Course Syllabus

University of Maryland - Shady Grove Campus
CCJS 418B: Cyber Investigations
Spring 2018 - Section SG91

Course Information

Day/Time: Wednesday, 12:30 PM – 3:00 PM

Location: Shady Grove Campus, Building III, Room 4219

Course description: This course will study cyber/network intrusion investigations and cyber security. It will provide an introduction to cyber attacks/network intrusions as well as cyber investigative methodologies and tools. Additionally, students will learn about common methods used by malicious cyber threat actors (attackers) and advanced persistent threat (APT) groups to compromise computers and networks. Students will learn how cyber investigators, incident response teams, and cyber security professionals use their expertise to triage, investigate, and prevent cyber/network intrusion attacks. Course topics will be reinforced through hands-on case studies and practical exercises covering recent cyber intrusion investigations. Previous completion of CCJS498I (Digital Forensics) is recommended and will assist students in this course, but it is not required.

Required reading:
### Grading Scale

<table>
<thead>
<tr>
<th>Grade</th>
<th>+</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>97 – 100 points</td>
<td>90 – 94 points</td>
</tr>
<tr>
<td></td>
<td>94 - 97 points</td>
<td>84 – 87 points</td>
</tr>
<tr>
<td>B</td>
<td>87 - 89 points</td>
<td>80 – 83 points</td>
</tr>
<tr>
<td></td>
<td>84 – 87 points</td>
<td>70 – 73 points</td>
</tr>
<tr>
<td>C</td>
<td>77 – 79 points</td>
<td>67 – 69 points</td>
</tr>
<tr>
<td></td>
<td>74 - 77 points</td>
<td>64 – 67 points</td>
</tr>
<tr>
<td>D</td>
<td>67 – 69 points</td>
<td>60 – 63 points</td>
</tr>
<tr>
<td>F</td>
<td>0 - 60 points</td>
<td></td>
</tr>
</tbody>
</table>

### Grading Criteria

<table>
<thead>
<tr>
<th>Component</th>
<th>Percentage of Final Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class Participation</td>
<td>10%</td>
</tr>
<tr>
<td>Mid-Term Exam <em>(open book)</em></td>
<td>30%</td>
</tr>
<tr>
<td>Case Studies/Scenarios/Labs</td>
<td>30%</td>
</tr>
<tr>
<td>Final Exam <em>(NOT open book)</em></td>
<td>30%</td>
</tr>
</tbody>
</table>

### Class Participation / Attendance Policy

Students are expected to participate in class. There will be various opportunities throughout the course to participate. Students will earn class participation points by attending class on time and participating in class discussions and asking/responding to questions in class. For each class that a student attends on time and actively participates, the student will receive 5 class participation points. Missed classes, late arrivals, and failure to participate will result in reduction of points. An unexcused absence will result in the loss of class participation points for that day. It is not possible to participate in class if you are not present in class. Students are asked not to use cell phones or be distracting to others during class.

Students are permitted to use laptop computers in class for note-taking purposes and use relating to class. Students who use cell phones and computers in class for any other reasons than those permitted by this syllabus will be penalized class participation points. A student's final class participation grade will be calculated at the end of the semester and will account for 10% of the student's final grade for the course.

An excused absence is an absence for which the student has the right to receive, and the instructor has the responsibility to provide, academic accommodation. Students are expected to take full responsibility for their own academic work and progress. Students, to progress satisfactorily, must meet all of the requirements of each course for which they are registered. Students are expected to attend classes
regularly. Consistent attendance offers students the most effective opportunity to gain command of course concepts and materials. Excused absences must be requested promptly and must be supported by appropriate documentation.

