Syllabus: AIT 673 - Cyber Incident Handling/Response

Term: Fall 2018

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

GMU Website: https://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, 7:20pm – 10:00pm

Where: East Room: 121

Textbooks (Required):


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.

Course Expectations:

1. Graduate education requires dedication and organization. Proper preparation is expected every week. You are expected to log into our Blackboard course each week and complete any assignments and activities on or before due dates.
2. Students must check their GMU email messages on a daily basis for course announcements, which may include reminders, revisions, and updates.
3. It is expected that you will familiarize yourself with and adhere to the Honor Code. (https://oai.gmu.edu/the-mason-honor-code-2/) Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.
4. It is essential to communicate any questions or problems to me promptly.

Learning Community:

This course is supported via Blackboard Courses (Log into https://mymason.gmu.edu/ select the Courses Tab, and the course can be found in the Course List).

Each week begins on Monday and ends on Sunday.

In our online learning community, we must be respectful of one another. Please be aware that innocent remarks can be easily misconstrued. Sarcasm and humor can be easily taken out of context. When communicating, please be positive and diplomatic!
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>In-class Labs or Alternate Assignments (5 @ 5%)</td>
<td>25%</td>
</tr>
<tr>
<td>Team Paper -- Case Study #2</td>
<td>15%</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>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>97 – above</td>
<td>A+</td>
<td>Passing</td>
</tr>
<tr>
<td>93 – 96%</td>
<td>A</td>
<td>Passing</td>
</tr>
<tr>
<td>90 – 92%</td>
<td>A-</td>
<td>Passing</td>
</tr>
<tr>
<td>87 – 89%</td>
<td>B+</td>
<td>Passing</td>
</tr>
<tr>
<td>83 – 86%</td>
<td>B</td>
<td>Passing</td>
</tr>
<tr>
<td>77 – 82%</td>
<td>B-</td>
<td>Passing</td>
</tr>
<tr>
<td>70 – 76%</td>
<td>C</td>
<td>Passing</td>
</tr>
<tr>
<td>0 – 69%</td>
<td>F</td>
<td>Failing</td>
</tr>
</tbody>
</table>
Current Cyber Event Papers (2 @ 10% each = 20%):
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 attacked, 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.

In-class Labs/Alternate Assignments (5 @ 5% = 25%):
Five (5) labs supporting incident handling/response actions, attack vectors, and network defense options.

If unable to complete an in-class lab – a written Internet researched paper assignment may be completed. (Must be completed within 2 weeks of the lab for credit.)

Team Paper -- Case Study #2 (15%):
Using Case Study #2 (Chapter 1, page 15) build a high-level remediation plan outline and answer four (4) incident response remediation questions.

Team Project and Presentation (30%):
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 45 pages. (One page is a single side of paper / double-spaced) On a separate attachment include your open source references. (APA formatting applies)

The report and presentation will be given during our final session.

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

Preparation/Discovery Section

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

Objective: Develop an understanding of the purpose of a Computer Emergency Response Team (CERT), why an organization needs a CERT, composition of a CERT team, and the incident response life cycle.

Course Goal Connection:
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.

Required Reading:
- Read: NIST Special Publication 800-100 (March 2007), Chapter 13

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 2: Incident Response Team and Case Study #1

Objective: Analyze the pre-incident preparation required by an incident response team and the organization. Identify key areas of the organization, incident response team, and corporate infrastructure needed to develop for a successful incident response capability.

Course Goal Connection:
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.

Required Reading:
- Read: Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 3, and Case Study #1
- Read: Mandiant, Incident Response Retainers, see Week 2 Weekly Module in Blackboard
- Review: NIST Special Publication 800-61 Revision 2 (August 2012), Chapter 2

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 2 Assignment:
Hands-on Activity #1 (Not graded) – in-class activity supporting incident handling/response actions, cyber tools, and processes we have been discussing
Week 3: Networking Security Monitoring and Indicators/Leads

Objective: Identify the types of networking monitoring an organization may implement and explain the benefits for implementing network monitoring within an organization. Define the value of a lead/indicator to an incident response team and follow-on value to the larger organization.

Course Goal Connection:
1. Increase knowledge on potential defenses and counter measures against common threat vectors/vulnerabilities.
2. Gain experience using tools and common processes in performing analysis of compromised systems and dynamic malware analysis.
3. Obtain current knowledge of events and tools/support kits in the subject area.

Required Reading:
- **Read:** Incident Response & Computer Forensics, 3rd Edition (2014), Chapter 5 and 9
- **Read:** Mandiant, APT1 Exposing One of China's Cyber Espionage Units -- see Week 3 Weekly Module in Blackboard
- **Read:** Ponemon/IBM, 2018 Cost of Data Breach Study -- see Week 3 Weekly Module
- **Read:** Ponemon/IBM, 2017 Cost of Data Breach Study -- see Week 3 Weekly Module
- **Read:** Ponemon/IBM, 2016 Cost of Data Breach Study -- see Week 3 Weekly Module

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 3 Assignment:
**Current Cyber Event Paper #1**

Week 4: Initial Incident Detection/Facts

Objective: Explain why initial facts in a potential incident are critical and how checklists can help provide objectivity to a potential incident detection. Identify three checklists that could assist the incident response team with objectivity regarding a potential incident detection.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.
4. Obtain current knowledge of events and tools/support kits in the subject area.

