Syllabus: AIT 673 - Cyber Incident Handling/Response

Term: Fall 2014

Instructor: Jay Holcomb, Adjunct Faculty, Department of Applied Information Technology, Volgenau School of Engineering

GMU Website: http://mason.gmu.edu/~jholcom9/

E-mail: jholcom9@gmu.edu

Course: AIT 673 -- Cyber Incident Handling/Response

Examines Computer Emergency Response Team (CERT), including Incident Response, Vulnerability Assessment, Incident Analysis, Malcode Analysis, Forensics and Investigations. Includes exercises in CERT operations and a final Incident Handling project.

Credits: 3

Day/Time: Thursday 7:20 pm-10:00 pm

Where: Music/Theater Building, Room: 1002

Textbooks (Required):

Textbooks (Recommended):

Other Resources:
Paper readings and Internet resources posted on Blackboard -- AIT 673 Course

Course Goals:
1. Obtain basic knowledge on dealing with system security related incidents.
2. Increase knowledge on potential defenses and counter measures against common threat vectors/vulnerabilities.
4. Obtain current knowledge of events and tools/support kits in the subject area.
Grading policy:

Grades will be determined based on the following:

<table>
<thead>
<tr>
<th>Grade Component</th>
<th>Weight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Cyber Event Paper #1</td>
<td>10%</td>
</tr>
<tr>
<td>Current Cyber Event Paper #2</td>
<td>10%</td>
</tr>
<tr>
<td>Quiz</td>
<td>10%</td>
</tr>
<tr>
<td>Lab assignments (10% each)</td>
<td>30%</td>
</tr>
<tr>
<td>Team Project and Presentation</td>
<td>30%</td>
</tr>
<tr>
<td>Class Participation</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

The grading scale for this course is:

<table>
<thead>
<tr>
<th>Numeric Grade</th>
<th>Letter Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>97 – 100%</td>
<td>A+</td>
</tr>
<tr>
<td>93 – 96%</td>
<td>A</td>
</tr>
<tr>
<td>90 – 92%</td>
<td>A-</td>
</tr>
<tr>
<td>87 – 89%</td>
<td>B+</td>
</tr>
<tr>
<td>83 – 86%</td>
<td>B</td>
</tr>
<tr>
<td>80 – 82%</td>
<td>B-</td>
</tr>
<tr>
<td>77 – 79%</td>
<td>C+</td>
</tr>
<tr>
<td>73 – 76%</td>
<td>C</td>
</tr>
<tr>
<td>70 – 72%</td>
<td>C-</td>
</tr>
<tr>
<td>60 – 69%</td>
<td>D</td>
</tr>
<tr>
<td>0 – 59%</td>
<td>F</td>
</tr>
</tbody>
</table>
Current Cyber Event Papers (2 – 10%):
Select a recent cyber event - research the event using open source references - then write an executive-level technical brief on the event. Include the following as a minimum: threat vector used, vulnerability, incident response actions taken, your recommended mitigations, business impact of this event. The length of this paper should be one page - maximum of two pages. (One page is a single side of paper) On a separate page include your open source references - minimum of two (2) unique sources are required.

Quiz (10%):
A 25 question open-book multiple-choice quiz covering the key terms/topics discussed during the first seven (7) weeks of the course.

If unable to complete the quiz within allotted time – a written make-up assignment may be completed. (Must be completed within 2 weeks of the quiz for credit.)

Lab Assignments (3 – 10%):
Three (3) labs supporting incident handling/response actions, attack vectors, and network defense options.

If unable to attend/participate in a lab – a written make-up assignment may be completed. (Must be completed within 2 weeks of the missed lab for credit.)

Team Project and Presentation (30%): (Five teams of 5 people each)
Incident response team -- select a fictitious critical infrastructure sector company and create a senior executive (CISO/CIO) level report, with accompanying executive briefing, highlighting why your company needs an internal CIRT/CERT team or why it should outsource the CIRT/CERT capability.