Absences stemming from work duties other than military obligation (e.g., unexpected changes in shift assignments) and traffic/transit problems do not typically qualify for excused absence. Events that justify an excused absence include:

- Religious observances
- Mandatory military obligation
- Illness of the student or illness of an immediate family member
- Participation in university activities at the request of university authorities
- Compelling circumstances beyond the student’s control (e.g., death in the family, required court appearance)

Excused absences do not alter the academic requirements for the course. Students are responsible for information and material missed on the day of absence. Students are, within reason, entitled to receive any materials provided to the class during the absence. Students are responsible for making provision to determine what course material they have missed and for completing required exercises in a timely manner. Students with excused absences will be entitled to a makeup exam at a mutually-agreed upon time between the professor and the student. However, students are reminded that except for emergencies, such arrangements must be made prior to the exam or assignment in which the student will miss due to an excused absence.

**Course Related Policies**

Students are strongly encouraged to review the University’s course-related policies and their rights related to various topics including: Academic Integrity, Code of Student Conduct, Sexual Misconduct, Discrimination, Accessibility, Attendance/Absences/Missed Assignments, Student Rights, Official UMD Communication, Mid-Term Grades, Complaints About Course Final Grades, Copyright and Intellectual Property, Final Exams, Course Evaluations, and Campus Resources. **Students should view these policies at the following URL. Additionally, these policies are posted on ELMS with this courses syllabus.**

http://www.ugst.umd.edu/courserelatedpolicies.html

**Inclement weather policy / Emergency evacuation**

In case of inclement weather, contact the Shady Grove campus hotline 301-738-6012. If class is cancelled for any reason, I will contact all students as soon as I am aware of the cancellation via e-mail and/or Elms/Canvass. Students may also sign up to receive electronic notification via www.shadygrove.umd.edu/weather/. In case of emergency, follow the emergency procedures discussed the first day of class and as posted in the building.

Students are strongly encouraged to sign up for the Shady Grove Campus Alert System (which is separate from the UMD College Park Alert System), at http://shadygrove.umd.edu/ (Click “USG Alerts” on the lower right-hand corner and sign up with one or multiple phone numbers and e-mail addresses.
Mid-Term and Final Exams

Students will be required to take a mid-term exam on **03/15/17 from 12:30 AM to 3:00 PM** and a final exam on the scheduled date, TO BE DETERMINED BY UMD. The mid-term exam will be open book/open notes and students will be able to use their textbooks, notes (handwritten and electronic), and any other course material including the slides from ELMS. The final exam will not be open book/open notes and students will not be permitted to utilize any reference material on the final exam. The mid-term and final exams will consist of multiple choice and true/false questions. Unless prior permission is given, all students are required to take the examination on the day it is administered. Before the mid-term and final exams an extensive exam review will be conducted. Students are strongly encouraged to attend these sessions. Excusal/make-up examinations will only be authorized for reasons consistent with University of Maryland policy. If prior permission is not obtained, students will receive a zero ("0") for that examination. If a make-up exam is granted, the make-up exam will consist of different questions than those originally offered. Both the mid-term and final exams will each account for 30% of the student's final grade in the course. The final exam will be cumulative, covering material that may have also been covered in the mid-term.

Case Studies/Practical Scenarios/Labs

During this course, there will be several "hands-on" exercises to demonstrate cyber investigative methods learned in this course. Completion of this exercises will generally be conducted in class, however some of them may be assigned as homework. These assignments will make up 30% of the student’s final grade. The instructor will decided on a case-by-case basis which of these practical exercises will allow for working together with other students and which must be an individual effort. This will be clearly states in the instructions of each of these practical exercises. For example:

- **Case Study:** Students will be provided a description of a real-world or fictional cyber attack/network intrusion and will be asked to answer questions about the case. These questions will be intended to reinforce specific topics learned in class. Generally, case studies are expected to be an individual efforts and will be completed as homework outside of class. Case studies will generally be no more than 10-15 questions. Case studies will generally be assigned as homework to be completed on ELMS. All case studies will be assigned in ELMS.