Required Reading:
- **Read:** Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 4
- **Read:** FireEye -- APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?
- **Read:** FireEye -- APT28 Targets Hospitality Sector, Presents Threat to Travelers « Threat Research Blog
- **Read:** NIST Special Publication 800-61 Rev 2 (August 2012), Chapter 3: pg 21 - 34

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 4 Assignment:
**Lab #1 - hands-on lab supporting incident handling/response actions, attack vectors, and network defense options and processes we have been discussing**
Data Collection/Analysis Section/Remediation

Week 5: Enterprise Services and Case Study #2

Objective: Identify at least five (5) enterprise network services that most organizations implement. Explain the functions and benefits of these network services to an organization and their importance to an incident response team.

Course Goal Connection:
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.

Required Reading:
- **Read**: Cisco – 2018 Annual Cybersecurity Report
- **Read**: Cisco – 2017 Annual Cybersecurity Report
- **Read**: Cisco – 2016 Midyear Cybersecurity Report
- **Review**: The Internet Assigned Numbers Authority (IANA) web site ([https://www.iana.org](https://www.iana.org)) and associated resources available on this web site.

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 5 Assignment:
**Hands-on Activity #2 (Not graded) -- in-class activity supporting incident handling/response actions, cyber tools, and processes we have been discussing**

Week 6: Forensic Duplication and Hashing

Objective: Identify the three primary types of forensic images an incident response team may create and differences between the three. Explain the process used to create a forensic duplication. Describe what hashing is, why it is important, and what benefits it provides to the incident response team.

Course Goal Connection:
4. Obtain current knowledge of events and tools/support kits in the subject area.

Required Reading:
- **Read** Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 8 and Chapter 15 (pages 474 and 475)

Other Reading (Recommended):
- Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 6 Assignment:
**Lab #2 - hands-on lab supporting incident handling/response actions, attack vectors, and network defense options and processes we have been discussing**
Week 7: Report Writing and Remediation

Objective: Explain why reporting writing is one of the most important functions of an incident response team. Identify and analyze the eight (8) high-level steps which make-up the incident response remediation process.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 16 and Chapter 17

Other Reading (Recommended):
• Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 7 Assignment:
Team Paper -- Case Study #2

Week 8: Live Data Collection

Objective: Explain the primary purpose for live data collection. Identify at least five (5) best practices for establishing a good process regarding live data collection. Compare and contrast memory collection on Microsoft Windows and Unix/Linux based systems.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.
4. Obtain current knowledge of events and tools/support kits in the subject area.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 7

Other Reading (Recommended):
• Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 8 Assignment:
Lab #3 -- hands-on lab supporting incident handling/response actions, attack vectors, and network defense options and processes we have been discussing
Analysis cont’d / Post Incident Section

Week 9: Analysis Methodology

Objective: Recommend a repeatable process to follow when preparing to gather and analyze incident response related data.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 11

Other Reading (Recommended):
• Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 9 Assignment:
Current Cyber Event Paper #2

Week 10: Investigating Applications (like Web Browsers/E-mail)

Objective: Explain the value of potential forensic evidence stored within user and server applications. Describe what application data is and where it is stored. Analyze web browser user data and the potential value of this data.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 14

Other Reading (Recommended):
• Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 10 Assignment:
Hands-on Activity #3 (Not graded) – in-class activity supporting incident handling/response actions, cyber tools, and processes we have been discussing

Week 11: Investigating Windows Systems

Objective: Identify potential sources of incident response data on a Microsoft Windows operating system. Explain purpose and potential evidence that may be found in the following areas; NTFS/File System, Prefetch, Event logs, Scheduled tasks, and the Windows registry.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 12

Other Reading (Recommended):
• Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 11 Assignment:
Lab #4 -- hands-on lab supporting incident handling/response actions, attack vectors, and network defense options and processes we have been discussing
Week 12: Investigating Mac OS X Systems

Objective: Identify the potential sources of incident response data on an Apple MC OS X operating system. Explain the purpose and potential evidence that may be found in the following areas; HFS+ file system, core operating system, Spotlight data, System and application logs, and Application and system configurations.

Course Goal Connection:
1. Obtain basic knowledge on dealing with system security related incidents.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 13

Other Reading (Recommended):
Paper readings and Internet resources posted on Blackboard -- AIT 673

Week 12 Assignment:
Team Breakout – Status and continue work in support of Final Team Reports and Presentations

Week 13: Malware Triage

Objective: Identify at least three (3) steps to decrease the infection opportunity while analyzing malware in a virtual environment and at least five (5) configuration/process changes that can decrease the infection opportunity. Explain Static malware analysis and why it can be useful to an incident response team. Explain Dynamic malware analysis and why it can be useful to an incident response team.

Course Goal Connection:
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.

Required Reading:
• Read Incident Response & Computer Forensics, 3rd Edition (August 8, 2014), Chapter 15

Other Reading (Recommended):
• Paper readings and Internet resources posted on Blackboard -- AIT 673 - Online Course

Week 13 Assignment:
Lab #5 -- hands-on lab supporting incident handling/response actions, attack vectors, and network defense options and processes we have been discussing

Team Project Delivery/Presentation

Week 14: Team Reports and Presentations
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, https://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 https://masonlive.gmu.edu/ for more information.

Other Useful Campus Resources:

Writing Center: A114 Robinson Hall; (703) 993-1200; https://writingcenter.gmu.edu/

University Libraries “Ask a Librarian”: https://library.gmu.edu/mudge/IM/IMRef.html

Counseling And Psychological Services (CAPS): (703) 993-2380; https://caps.gmu.edu/

University Policies: The University Catalog, https://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 https://universitypolicy.gmu.edu/. All members of the university community are responsible for knowing and following established policies.