CFRS/TCOM 660
Network Forensics
Spring 2016

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 Section
Day: Saturday
Time: 9:00 AM – 11:45 AM
Where: Engr 5358

Course Description: This course deals with the collection, preservation, and analysis of network generated digital evidence such that this evidence can be successfully presented in a court of law (both civil and criminal). The relevant federal laws will be examined as well as private sector applications. The capture/intercept of digital evidence, the collection and analysis of volatile data, and the reporting of such information will be examined.

Course Goals: At the conclusion of this course, the student will have learned the laws applicable to presenting network digital evidence in a court of law. The student will be able to successfully intercept network traffic, collect and analyze volatile data, decipher network traffic, and report this information in a suitable format.

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

Prerequisites: TCOM 509/529 (aka TCOM 535) and working knowledge of a computer language and operating systems

Cross Listed: TCOM 660

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

Week	Date	Topic	Reading Assignments	Projects Due
1	1/23/2016	L-1 Introduction and review of Network Protocols Application to Network Intercepts	Notes from Blackboard Chappell Ch 1 & 2 Bejtlilch Ch 2	

2	1/30/2016	Federal laws pertaining to the interception of digital evidence will be presented.	Notes and pdf's from Blackboard www.house.gov www.cybercrime.gov	
3	2/6/2016	L-3 Incident Response Windows	ABJP Ch 1	
4	2/13/2016	L-4 Incident Response Unix/Linux	JBR Ch 2	Project 1
5	2/20/2016	L-5 Collecting Network Based Evidence	Chappell Ch 3 & 4 Bejtlich Ch 1	
6	2/27/2016	L-6 Building Response Tools	JBR Ch 16	
7	3/5/2016	Midterm – In Class - 2 Hour Timed Exam – Open Book & Notes		Project 2
	3/12/2016	Spring Break		
7	3/19/2016	L-8 Unknown Code Analysis	ABJP Ch 10	
9	3/26/2016	L-9 Windows Memory Analysis and Persistence	ABJP Ch 3, 6, 9	
9	4/2/2016	L-7 Email Analysis - Pre-recorded on Blackboard – Do not come to class	Notes from Blackboard Chappell Ch 25	
10	4/9/2016	L-10 Analyzing Network Traffic	Chappell Ch 28 & 29	Project 3
11	4/16/2016	L-11 Analyzing Network Traffic	Chappell Ch 30 & 31 Bejtlich 6 & 7	
12	4/23/2016	More Analyzing Network Traffic	Bejtlich Ch 7	
13	4/30/2016	L-12 Routers/Firewalls	Notes from Blackboard Liu – Cisco Router & Switch Forensics	Project 4
14	5/7/2016	Final Exam - In Class - 2 Hour Timed Exam – Open Book, Notes, and Computer		

Grading: **Mid-term:** **30% (Open Book, Notes, and Computer)**
4 Projects: **40%**
Final: **30% (Open Book, Notes, and Computer)**

Projects: There will be four projects assigned during the semester. All projects must be typed, Times Roman 12 point, double spaced, with one inch margins. Each project will have a **maximum** length not including diagrams and bibliography. Each project is worth 10% of the total grade.

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: In certain situations, we will have class online via Blackboard Collaborate. You will be contacted by email ahead of time should a class be held online. Online classes will be recorded and saved 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-660-001/TCOM-660-001(Fall 2014) course

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

External USB Drive Required (500 GB or higher)

An External USB drive is required in order to maintain your software and virtual machines. An Ubuntu 14.XX or later VM is required.

Thumb Drive (16 GB or higher)

A Thumb Drive is required for Project 3. This Thumb Drive will be returned to you after Project 3 is graded.

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)
-Others TBD	

These tools are available on Blackboard or if you wish the latest and greatest, you can just Google for the tool.

VM's – Have VM's of Kali and Ubuntu

Lab Computers – In class we will be using lab computers. **Please make sure that your computer is working properly prior to the start of class**. If your machine is not working, please let me know and switch to another computer.

Open Computer Lab - The open computer lab is located in Engr 1506. BlackLight and Nuix as well as the tools listed above are installed on these computers as well as the software listed above.

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: The Practice of Network Security Monitoring, Richard Bejtlich, No Starch Press, ISBN: 978-1-59327-509-9 (**Bejtlich**)

Required: Wireshark Network Analysis 2nd Ed, Laura Chappell, Chappell University, www.wiresharkbook.com, ISBN 978-1-893939-94-3 (**Chappell**)

Optional: Mastering Windows Network Forensics and Investigation 2nd Edition; Anson, Bunting, Johnson, and Pearson; Sybex, 2012; ISBN: 978-1-118-16382-5 (**ABJP**)

Optional: Windows Forensic Analysis, Harlan Carvey, Syngress, ISBN #9781597494229

Optional: Real Digital Forensics; Jones, Bejtlich, and Rose; Addison Wesley; ISBN #0321240693 (**JBR**)

Optional: Mastering Windows Network Forensics and Investigation; Anson and Bunting; Sybex; ISBN #9780470097625

Optional: Wireshark & Ethereal Packet Sniffing; Orebaugh, Ramirez, and Beale; Syngress; ISBN #1597490733

Optional: Incident Response & Computer Forensics, Second and Third Editions; Kevin Mandia, Chris Prosise, & Matt Pepe; McGraw
Hill; ISBN #007222696X (2nd Ed), #9780071798686 (3rd Ed)

Optional: Web Security; Mike Shema; Osborne; ISBN #0072227842

Optional: Cisco Router and Switch Forensics; Dale Liu; Syngress; ISBN #9781597494182 (**Liu**)

Optional: Practical Malware Analysis; Sikorski and Hinig; No Starch Press; ISBN # 9781593272906

References from the Web include the following sites:

U. S. Congress: http://www.house.gov
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
Mandiant: www.mandiant.com Now Part of FireEye

Visio

Visio is a Microsoft Office product that you should all be familiar with.

Visio can be purchased @ the Mason Computer Store @ a reduced price, you can use the free Visio viewer (with limited functionality), you can use any of the open Mason computer labs since they all have Visio, Mason Virtual Computing Lab (http://www.vcl.gmu.edu) , or you can obtain Visio through MSDN.

Mason VMWare link is below

http://e5.onthehub.com/WebStore/ProductsByMajorVersionList.aspx?ws=57245579-6f24-de11-a497-0030485a8df0&vsro=8&JSEnabled=1

Other software packages that can be obtained through this link.

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

Projects 1, 2, and 4 will be delivered by you through Blackboard. Project 3 must be physically handed in.