The George Mason University
Department of Information Sciences & Technology
Volgenau School of Engineering

Incident Handling and Penetration Testing

I. **Course Information:**
AIT 702 — Incident Handling and Penetration Testing, 3 credit hours
Dates: Summer 2019
Location: Online
Course prerequisite: AIT 660: Cyber Security Fundamentals
AIT Cyber Security Concentration

II. **Instructor:**
Dan VanBelleghem
dvanbell@gmu.edu
Phone: 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. Preparation and Student Expectations:
Reading Assignments: Students are expected to read any “assigned” readings in order to fully participate in discussion topics. 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.

VII. 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 http://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 found doing this will be severely punished in line with the University Policy on Academic Integrity.**

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

**VIII. 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 to 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.

The following table features the percentage breakdown of each assignment area towards the final grade and the grading scale.
Assignment Area Percentages:

<table>
<thead>
<tr>
<th>Assignment Area</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weekly Assignments</td>
<td>50%</td>
</tr>
<tr>
<td>Final Examination</td>
<td>20%</td>
</tr>
<tr>
<td>Technical Paper</td>
<td>20%</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>

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

Through open source materials and personal research you should have access to 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. All project materials are included in the course – with few exceptions, there are no textbooks *required* in order to complete projects. However, I recommend the following books for this class:

**Penetration Testing Essentials**

**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:

- 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.
X. **Course Schedule**

Start: June 3, 2019  
End: July 27, 2019  
Total Number of Weekly Sessions: 8

<table>
<thead>
<tr>
<th>Unit</th>
<th>Week</th>
<th>Topic</th>
<th>Weekly Discussion Topics and Assignments</th>
</tr>
</thead>
</table>
| 1    | June 3 | Introduction  
  • Class overview  
  • Objectives  
  • Syllabus Review  
Why Penetration Testing?  
  • Challenges  
  • Opportunities  
Complexity and Trends  
  • Mobility  
  • Consumerization  
  • Cloud  
Threat Landscape  
  • Internet  
  • Insiders  
  • Proximity  
  • Supply Chain  
Overview of Enterprise Drivers  
  • Legislation  
  • Business practices  
IT Security Principles and Control Frameworks  
  • Management  
  • Operational  
  • Technical  
Designing Enterprise Policy  
  • Regulations/laws  
  • Mission/Business focus  
Continuous IT Security Assessments  
  • Risk Assessments (e.g., NIST RMF)  
  • Audits  
  • Vulnerability Testing | • Introduce Yourself  
• Review the Syllabus  
• Prepare for course projects  
• Review topics that you feel are helpful to your project and upcoming classes  
• Consult with your professor as required |
| 2    | June 10| Policy for Penetration Testing  
Testing Methodology  
Planning the test  
  • Test Plans  
  • Scenarios  
  • Rules of Engagement | Technical Paper Proposals Due.  
Assignment 1 Due  
Describe the main purpose of the penetration test plan:  
  • What should be included?  
  • Amount of detail?  
  • Approval process? |
<table>
<thead>
<tr>
<th>Date</th>
<th>Topic</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 3 June 17 | Gathering Intelligence and Reconnaissance  
- Footprinting  
- Open source  
- Infrastructure  
- Job Boards  
- Financials  
- Social Media  
- Maintaining anonymity  
Scanning and Enumeration  
- Passive  
- Active  
- Proxy  
- Enumeration  
Tool History  
Vulnerability scanning  
- Benefits  
- Platforms |  
Covert or overt – which techniques is best when conducting reconnaissance?  
List possible risks and mitigations for conducting scanning.  
Pros and cons for implementing an active scanning component to a security program. |
| 3 | Exploitation, Pivoting, and Reporting  
- Methods  
- Tools  
- Metasploit  
- Reporting constraints  
- Access Controls  
- Quality controls  
Social Engineering and Physical Security  
- Weakest link  
- Proximity  
- User awareness  
- Human vulnerabilities  
- Social Networking  
Wireless Testing  
- Wireless challenges  
- Wireless encryption  
- Bluetooth  
- Internet of Things  
- Tools | **Assignment 2 Due**  
Discuss the possible liability to an organization from penetration test results.  
Describe the risks involved with executing exploits within a production environment.  
Challenges and liabilities to consider when wireless networks are included with the test. |
| 4 June 24 | Monitoring, Detections, and Incident Response  
- Preparation  
- Detection  
- Containment  
- Remediation  
- Recovery  
- Lessons Learned  
Password Cracking  
- Online/Offline  
- Brute force | **Assignment 3 Due**  
Review Cyber Defense Matrix  
Does deception add value or is it only security through obscurity?  
Identify possible password alternatives for consumers, enterprise, and cloud providers. |
<table>
<thead>
<tr>
<th></th>
<th>July 1</th>
<th>Assignment 4 Due</th>
</tr>
</thead>
</table>
|   | Incident Response Playbooks  
    • Cybersecurity Framework  
    • Cyber Defense Matrix  
    • Cyber Resilience  
    • Threat Intelligence | Describe vulnerabilities associated with an organization’s supply chain. How are these exploited? |
| 6 | July 8 | Assignment 5 Due |
|   | Intelligence Driven Security Incident Response Testing  
    Deception Techniques  
    • Cost Vs Benefits  
    • Platforms  
    • Management Exploits  
    • Risks and mitigations  
    • Custom | Discuss how best to provide cost vs benefits for penetration testing. |
| 7 | July 15 |  |
|   | Cybersecurity Maturity Models Trends  
    • Cloud  
    • Mobile  
    • BYOD  
    • IoT  
    • Remote workforce  
    • Outsourcing Pen Test: Putting it all together | Effective ways to present results to various audiences to include technical, auditors, executives, and legal.  
What types of training programs would you require for an internal penetration testing team? Include justification for each one. |
| 8 | July 22 | Technical Papers Due Final Exam |
|   | Training and Exercises  
    Test Ranges  
    Open challenges  
    Current research  
    Course review  
    Final Exam | Discussion on current penetration testing challenges: personnel, compliance, legal, and liabilities.  
Identify research projects in the field – describe applicability. |