Administrative Information

Instructor:

Dr. Aleksandar Lazarevich

Email: alazarev@gmu.edu subject=GMU-TCOM590-Sec/003_Your name

Phone: 703-393-2247

Office hours: By appointment

Teaching Assistant

TBD

Day/time of class: Wednesday 4:30-7:10 pm

Location: Innovation Hall 317

Class section: 001

Course Description

590 Sec 001 Incident Response and Corporate Forensics (3:3:0)

Prerequisites: Permission of Instructor. Much of today’s computer is aimed at corporate America. These crimes are perpetrated either directly against the companies or through the victimization of the consumer and using that data to access those same companies. These crimes are usually detected initially as a computer incident. As these incidents are investigated, many become escalated into full blown forensic investigations that are the either turned over to law enforcement or become litigations. 80% of computer forensic work today is done by private companies. This course will address incident detection, response, and those aspects of computer forensics pertinent to the investigation of trade secret theft, economic espionage, copyright infringement, piracy, and fraud.

Textbooks

Computer Security Incident Handling Guide, NIST Publication SP800-61 Revision 1 (Draft), Grace, Kent, Kim, September 2007,


http://cengagesites.com/academic/?site=3136&section=11

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

Homeworks (5@10% each) 50%
Mid-term exam 25%
Final exam 25%

These components are outlined in the following sections.

Homework
Homework 1 - In a 3-4 page paper, describe an incident response plan. Ensure you include who will respond and escalation criteria and procedures.

Homework 2 - Complete Hands-on Project 4-1 from the Nelson text found on page 141 (3rd Edition - page 149). Write a summary report on what steps you took and what observations you made. Include screen captures of significant steps or findings. This report should be 3-10 pages in length.

Homework 3 – Complete Case Project 9-1 from the Nelson text found on page 334 (3rd Edition - page 396). Create a summary report as directed in the text. This report should be 3-10 pages.

Homework 4 - In a 3-4 page paper, address the following: When performing forensics during incident response, an important consideration is how and when the incident should be contained. Modify the plan from homework 2 to account for this need.
Homework 5 - Complete Case Project 10-4 from the Nelson text found on page 402 (3rd Edition - page 440). Create a report as directed in the text. This report should be 3-10 pages in length.

Reports will due in Weeks 4, 6, 10, 12, and 15. Late reports will be assessed a penalty of 25% of the assignment grade for each week or part thereof it is late.

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 and will be posted on blackboard

Final exam
The final exam will be held the week after the final class in the same room used for classes and will cover material from the weeks 9-15.

The final exam will be take home and will be posted on blackboard

Schedule

<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Reading Assignments</th>
<th>Projects Due</th>
</tr>
</thead>
<tbody>
<tr>
<td>Week 1</td>
<td>1/21/2009</td>
<td>Incident Response</td>
<td>SP800-61 Chapt 2-3</td>
<td></td>
</tr>
<tr>
<td>Week 2</td>
<td>1/28/2009</td>
<td>Incident Response (Cont)</td>
<td>SP800-61 Chapt 4-8</td>
<td></td>
</tr>
<tr>
<td>Week 3</td>
<td>2/4/2008</td>
<td>Forensic Investigations</td>
<td>Book Chapt 1 &amp; 2</td>
<td></td>
</tr>
<tr>
<td>Week 4</td>
<td>2/11/2008</td>
<td>Data Collection</td>
<td>Book Chapt 4</td>
<td>Report 1 due</td>
</tr>
<tr>
<td>Week 5</td>
<td>2/18/2008</td>
<td>Processing Scenes</td>
<td>Book Chapt 5</td>
<td></td>
</tr>
<tr>
<td>Week 6</td>
<td>2/25/2008</td>
<td>Windows &amp; Linux</td>
<td>Book Chapt 6 &amp; 8</td>
<td>Report 2 due</td>
</tr>
<tr>
<td>Week 7</td>
<td>3/4/2008</td>
<td>Mid-Term</td>
<td>Covers weeks 1-6</td>
<td></td>
</tr>
<tr>
<td>Week 8</td>
<td>3/11/2008</td>
<td>Spring Break</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Week 9</td>
<td>3/18/2008</td>
<td>Forensic tools and Evaluation</td>
<td>Book Chapt 7 &amp; 9</td>
<td></td>
</tr>
<tr>
<td>Week 10</td>
<td>3/25/2008</td>
<td>Forensic Integration</td>
<td>SP 800-86 Chapt. 2 &amp; 3</td>
<td>Report 3 due</td>
</tr>
<tr>
<td>Week 11</td>
<td>4/1/2008</td>
<td>Forensic Integration (Cont)</td>
<td>SP 800-86 Chapt. 4-8</td>
<td></td>
</tr>
<tr>
<td>Week 13</td>
<td>4/15/2008</td>
<td>Networks and emails</td>
<td>Book Chapt 11 &amp; 12</td>
<td></td>
</tr>
<tr>
<td>Week 14</td>
<td>4/22/2008</td>
<td>Cell phones</td>
<td>Book Chapt 13</td>
<td></td>
</tr>
<tr>
<td>Week 16</td>
<td>5/6/2007</td>
<td>Final exam</td>
<td>Covers weeks 9-15</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

<table>
<thead>
<tr>
<th>Event</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last day to add classes</td>
<td>Tuesday Feb 3</td>
</tr>
<tr>
<td>Last day to drop with no tuition liability</td>
<td>Tuesday Feb 3</td>
</tr>
<tr>
<td>Last day to drop</td>
<td>Friday Feb 20</td>
</tr>
</tbody>
</table>

From [http://registrar.gmu.edu/calendars/200910_sem_cal.pdf](http://registrar.gmu.edu/calendars/200910_sem_cal.pdf)
See that Web page for more information.

**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.

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