Course:	DFOR 664 (aka TCOM 664) DL1 Incident Response Forensics
Semester:	Spring 2022
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 text. For the purpose of exam preparation, Blackboard notes are stressed, but not used exclusively.
- Required:	Luttgens, J. T., Pepe, M., and Mandia, K. (2014). *Incident Response & Computer Forensics*. Third Edition. McGraw-Hill Education. ISBN: 978-0071798686.
- 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.

Murdoch, D. (2014). *Blue Team Handbook: Incident Response Edition*. Second Edition. CreateSpace. ISBN: 978-1500734756.

Important Dates:

Last day to drop with no tuition penalty	February 7
Last day to drop with a 50% tuition penalty	February 14
Last day of unrestricted withdrawal period	March 1
Final Exams	May 11-18

Academic Calendar: https://registrar.gmu.edu/calendars/spring-2021

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

Week	**Date**	**Topic**	**Reading Assignment** (to be completed by class date)	**Hands-on Activity**	**Deliverable**
1	Jan 28	Introduction Real World Incidents	*Incident Response & Computer Forensics.* Chapter 1	PowerShell 1	
2	Feb 4	Incident Response Handbook	*Incident Response & Computer Forensics.* Chapter 2	PowerShell 2	
3	Feb 11	Pre-incident Preparation	*Incident Response & Computer Forensics.* Chapter 3	PowerShell 3	Topics for Project 1
4	Feb 18	Starting the Incident Response	*Incident Response & Computer Forensics.* Chapter 4	PowerShell 4	
5	Feb 25	Scope and Lead Development	*Incident Response & Computer Forensics.* Chapters 5 & 6	PowerShell 5 ICMP traffic	
6	Mar 4	Live Data Collection (Memory)	*Incident Response & Computer Forensics.* Chapter 7	PowerShell 6 Persistence	
7	Mar 11	Forensic Duplication – Digital Media	*Incident Response & Computer Forensics.* Chapter 8	-	Mid-term exam
	Mar 18	Spring Break			
8	Mar 25	Network Evidence	*Incident Response & Computer Forensics.* Chapter 9	PowerShell 7 Parameters	Project 1 – Case Study
9	Apr 1	Enterprise Services	*Incident Response & Computer Forensics.* Chapter 10	PowerShell 8	
10	Apr 8	Investigating Applications / Systems	*Incident Response & Computer Forensics.* Chapter 12, 14	PowerShell 9 Hunting exercise	
11	Apr 15	WMIC Offense, Defense, and Forensics		PowerShell 10	

				Hunting exercises	
12	Apr 22	Student Presentations		Hunting exercise	Project 1 – Presentation
13	Apr 29	Student Presentations		Insider Risk example	Project 2 – PowerShell script
14	May 6	Student Presentations			
15	May 13				Final exam

Grading:

Mid-term:	35%	(Open book, open notes)
Project 1:	10%	
Presentation:	5%	
Project 2:	15%	
Final:	35%	(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: The following software will be helpful for completing the course. It should be installed on your personal computer.

Wireshark – www.wireshark.org
Snort – www.snort.org
Xpilco – www.xplico.org
Power Shell ISE – native to Microsoft Windows
WMIC – native to Microsoft Windows
Mandiant Redline – https://www.fireeye.com/services/freeware/redline.html

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.