CFRS 664
IR
Spring 2017

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
Saturday 8:00 AM – 9:00 AM
And also by appointment

Classes Meet:

In Class
Day: Monday
Time: 4:30 – 7:10 PM
Where: Engr 4457

Course Description: Examines 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 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: http://registrar.gmu.edu/calendar.html

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

Week	Date	Topic	Reading Assignments	Projects Due
1	1/23/2017	Intro and Real-World Incidents	LPM Chapter 1	
2	1/30/2017	IR Handbook	LPM Chapter 2	
3	2/6/2017	Pre-Incident Preparation	LPM Chapter 3	
4	2/13/2017	Getting the IR Started	LPM Chapter 4	
5	2/20/2017	Scope and Lead Development	LPM Chapters 5 & 6	
6	2/27/2017	Live Data Collection (Memory)	LPM Chapter 7	
	3/6/2017	Midterm – 2 Hour Online Timed Exam: Open Book, Notes, Computer		Project 1
	3/13/2017	Spring Break		

7	3/20/2017	Forensic Duplication – Digital Media	LPM Chapter 8	
8	3/27/2017	Network Evidence	LPM Chapter 9	
9	4/3/2017	Enterprise Services	LPM Chapter 10	
10	4/10/2017	Analysis Methodology	LPM Chapter 11	Project 2
11	4/17/2017	Investigating Systems	Murdoch	
12	4/24/2017	Investigating Applications	LPM Chapter 14	
13	5/1/2017	Presentations		
	5/8/2017	Presentation		
	5/15/2017	Final Exam - 2 Hour Online Timed Exam: Open Book, Notes, and Computer		

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 and notes.

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

Mason Calendar: http://registrar.gmu.edu/calendar.html

The above link will provide you with Mason's important dates and deadlines.

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

In order for Blackboard to work right, what do I need loaded on my computer

-JAVA
-Quicktime
-Flash

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
-Network Miner	sourceforge.net/projects/networkminer/
-SNORT (offline mode only)	www.snort.org
-Xplico	www.xplico.org
-Process Monitor	Technet
-Process Explorer	Technet
-TCPView	Technet
-PEID	Technet
-Dependency Walker	Technet
-Mandiant RedLine	Fireeye (Mandiant)
-Autospsy	http://www.autopsy.com/
-FTK Imager	http://accessdata.com/
-Volatility	http://www.volatilityfoundation.org/

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
Perl: www.perl.org
Python: www.python.org
Foundstone: www.foundstone.com

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