- **Practical Scenarios/Labs:** Students will participate in practical scenarios/labs in which they will utilize methods and/or tools learned in class. Students will be asked a series of questions about their scenario/lab. For example, after the class on the cyber attack method of “reconnaissance”, students may be asked to utilize open-source tools such as Google to conduct reconnaissance on an actual company and answer questions about that company. These practical scenarios/labs will generally be conducted during class and will be 10-15 questions. The instructor may allow collaboration with other students; this will be determined on a case-by-case basis depending on the goals of each individual practical scenario/lab.
**Academic Integrity**

The University of Maryland has a nationally recognized Code of Academic Integrity. The Code sets standards for academic integrity at Maryland for all undergraduate and graduate students. All students are expected to know and adhere to the Code of Academic Integrity, which is designed to ensure that the principle of academic honesty is upheld. All members of the University community share the responsibility and authority to challenge and make known acts of apparent academic dishonesty. All cases of suspect academic misconduct will be referred to the Student Honor Council at University of Maryland, College Park. Examples of violations of the Code of Academic Integrity include:

- **Cheating**: fraud, deceit, or dishonesty in any academic course or exercise in an attempt to gain an unfair advantage and/or intentionally using or attempting to use unauthorized materials, information, or study aids in any academic course or exercise.

- **Fabrication**: intentional and unauthorized falsification or invention of any information or citation in an academic course or exercise.

- **Facilitating Academic Dishonesty**: intentionally or knowingly helping or attempting to help another to violate any provision of this Code.

- **Plagiarism**: intentionally or knowingly representing the words or ideas of another as one's own in any academic course or exercise.

Cheating on any assignment or exam may result in the following disciplinary action: "XF" (a "cheating F") will be the grade earned for the course and you may face possible expulsion from the University of Maryland. Students are expected to write, sign, and/or agree to the Honor Pledge for all exams, papers, projects, and other graded materials:

> I pledge on my honor that I have not given or received any unauthorized assistance on this assignment/examination.

**Students Requiring Special Accommodations**

The Universities at Shady Grove (USG), in collaboration with institutional partners, is committed to ensuring the success of students. Through comprehensive services provided by Student and Academic Services (SAS), students receive academic, personal, social and career support. Our service centers offer a variety of resources such as personal and relationship counseling, academic and disability support, career coaching and resume development, student life events and financial aid assistance.

Specifically, for academic support, the Center for Academic Success (CAS) offers feedback on your papers and coaching on effective time management and study strategies. Schedule a one-on-one appointment today at https://sg.mywconline.com.

For information about all of our services, visit the SAS website: [http://shadygrove.umd.edu/campus-services/SAS](http://shadygrove.umd.edu/campus-services/SAS)

The University of Maryland is committed to creating and maintaining a welcoming and inclusive educational, working, and living environment for people of all abilities. The University of Maryland is committed to the principle that no qualified individual with a disability shall, on the basis of disability, be
excluded from participation in or be denied the benefits of the services, programs, or activities of the University, or be subjected to discrimination. The University of Maryland provides reasonable accommodations to qualified individuals. Disability Support Services (DSS) facilitates reasonable accommodations to qualified individuals. For assistance in obtaining an accommodation, contact Disability Support Service at 301.314.7682, or dissup@umd.edu.

Students that have an Accommodations Letter from DSS should bring this to the attention of the course instructor as soon as possible (within the first two weeks of class) in order to facilitate necessary accommodations. All requests requiring special accommodations will be addressed in accordance with University of Maryland policies.

**Course Evaluations**

Your participation in CourseEvalUM course evaluations is both your right and responsibility as a student. Your feedback is confidential and important to the improvement of teaching and learning at the University of Maryland as well as to the tenure, promotion, and retention of its instructors. You can go directly to the website (www.courseevalum.umd.edu) to complete your evaluations.

**Intellectual Property**

The lectures delivered in course and the course materials that are created/distributed in this course are protected by federal copyright law. Students are permitted to take notes and will be given access to class PowerPoint slides and other course material via Elms/Canvass. Students may not reproduce or distribute the lectures, slides, presentation material, articles, or other course material without explicit written consent from the instructor. Any student who wishes to record the all or part of this course must receive prior permission from the instructor. Recording any conversation in the State of Maryland is violation of Maryland Criminal Law.

