6.

The mid-term exam will be take-home. Students must complete with no collaboration.

**Final exam**

Each student should pick a research paper with a focus on intrusion detection 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:

a. A summary of what was done.
b. What are the central contributions of the paper?
c. A summary of related work.
d. What are the principal shortcomings of the technical content of the paper?
e. Other advantages and disadvantages of the technique.
f. 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. Papers must be 5-10 pages in length.
Papers may be accessed through the ACM Digital Library accessible through GMU or other search engines.
The final paper is due Dec. 9 by 4:30pm.

**Schedule**

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Projects Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>8/26/2008</td>
<td>Course overview and TCP/IP review</td>
<td></td>
</tr>
<tr>
<td>Week 2</td>
<td>9/2/2008</td>
<td>Packet Analysis Part 1</td>
<td></td>
</tr>
<tr>
<td>Week 3</td>
<td>9/9/2008</td>
<td>Packet Analysis Part 2</td>
<td></td>
</tr>
<tr>
<td>Week 4</td>
<td>9/16/2008</td>
<td>Fundamentals of IDS Part 1</td>
<td>Homework 1 due</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>Week 5</td>
<td>9/23/2008</td>
<td>Fundamentals of IDS Part 2</td>
<td></td>
</tr>
<tr>
<td>Week 6</td>
<td>9/30/2008</td>
<td>Introduction to Snort</td>
<td>Submit research paper chosen for final exam</td>
</tr>
<tr>
<td>Week 7</td>
<td>10/7/2008</td>
<td>Mid Term exam posted (in class)</td>
<td>Covers weeks 2-6</td>
</tr>
<tr>
<td>Week 8</td>
<td>10/14/2008</td>
<td>Columbus day</td>
<td></td>
</tr>
<tr>
<td>Week 9</td>
<td>10/21/2008</td>
<td>Snort Signatures and Analysis</td>
<td></td>
</tr>
<tr>
<td>Week 10</td>
<td>10/28/2008</td>
<td>Advanced Intrusion Detection and Intrusion Prevention Techniques</td>
<td></td>
</tr>
<tr>
<td>Week 11</td>
<td>11/4/2008</td>
<td>Alert Correlation for Incident and Forensic Analysis</td>
<td>Homework 2 due</td>
</tr>
<tr>
<td>Week 12</td>
<td>11/11/2008</td>
<td>Advanced IDS Methods for Behavior Analysis and Proactive Forensics</td>
<td></td>
</tr>
<tr>
<td>Week 13</td>
<td>11/18/2008</td>
<td>Student presentations</td>
<td>Homework 3 due</td>
</tr>
<tr>
<td>Week 14</td>
<td>11/25/2008</td>
<td>Student presentations</td>
<td></td>
</tr>
<tr>
<td>Week 15</td>
<td>12/2/2007</td>
<td>Final exam (no class).</td>
<td></td>
</tr>
<tr>
<td>Week 16</td>
<td>12/9/2007</td>
<td>Final is due Dec. 9 by normal class time</td>
<td></td>
</tr>
</tbody>
</table>

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).

Important Dates

Last day to add classes: Tues. SEP 9
Last day to drop with no tuition liability: Tues. SEP 9
Last day to drop: Fri SEP 26

From [http://registrar.gmu.edu/calendars/Fall%202007%20Pdf%20Sched.pdf](http://registrar.gmu.edu/calendars/Fall%202007%20Pdf%20Sched.pdf)
See that Web page for more information.

**Resources:**


**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.


"You plagiarize when, intentionally or not, you use someone else's words or ideas but fail to credit that person. You plagiarize even when you do credit the author but use his exact words without so indicating with quotation marks or block indentation. You also plagiarize when you use words so close to those in your source, that if you placed your work next to the source, you would see that you could not have written what you did without the source at your elbow" (p. 167).

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