I. **Course Information:**
AIT 702 — Incident Handling and Penetration Testing, 3 credit hours
Location: ONLINE
Course prerequisite: AIT 660: Cyber Security Fundamentals
AIT Cyber Security Concentration

II. **Instructor:**
Dan VanBelleghem
dvanbell@gmu.edu
o. 703-852-1712
Virtual Office Hours: By appointment via Blackboard Collaborate

III. **Course Description:**
Presents students with a principled approach to penetration testing to include an in-depth analysis of the overall process, aspects related to scanning, testing, ethically attacking, and eventually securing systems and networks. The course covers popular attack tools such as Social Engineering and DDoS, and concludes with a discussion about open challenges and current research in the area. Incident handling concepts will be discussed that include incident response lifecycle, cyber threat intelligence integration, and a comprehensive approach to response automation.

IV. **Goals and Objectives**
Students will be able to:
- Evaluate the strategies for testing controls that address common security risks.
- Understand the framework for effective penetration testing planning and development.
- Address the primary challenges to implementing a successful penetration testing program.
- Be familiar with various tools and techniques required for effective penetration testing.
- Understand effective incident response automation approaches and methodologies.
- Identify integration points between penetration testing and incident handling processes.
- Recognize open challenges and current research in the area.
V. Course Delivery:
The course will be delivered via Blackboard and will include lectures, weekly assignments, and a final exam. This course will be taught via a series of modules, each of which will introduce an important topic, fundamental or building block required for a comprehensive understanding of information systems protection concepts. Articles, videos, white papers, journals, and online discussions will supplement weekly lectures. Students will be required to write a technical paper on a topic to be approved by the instructor. Interaction with classmates is encouraged; however, 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.

VI. Communications
Registered students will be given access to a section of the Blackboard Learning System for this course. Blackboard will be used as the primary mechanism to disseminate course information, including announcements, lecture slides, homework and other assignments, and scores for homework and exams.

Communication with the Instructor on issues relating to the individual student should be conducted using Mason email, via telephone, or in person - not in the public forums on Blackboard. Mason Mail is the preferred method – for urgent messages, you should also attempt to contact the Instructor via telephone. Federal privacy law and Mason policy require that any communication with a student related in any way to a student's status be conducted using secure Mason systems – if you use email to communicate with the Instructor you MUST send messages from your Mason email account.

When sending an e-mail to the instructor, please include the following:
- Course number
- Section number
- Your full name

VII. Preparation and Student Expectations:

Reading Assignments: Students are expected to read any “assigned” readings before the class in which the topics will be discussed. Students are also encouraged to read as much of the suggested readings as possible to enhance their insight into the course subject matter. The instructor will provide additional materials such as related white papers, reprinted articles, and URLs to related material located on public Internet servers. As a preliminary preparation for this course, it is necessary that the students effectively review all materials and complete the individual assignments by the due dates.

Course Policy:
- All work done outside of class and in conjunction with the course must be typed. The instructor reserves the right to impose other formatting instructions as the need arises (e.g.,
footnotes should be included at the end of assignments instead of at the bottom of each page, etc.).

- Work is due when scheduled. **No exceptions.** Failure to meet deadlines will result in reduced grades. **Late assignments will be reflected by the following reduction in your grade:**
  - Up to 1 week 10% reduction
  - More than 1 week 20% reduction

- Students should be prepared to devote several hours per week to conduct research in support of weekly assignments.
- Each student is expected to participate in online discussions and case study activity.

**VIII. Plagiarism and Academic Integrity Policy**

It is expected that students adhere to the George Mason University Honor Code as it relates to integrity regarding coursework and grades. The Honor Code reads as follows, “To promote a stronger sense of mutual responsibility, respect, trust, and fairness among all members of the George Mason University community and with the desire for greater academic and personal achievement, we, the student members of the University Community have set forth this: Student members of the George Mason University community pledge not to cheat, plagiarize, steal and/or lie in matters related to academic work.” More information about the Honor Code, including definitions of cheating, lying, and plagiarism, can be found at the Office of Academic Integrity website at [https://oai.gmu.edu/](https://oai.gmu.edu/)

All papers and projects will be turned in electronically and will be scanned for evidence of plagiarism. Specifically the plagiarism policy with respect to this class is:

**Do not use any material verbatim in detail without citing it, and never quote more than a paragraph or two, without checking with the instructor first. Do not capture material from (other’s) Web pages and represent it as your own. This is plagiarism and anyone suspected of this will be referred to the GMU Office of Academic Integrity.**

If you are unsure of what this means, ask the instructor.

**IX. Evaluation and Grading Criteria:**

Student grades will be determined by class participation, course assignments, examinations, case study work, and other projects. Students are expected to complete all assigned reading and problems and take all examinations by the assigned dates. To get the most out of the class, students should read the chapters and complete assignments on time and stay current with the material. Also, students should log on the class Blackboard page frequently to keep current with questions/answers and other postings.
PARTICIPATION
Weekly discussion topics will be posted. Students are **required** to participate in online discussions by posting comments, observations, or relevant articles to support the units of instruction. Interaction with classmates is encouraged; however, 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.

EXAMS
The course examinations cover the fundamental concepts and their application. The examinations are used to ensure the concepts and principles of the course are mastered so that the student realizes a satisfactory grade. The examinations will also assure the development of a workable knowledge base in computer security and proficiency in applying the concepts to address real world requirements and situations.