At a minimum cover what will happen when your company is hit with malicious software, or a breach, describing a potential Company incident in great detail. Include how your recommended CIRT/CERT team will approach/engage, processes they will use, tools (software and hardware) that you expect them to have/use, timing and potential business impacts, estimated incident costs (to include potential CIRT/CERT team set-up and team O&M), team skills needed with estimated costs, and the [critical] reporting processes.

The length of the report should be less than 20 pages. (One page is a single side of paper) On a separate attachment include your open source references.

The report and presentation will be given during our final two sessions.

Class Participation (10%):
Active participation in weekly lectures, labs, and team assignments.
Lecture Schedule (Tentative):

**Week 1:** Introduction to Incident Response and Handling -- CIRT/CERT Overview

**Reading:**
- **Review** NIST Special Publication 800-100 (October 2006)

### Preparation/Discovery Section

**Week 2:** Incident Response Team and Case Study #1

**Reading:**
- **Review** NIST Special Publication 800-61 Revision 2 (August 2012)
  - Chapter 2 and 3
  - Chapter 2, Chapter 3, and Case Study #1

**Week 3:** Networking Security Monitoring – Lab Preparation

**Reading:**
  - Chapter 5 and Chapter 9
  - Chapter 3 in NSM book.

**Week 4:** **Lab #1**

### Data Collection/Analysis Section/Remediation

**Week 5:** Enterprise Services and Case Study #2

**Reading:**
  - Chapter 10 and Case Study #2

*(Current Cyber Event Paper # 1 due)*
**Data Collection/Analysis Section/Remediation**

**Week 6:** Hashing, Live Data Collection, and Forensic Duplication

**Reading:**
  Chapter 7 and Chapter 8

**Week 7:** *(VIRTUAL WEEK – testing online class process)* Report Writing and Remediation

**Reading:**
  Chapter 16, Chapter 17, and Chapter 18
- Assignment (due Sunday, October 12th at midnight) – Teams complete five (5) questions on page 572. (Maximum 5 pages)

**Week 8:** **Lab #2**
*(Quiz opens)*

**Analysis cont’d/ Post Incident Section**

**Week 9:** Investigating Applications (like Web Browsers/E-mail)

**Reading:**
  Chapter 14
  *(Quiz closes)*

**Week 10:** Investigating Windows Systems

**Reading:**
  Chapter 12
  *(Current Cyber Event Paper # 2 due)*

**Week 11:** Malware Triage

**Reading:**
  Chapter 15
Honor Code:
All work performed in this course will be subject to the GMU’s Honor Code. Any violation will be reported to the honor committee.

Academic Integrity:
GMU is an Honor Code university; please see the Office for Academic Integrity for a full description of the code and the honor committee process. The principle of academic integrity is taken very seriously and violations are treated gravely. What does academic integrity mean in this course? Essentially this: when you are responsible for a task, you will perform that task. When you rely on someone else’s work in an aspect of the performance of that task, you will give full credit in the proper, accepted form. Another aspect of academic integrity is the free play of ideas. Vigorous discussion and debate are encouraged in this course, with the firm expectation that all aspects of the class will be conducted with civility and respect for differing ideas, perspectives, and traditions. When in doubt (of any kind) please ask for guidance and clarification.

Office of Disability Services:
If you are a student with a disability and you need academic accommodations, please see me and contact the Office for Disability Services (ODS) at 993-2474, http://ods.gmu.edu. All academic accommodations must be arranged through the ODS.

Mason e-mail Accounts:
Students must use their MasonLIVE email account to receive important University information, including messages related to this class. See http://masonlive.gmu.edu for more information.

Other Useful Campus Resources:
Writing Center: A114 Robinson Hall; (703) 993-1200; http://writingcenter.gmu.edu
University Libraries “Ask a Librarian”: http://library.gmu.edu/mudge/IM/IMRef.html
Counseling And Psychological Services (CAPS): (703) 993-2380; http://caps.gmu.edu

University Policies: The University Catalog, http://catalog.gmu.edu, is the central resource for university policies affecting student, faculty, and staff conduct in university academic affairs. Other policies are available at http://universitypolicy.gmu.edu. All members of the university community are responsible for knowing and following established policies.