**Classes / Topics**

| Class 1 | 01/24/18 | Introduction / Course Overview / Syllabus Review  
Cyber Incident Handling  
Introduction to Hacking Methods  
For next class:  
• Textbook – Incident Response - Chapter 1 |
|---|---|---|
| Class 2 | 01/31/18 | Intro / Review: Basic Networking and the Internet  
Introduction to Cyber Defense/Cyber Security  
Cyber Attack Methods – Reconnaissance  
Cyber Attack Methods – Scanning  
For next class:  
• Textbook – Incident Response - Chapter 2 |
| Class 3 | 02/07/18 | Cyber Attack Methods – Exploitation  
For next class:  
• Textbook – Incident Response - Chapter 3 |
<table>
<thead>
<tr>
<th>Class</th>
<th>Date</th>
<th>Topic</th>
<th>For next class</th>
</tr>
</thead>
</table>
| Class 4| 02/14/18 | Cyber Attack Methods – Persistence  
Cyber Attack Methods – Covering Tracks          | • Textbook – Incident Response - Chapter 4       |
| Class 5| 02/21/18 | The Advanced Persistent Threat (APT)  
Cyber Incident Management  
Cyber Threat Intelligence                          | • Textbook – Incident Response - Chapter 5 (skip pages 90-108)  
• Textbook – Incident Response - Chapter 6         |
| Class 6| 02/28/18 | Evidence Collection and Acquisition  
Intro / Review: Digital Forensics Methodologies  
Cyber Investigative Methods: Incident Response Tools | • Textbook – Incident Response, Chapter 9        |
| Class 7| 03/07/18 | CLASS WILL MEET IN COMPUTER LAB  
Cyber Investigative Methods: Network Forensics  
Mid-Term Review                                    | • Study for mid-term                             |
| Class 8| 03/14/18 | CLASS WILL MEET IN COMPUTER LAB  
Mid-Term Exam                                        | OPEN BOOK                                        | • Spring Break!                                   |
| Class 9| 03/28/18 | CLASS WILL MEET IN COMPUTER LAB  
Intro/Review - Encryption  
Cyber Attack Methods: Password Attacks  
Cyber Attack Methods: Cryptolocker/Ransomware Attacks | • Textbook – Incident Response, Chapter 11  
• Assigned ELMS reading                        |
| Class 10| 04/04/18| CLASS WILL MEET IN COMPUTER LAB  
Digital Forensics / Incident Response  
Cyber Threat Hunting                                 | • Textbook – Incident Response, Chapter 12  
• Assigned ELMS reading                        |
| Class 11| 04/11/18| Cyber Investigative Methods - Memory Forensics  
Cyber Investigative Methods - Timeline Analysis | • Textbook – Incident Response, Chapter 14  
• Assigned ELMS reading                        |
| Class 12| 04/18/18| Cyber Security Field / Cyber Vulnerability Assessments  
Network Penetration Testing (Pen Testing) | • Textbook – Incident Response, Chapter 15  
• Assigned ELMS reading                        |
| Class 13 | 04/25/18 | Cyber Investigative Methods: Malware Analysis/Reverse Engineering  
Managing a Cyber Investigative Unit |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>For next class:</td>
<td>• Assigned ELMS reading</td>
<td></td>
</tr>
</tbody>
</table>
| Class 14 | 05/02/18 | Cyber Espionage  
Cyber Warfare |
| For next class: | • Assigned ELMS reading |
| Class 15 | 05/09/17 | Cyber/Incident Response Trends  
Course Review  
Final Exam Review |
| FINAL | TBD | CLASS WILL MEET IN COMPUTER LAB  
FINAL EXAM  
THIS DATE/TIME HAS NOT YET BEEN DETERMINED BY UMD |