CFRS 664 (aka TCOM 664)
IR
Spring 2019

Read this document in its entirety. You are responsible for its contents!

Instructor: Bob Osgood
rosgood@gmu.edu
Engr 3255 Office Hours Thursday 2:00 PM – 5:00 PM
And also by appointment

Classes Meet:

In Class
Day: Friday
Time: 4:30 – 7:10 PM
Where: Engr 1505

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 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 is in effect http://oai.gmu.edu/honor-code/masons-honor-code/

Student members of the George Mason University community pledge not to cheat, plagiarize, steal, and/or lie in matters related to academic work.

Mason Calendar: https://registrar.gmu.edu/calendars/spring-2018/

Course Schedule: (**Subject to Change**)

The 1st class is on Friday, 1/25/2019, 4:30 PM, Engr 1505
Midterm Friday, TBD, 4:30 PM, Engr 1505
Final Friday, 5/10/2019, 4:30 PM, Engr 1505

Week	Topic	Reading Assignments	Projects Due
1	Intro and Real-World Incidents	LPM Chapter 1	
2	IR Handbook	LPM Chapter 2	
3	Pre-Incident Preparation	LPM Chapter 3	Project 1 Topics Due 2/8/2019
4	Getting the IR Started	LPM Chapter 4	
5	Scope and Lead Development	LPM Chapters 5 & 6	
6	Live Data Collection (Memory)	LPM Chapter 7	
	Midterm – 2 Hour Online Timed Exam: Open Book, Notes, Computer		

7	Forensic Duplication – Digital Media	LPM Chapter 8	
	Spring Break No Class		Project 1 3/15/2019
8	Network Evidence	LPM Chapter 9	
9	Enterprise Services Google Rapid Response	LPM Chapter 10	
10	Investigating Applications/Systems	LPM Chapter 14	
11	WMIC Offense, Defense, and Forensics	See Black Board	
12	WMIC Offense, Defense, and Forensics	See Black Board	
13	Presentations		Project 2 4/19/2019
14	Presentations		4/26/2018
15	Presentations		5/3/2019
	Final Exam - 2 Hour Online Timed Exam: Open Book, Notes, and Computer		5/10/2019

Grading: **Mid-term:** **35% (Open Book, Notes, and Computer)**
Projects: **30%**
Final: **35% (Open Book, Notes, and Computer)**

Exams: The format of exams 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, notes, and computer.

Online Lectures: If required, online lectures will be synchronous online via Blackboard Collaborate. Barring technical difficulties, all lectures will be recorded for later review.

Course Material: All course material is available on Mason Blackboard.

How do you get on Blackboard?

-Go to: https://mymasonportal.gmu.edu/webapps/portal/frameset.jsp
-Login with your Mason Credentials
-Click on the Courses tab
-Click on the CFRS-664

How do I get to the online lectures?

-Follow instructions to login into Blackboard
-Click on **Tools**
-Click on **Blackboard Collaborate**
-You should see the current session listed
-Previously recorded sessions are accessed via the **Previously Recorded** Tab

Software That You Will Need (Free Stuff) (place on your external drive and/or laptop)

Software that you should have loaded on your personal computer include

-Wireshark www.wireshark.org
-SNORT (offline mode only) www.snort.org
-Xplico www.xplico.org

-Power Shell ISE	Native to Microsoft
-WMIC	Native to Microsoft
-Mandiant RedLine	Fireeye (Mandiant)
-GRR	https://github.com/google/grr

Required Reading and Reference Material: Multiple books and sources are used to create this course. No one book is used exclusively. Of these, two are required text. For the purpose of exam preparation, the Blackboard notes are stressed.

Required: Incident Response & Computer Forensics, 3rd Edition, Luttgens, Pepe, and Mandia, McGraw Hill, ISBN: 97800717986866

Required: Don Murdoch, Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder, CreateSpace Independent Publishing Platform; 2.0 edition (August 3, 2014), ISBN: 9781500734756

Optional: Learn Windows PowerShell in a Month of Lunches 3rd Ed, Don Jones and Jeffrey Hicks, Manning, ISBN: 978-1-61729-416-7

References from the Web include the following sites:

Cert: http://www.cert.org
Cisco: http://www.cisco.com
Technet: http://technet.microsoft.com/en-us/default.aspx
Sourceforge.net: http://sourceforge.net

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.

Note: ALL STUDENTS MUST HAVE GMU CREDENTIALS (EMAIL ACCOUNT) AND HAVE ACCESS TO https://mymasonportal.gmu.edu !!

Note: All Email Correspondence Will Take Place From Your GMU Account to rosgood@gmu.edu!!!

Note: All Students Are Responsible for All of the Material in This Course