WEEKLY ASSIGNMENTS
The instructor assigns weekly assignments that will draw upon student’s knowledge and proficiency with security concepts and principles in order to challenge their ability to implement practical computer security solutions and collaborate as a team as necessary in the real world. Completing the weekly assignments allows the student to more fully participate each week in class.

TECHNICAL PAPER
Each student must complete a technical paper on a security topic of interest to the student. Students will be responsible for defining their projects. The instructor will participate in the project by conducting review sessions and interim checkpoints. These activities will be conducted in an agreed upon time to assist students to focus on the subject matter and formulate the term paper outline.

The content contained in the project report must be relative to the subject and goals of the class. How well the student is able demonstrate knowledge learned from the project will be a major factor in his/her grades.

Project evaluation areas include the following:

1. Communication:
   a. Project is coherent, with clear description of project objectives.
   b. Thoughtful responses offered to questions raised in discussion.

2. Scope and Relevancy
   a. Explored systems, solutions, tools, or components relative to the topic.
   b. Appropriate security principles were defined and presented.

3. Analysis:
   a. Clearly articulates what worked well and why, what did not work well and why, and lessons learned.
   b. Valid conclusions based on stated criteria, relevant constraints (technical, business, legal, environment, etc.).
c. Alternatives are considered and presented.

4. Content:
   a. Explanations are complete.
   b. Information is relevant and accurate.
   c. Resources are legitimate and referenced.
   d. Demonstrates intimate knowledge of the subject.

Suggested project paper outline:
• Title
• Introduction (purpose, methodology, structure)
• Approach
• Background and discussion relevant to the topic
• Body of discussion
• Conclusions and Summary
• References and bibliography

Grading will be based on the quality of the report. In addition to the content contained in the paper, the topic must be relative to the subject and goals of the class. How well the student is able to demonstrate knowledge learned from the project will be a major factor in his/her grades.

X. Grading
Grades will be awarded in accordance with the Mason Grading System for graduate students. See the university catalog for policies: http://catalog.gmu.edu for more information.

The grading scale for this course is:

<table>
<thead>
<tr>
<th>Percentage</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>77 – 82%</td>
<td>B-</td>
</tr>
<tr>
<td>70 – 76%</td>
<td>C</td>
</tr>
<tr>
<td>0 – 69%</td>
<td>F</td>
</tr>
</tbody>
</table>

Raw scores may be adjusted by the Instructor to calculate final grades.

Students are responsible for checking the currency of their grade books. Grade discrepancies must be brought to instructor’s attention within one week of assignment submission and 48 hours of exam submission.
**Assignment Area Percentages:**
The following tables feature the percentage breakdown of each assignment area towards the final grade and the grading scale.

<table>
<thead>
<tr>
<th>Assignment Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly Assignments</td>
<td>40%</td>
</tr>
<tr>
<td>Final examination</td>
<td>25%</td>
</tr>
<tr>
<td>Term Project (Technical Paper)</td>
<td>25%</td>
</tr>
<tr>
<td>Class Participation/Discussion Boards</td>
<td>10%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**XI. Recommended Textbook/Reference Materials:**

All project materials are included in the course – with few exceptions, there are no textbooks required in order to complete projects. Through open source materials and personal research you should have access the information necessary to prepare for classes, exams, and project. You may also access the GMU Library to explore topics in more depth and perform additional research.

Chuck Easttom, ISBN: 9780134854564 | Published by Pearson IT Certification, 2018

**Intelligence Driven Incident Response**

Intelligence Driven Incident Response is available electronically through the **Safari Tech Books Online collection.** You can access this book by following these steps:

- Go to [https://learning-oreilly-com.mutex.gmu.edu/](https://learning-oreilly-com.mutex.gmu.edu/)
- If you are off-campus, you will be asked to login using your Mason email user name and password.
- Type the ISBN number of the book into the search box and click search, then click on the book title in the search results page. The next page that will open is the homepage for the book.
- Click on the Start Reading button to open the book.

**XII. Course Schedule**

Start: January 25, 2021
End: May 7, 2021
<table>
<thead>
<tr>
<th>Unit</th>
<th>Week</th>
<th>Topic</th>
<th>Weekly Topics and Assignments</th>
</tr>
</thead>
</table>
| 1    | Jan 25 | Introduction, Logistics, Class overview, Objectives Why Penetration Testing? | • Introduce Yourself  
• Review the Syllabus |
| 2    | Feb 1  | Penetration Testing Lifecycle | Assignment 1 Due  
Term Project Proposal Due |
| 3    | Feb 8  | Penetration Testing Execution - 1 Reconnaissance |  |
| 4    | Feb 15 | Penetration Testing Execution - 2 Scanning and Enumeration | Assignment 2 Due |
| 5    | Feb 22 | Social Engineering |  |
| 6    | Mar 1  | Physical Security, Training, Wireless |  |
| 7    | Mar 8  | Password Security | Assignment 3 Due |
| 8    | Mar 15 | Zero Days |  |
| 9    | Mar 22 | Incident Response Lifecycle | Assignment 4 Due |
| 10   | Mar 29 | Playbooks, Cyber Defense Matrix |  |
| 11   | Apr 5  | Kill Chain, MITRE ATT&CK, Threat Intelligence | Assignment 5 Due |
| 12   | Apr 12 | Incident Response Testing and Deception Techniques |  |
| 13   | Apr 19 | Cybersecurity Maturity Models, Open challenges, Current research |  |
| 14   | Apr 26 | Course Review | Term Reports Due  
Presentations (Optional) |
| 15   | May 3  | **FINAL EXAM** |  |