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: Tuesdays 7:20-10:00 PM
   Jan 22, 29; Feb 5, 12, 19, 26; Mar 5, 19, 26; Apr 2, 9, 16, 23, 30; May 14
Location: Innovation Hall 129
Course prerequisite: AIT 660: Cyber Security Fundamentals
AIT Cyber Security Concentration

II. Instructor:
Dan VanBelleghem
dan.vanbelleghe@gdit.com
dvanbell@gmu.edu
c. 703-447-2999 / o. 703-852-1712
Virtual Office Hours: By appointment via Blackboard Collaborate

III. Course Description:
Presents students with a principled approach to ethical hacking, and offers an in-depth analysis of the overall process, including 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.

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.
- Recognize open challenges and current research in the area.

V. Course Delivery:
The course will be delivered by instruction, lecture notes, case studies and group collaboration on course projects. Presentations supplemented by the articles, videos, white papers journals, and instructor led discussions will be provided. Interaction with classmates is encouraged. 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. Each of the modules will be supported by assigned readings and course work. Visiting experts from the field of cybersecurity will enrich classroom discussions.

VI. **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:

- **Class attendance is mandatory.** If unforeseeable circumstances cause students to miss three or more classes, that student is expected to discuss the situation in advance with the instructor to make up assignments.
- 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.
- Before each class, each student should study appropriate materials, independent research, and designated reading materials assigned by the instructor. Each student is expected to participate in classroom 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](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.

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 DISCUSSION 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.

TERM PROJECT
Each student must complete a research project 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 check points. 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 projects may be performed solo or in groups, with a maximum group size of two students. The instructor will make the final determination in the makeup of the groups and approval for the project.
The following deliverables will determine the grade for the project:

- **Proposal** - One-page proposal that identifies the group members and suggested research topic that includes an *outline* of the implementation or experimental work proposed.
- **Project Report** – Set of briefing slides used to document the project results.
- **Project Presentation** – Presentation in class that summarizes and highlights the results of the project.

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. Slides effectively contribute to the presentation.
   - c. Information is relevant and accurate.
   - d. Resources are legitimate and referenced.
   - e. Demonstrates intimate knowledge of the subject.

**Suggested project paper outline (7-10 Slides):**

- Title Page
- Introduction (purpose, methodology, structure)
- Approach
- Background and discussion relevant to the topic
- Body of discussion
- Conclusions and Summary
- References and bibliography
Project grading will be based on the quality of the presentations and demonstration. In addition the content contained in the paper and presentation must be relative to the subject and goals of the project. How well the student is able to demonstrate knowledge learned from the project will be a major factor in his/her grades.

The following tables feature 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>Class participation</td>
<td>10%</td>
</tr>
<tr>
<td>Midterm examination</td>
<td>25%</td>
</tr>
<tr>
<td>Final examination</td>
<td>25%</td>
</tr>
<tr>
<td>Term project</td>
<td>40%</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>100%</strong></td>
</tr>
</tbody>
</table>

**IX. 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.

**The Hacker Playbook 3: Practical Guide To Penetration Testing**

**Penetration Testing Essentials**

**X. Course Schedule**
Week Start: Tuesday Morning – January 22, 2019  
Week Ending: Monday Midnight – May 6, 2019  
Total Number of Weekly Lecture Sessions: 13  
Important Dates:  
- Mid Term Exam: Tuesday, March 5, 2019 (No Lecture posting for the Week of March 4th)  
- Spring Break: March 11-17, 2019 (No Lecture posting during this week)  
- Final Exam: Tuesday, May 14, 2019 (7:30 – 10:00 PM)  

<table>
<thead>
<tr>
<th>Unit</th>
<th>Date</th>
<th>Topic</th>
<th>Weekly Discussion</th>
</tr>
</thead>
</table>
| 1    | 1/22  | Introduction  
Why Penetration Testing?  
Complexity and Trends  
Threat Landscape  | • 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    | 1/29  | Overview of Enterprise Drivers  
IT Security Principles and Control Frameworks  
Designing Enterprise Policy  
Continuous IT Security Assessments  
Penetration Testing (Red Team/Blue Team)  | Major breaches (e.g., OPM, etc.):  
- Review what happened  
- Organization Impact  
- Response  
- Lessons learned  
- Possible prevention and future mitigations |
| 3    | 2/5   | Planning the test  | Project Proposals Due.  
Describe the main purpose of the |
<table>
<thead>
<tr>
<th>Week</th>
<th>Date</th>
<th>Topic</th>
<th>Details</th>
</tr>
</thead>
</table>
| 4    | 2/12 | Scanning and Enumeration | • Passive  
• Active  
• Proxy  
• Enumeration  
Vulnerability scanning  
• Benefits  
• Platforms  
penetration test plan:  
• What should be included?  
• Amount of detail?  
• Approval process?  
Covert or overt – which techniques is best when conducting reconnaissance? |
| 5    | 2/19 | Exploitation, Pivoting, and Reporting | • Methods  
• Tools  
• Metasploit  
• Reporting constraints  
• Access Controls  
• Quality controls  
Risks and mitigations for conducting scanning.  
Pros and cons for implementing an active scanning component to a security program. |
| 6    | 2/26 | Social Engineering and Physical Security | • Weakest link  
• Proximity  
• User awareness  
• Human vulnerabilities  
• Social Networking  
Class Exercise/Assignment:  
• Developing test plans  
• Rules of engagement  
• Test reports |
| 3/5  | MIDTERM EXAM | |
| 3/12 | 2/12 | Spring Break – No Class | |
| 7    | 3/19 | Monitoring, Detections, and Incident Response | • Preparation  
• Detection  
• Containment  
• Remediation  
• Recovery  
• Lessons Learned  
Deception Techniques  
• Cost Vs Benefits  
• Platforms  
• Management  
Review Cyber Defense Matrix  
Does deception add value or is it only security through obscurity? |
<p>| 8    | 3/26 | Wireless Testing | Challenges and liabilities to |</p>
<table>
<thead>
<tr>
<th>Date</th>
<th>Day</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>9/4</td>
<td>2</td>
<td>Penetration Testing Tools and Platforms</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- History of tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Crowd sourcing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Kali Linux</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trends</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Cloud</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Mobile</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- BYOD</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- IoT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Remote workforce</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Outsourcing</td>
</tr>
<tr>
<td>9/10</td>
<td>9</td>
<td>Password Cracking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Online/Offline</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Brute force</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Exploits</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Risks and mitigations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Custom</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tricks and Tradecraft</td>
</tr>
<tr>
<td>9/11</td>
<td>16</td>
<td>Pen Test: Putting it all together</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Presentations (Volunteers to go first)</td>
</tr>
<tr>
<td>9/12</td>
<td>23</td>
<td>Training and Exercises</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Test Ranges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Presentations</td>
</tr>
<tr>
<td>9/13</td>
<td>30</td>
<td>Open challenges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Current research</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Course review</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Project Presentations</td>
</tr>
<tr>
<td>5/7</td>
<td></td>
<td>Reading Day – No Classes</td>
</tr>
<tr>
<td>5/14</td>
<td></td>
<td><strong>FINAL EXAM</strong></td>
</tr>
</tbody>
</table>