Course: DFOR 664 (aka TCOM 664) DL1 Incident Response Forensics

Semester: Spring 2024

Instructor: Michael Robinson (mrobinsv@gmu.edu)

Office Hours: Upon request

Course Meeting: Fridays, 4:30PM ET – 7:00PM ET

Location: Online

Course Description: Examines the workings of a Computer Emergency Response Team (CERT), including Incident Response, Vulnerability Assessment, Incident Analysis, Forensics, and Investigations.

Course Goals: At the conclusion of this course, the student will be familiar with incident response process to include the collection and analysis of artifacts. The student will be fully functional with the cyber critical incident response cycle. The course will also offer a theoretical as well as a practical (hands-on) approach to IR especially in the area of data collection and analysis.

Honor Code: The Mason Honor Code (http://oai.gmu.edu/honor-code/masons-honor-code/) is in effect. Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.

Course Material: The material provided in the course is proprietary. Uploading this material anywhere without the express permission of the instructor is strictly prohibited and a violation of the Mason Honor Code.

Textbooks: Multiple texts and sources are used in this course. No one book is used exclusively. Two books are required texts. For the purpose of exam preparation, Blackboard notes are stressed, but not used exclusively.

- Required: Clark, C. (2020). *Cybersecurity Incident Management Masters Guide. Volume 1: Preparation, Threat Response & Post-Incident Activity.* ISBN: 979-8656487900

Robinson, M. K. (2023). *Incident Response Workbook: Hands-on Activities in Incident Response Using PowerShell*. ISBN: 979-8392577197

- Optional: Cichonski, P., Millar, T., Grance, T., and Scarfone K. (2012). "SP 800-61 Rev 2: Computer Security Incident Handling Guide." National Institute of Standards and Technology.

Jones, D. W. and Hicks, J. (2017). *Learn Windows PowerShell in a Month of Lunches*. Third Edition. Manning Publications, Co.
ISBN: 978-1617294167

Important Dates:

Last day to drop with no tuition penalty	January 30
Last day to drop with a 50% tuition penalty	February 6
Last day of unrestricted withdrawal period	February 20
Final Exams	May 1-8

Academic Calendar: https://registrar.gmu.edu/calendars/spring_2024/

Course Schedule: The following table outlines the course schedule. Any changes to the syllabus will be posted in Blackboard.

Week	**Date**	**Topic**	**Reading Assignment** (read by class date)	**Presentation** (view by class date)	**Hands-on Activity** (done in class)	**Deliverable**
1	Jan 19	Introduction Incident Response / Incident Management	*Cybersecurity Incident Management* Chapters 1-3	Module 1	*Incident Response Workbook* Chapters 1-3	
2	Jan 26	Incident Management Methods and Teams	*Cybersecurity Incident Management* Chapters 4-5; 28	Module 2	*Incident Response Workbook* Chapter 4	
3	Feb 2	Pre-incident Preparation	*Cybersecurity Incident Management* Chapters 9-10	Module 3	*Incident Response Workbook* Chapter 5	Topics for Project 1
4	Feb 9	Starting the Incident Response	*Cybersecurity Incident Management* Chapters 14-15	Module 4	*Incident Response Workbook* Chapter 6	
5	Feb 16	Scope and Lead Development	*Cybersecurity Incident Management* Chapters 17-19	Module 5	*Incident Response Workbook* Chapter 7	
6	Feb 23	Live Data Collection	*Cybersecurity Incident Management* Chapters 20, 29	Module 6	*Incident Response Workbook* Chapter 8	
7	Mar 1	Forensic Duplication	-	Module 7	-	Mid-term exam (Content: Weeks 1-6)
	Mar 8	Spring Break	-	-	-	
8	Mar 15	Network Evidence	*Cybersecurity Incident Management* Chapter 23	Module 8	*Incident Response Workbook* Chapters 9	Project 1 – Case Study
9	Mar 22	Enterprise Services	*Cybersecurity Incident Management* Chapter 31	Module 9	*Incident Response Workbook* Chapter 10	

10	Mar 29	Investigating Applications / Systems	-	Module 10	*Incident Response Workbook* Chapter 11	
11	Apr 5	Student Presentations	*Cybersecurity Incident Management* Chapter 11	Module 11	*Incident Response Workbook* Chapter 12	Project 1 – Presentation
12	Apr 12	Student Presentations	*Cybersecurity Incident Management* Chapters 6-8, 16	Module 12	*Incident Response Workbook* Chapter 13	
13	Apr 19	Student Presentations	-	-		
14	Apr 26	Practical	-	-		Project 2 – Part 1 Project 2 – Part 2
15	May 3	Final Exam	-	-		Final exam (Content: Mostly on Weeks 7-13)

Grading:

Mid-term:	32%	(Open book, open notes)
Project 1: Paper	10%	
Project 1: Presentation:	5%	
Project 2 – Part 1:	15%	
Project 2 – Part 2:	5%	
Final:	33%	(Open book, open notes)

The following criteria will be used for the assignment of letter grades

A	92-100
A-	90-91
B+	87-89
B	83-86
B-	80-82
C	70-79
F	0-69

Exams: The format of mid-term and final exam will be a combination of multiple choice, fill-in, and short answer questions. Expect approximately 50 – 70 questions per exam. The final exam is not cumulative *per se*; however, knowledge of the material covered in the first half of the semester is integrated into material covered in the second half of the course. The exams will have a duration of 2 hours and be open book and open notes.

Projects: Project 1 is a research project where you will apply your knowledge of IR to an intrusion incident that you identify from online sources.
See project 1 document for details.

Project 2 is a PowerShell scripting exercise. See project 2 document for details.

Projects will be submitted via Blackboard. Projects will not be accepted via email or in-person.

Lectures and Discussions: Lectures will be recorded and made available via Blackboard. Students are required to watch each lecture and be familiar with the content. Ideally, the presentations should be watched prior to class. In each class, additional clarifying remarks may be made and a group discussion will be held to answer any questions that may exist.

Course Material: All course material will be available on GMU's Blackboard.

Software: Students will require access to a Windows-based computer or a virtual machine running Windows.

The following software will be helpful for completing the course. It should be installed on your personal computer.

Power Shell ISE – native to Microsoft Windows
WMIC – native to Microsoft Windows

Student Welcome: This link provides up to date information on IT services:
http://labs.vse.gmu.edu/uploads/FacultyFAQ/StudentWelcome.pdf

Students with disabilities who seek accommodations in a course must be registered with the GMU Office of Disability Services (ODS) and inform the instructor, in writing, at the beginning of the semester. See http://www2.gmu.edu/dpt/unilife/ods/ or call 703-993-2474 to access the ODS.

Communications: GMU's email system will be required for all written communication. Students may not use personal email accounts. Please see: https://mail.gmu.edu.