George Mason University
CFRS 780-001: Deep Packet Inspection
CRN: 77076
Fall 2014, August 25, 2014 - December 9, 2014
Innovation Hall 318, Tuesdays 7:20 - 10:00

Instructor

Jennifer Deavers
jdeavers@gmu.edu
Office Hours: Available upon request

Description

This course will familiarize students with network forensics. Students will identify data that can be retrieved from packets. Students will correlate data. Students will apply industry best practices to evidence collection and analysis with hands-on exercises using current tools. Student should be ready to perform the majority of their work in a terminal command line environment.

Learning Objectives

Upon completing the course, students will be able to:

- ❏ Analyze data retrieved from network packet capture data using current tools
- ❏ Select and configure various open-source tools for live and network forensics analysis and utilise these tools for live and network investigation
- ❏ Develop and practice an advanced knowledge of key live and network forensic principles and methods
- ❏ Comprehend common threats and vulnerabilities to which a network may be exposed

Grading

Each assignment, quiz, project, and exam will be graded on a 0-100 point scale.

The final average is calculated by the following weights.

Homework: 30%
Midterm: 30%
Final: 40%
Total: 100%

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

The course will adhere to the university's policies on grading.

Homework

Homework labs will be provided to students over the course to allow students to apply the methods discussed in class. These assignments will be provided in class and announced via the course website. Homework assignments are due two weeks following the assigned date. Homework assignments are worth thirty percent (30%) of your overall grade. Late homework assignments will be assessed a penalty of twenty - five (25%) of the assignment grade for each day of tardiness. **No homework will be accepted after the third day.**

Midterm

A midterm exam will be given during week eight and will cover information provided during lectures, required and supplemental readings , and any information derived from homework assignments.

Software Requirements

Students are to bring the following materials to class:

- ❏ At least one USB flash drive
- ❏ Laptops with VMware, VM Fusion, or VMplayer

Textbook

Title: Network Forensics: Tracking Hackers through Cyberspace
Author: Sherri Davidoff, Jonathan Ham
Publisher: Prentice Hall
ISBN 10: 0132564718

Class Attendance

Attendance is mandatory. A number of classes will involve the hands-on use of forensics tools, which will be used in the classroom. In the event that a student cannot attend class due to an emergency or crisis, the student is to contact the instructor as soon as possible.

Responsible Use of Computing Policy

Use of computer equipment, including Internet connections within the classroom will be conducted in accordance with the University's Responsible Use of Computing (RUC) Policy. This applies to all academic and operational departments and offices at all university locations owned or leased. The policies and procedures provided herein apply to all Mason faculty, staff, students, visitors, and contractors.

The university provides and maintains general computing services, including web and Internet resources, and telecommunication technology to support the education, research, and work of its faculty, staff, and students. At the same time, Mason wishes to protect all users' rights to an open exchange of ideas and information. This policy sets forth the responsibilities of each member of the Mason community in preserving the security, confidentiality, availability, and integrity of Mason computing resources. To accomplish these ends, this policy supports investigations of complaints involving Mason computing abuse, including sexual harassment, honor code, federal, state, applicable industry, and local law violations.

University faculty and staff members, as state employees, are subject to the Freedom of Information Act, §2.2-3700, et seq., of the Code of Virginia, and all applicable state and federal rules and regulations. While this policy endeavors to maintain user confidentiality, it cannot create, nor should faculty or staff members presume, any expectation of privacy.

Violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities. It is the responsibility of all users of Mason computing resources to read and follow this policy and all applicable laws and procedures (user sign-on agreement).

For more information regarding the RUC Policy, consult the student handbook.

Communications

Communication on issues relating to the individual student should be conducted using email. Email messages from the Instructor to all class members will be sent to students' GMU email addresses if you use another email account as your primary address, you should forward your GMU email to that account.

*Schedule

Week	Date	Tools or Topics
1	08/26/2014	Introduction
2	09/02/2014	Packet Carving - GUI vs. Command Line
3	09/09/2014	Tools I
4	09/16/2014	Tools II
5	09/23/2014	Tools III
6	09/30/2014	Tools IV
7	**10/07/2014**	**MIDTERM**
8	**10/14/2014**	**CLASS DOES NOT MEET**
9	10/21/2014	python scripting for packet carving I
10	10/28/2014	python scripting for packet carving part II
11	11/04/2014	Network Tunneling
12	11/11/2014	Command and Control Communication
13	11/18/2014	I can hear you! Pcap files containing VoIP
14	11/25/2014	Take it up a level - Looking at netflow
15	12/02/2014	Visualization
16	12/09/2014	Packet Challenge
17	**12/16/2014**	**FINAL**

*This schedule is subject to revision before and during this course.

Key Dates - http://studentaccounts.gmu.edu/dates.html#fall

Fall 2014	Date
First day of classes; last day to submit Domicile Reclassification Application; **Payment Due Date**	August 25
Labor Day, university closed	September 1
Last day to drop with no tuition penalty	September 2
Last day to add classes — all individualized section forms due	September 2
Last day to drop with a 33% tuition penalty	September 16
Last day to drop with a 67% tuition penalty	September 26
Last day to drop; Last day Third Party Billing Authorizations accepted	September 26
Last Day to enroll in Mason 2 Payment Plan	September 9
Midterm progress reporting period (100-200 level classes)—grades available via Patriot Web	September 22 - October 17
Selective Withdrawal Period (undergraduate students only)	September 29 - October 24
Columbus Day recess (Monday classes/labs meet Tuesday. Tuesday classes do not meet this week)	October 13
Incomplete work from spring/summer 2014 due to instructor	October 24
Incomplete grade changes from spring/summer 2014 due to registrar	October 31
Thanksgiving recess	November 26 - November 30
Last day of classes	December 6
Reading Days	December 8 - December 9
Exam Period	December 10 - December 17
Degree Conferral Date	December 18, 2014