George Mason University
CFRS 730-001: Deep Packet Inspection
CRN: 14475
Jan 19, 2015 - May 13, 2015
Nguyen Engineering Building 5358, 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 command line tools
- ❏ Select and configure various open-source tools for live and network forensics analysis and utilise these tools for 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

Tool Share: 25%
Midterm: 25%
PCAP Challenge: 25%
Final: 25%
Total: 100%

Tool Share

The class will consist of a tool share. The tool share project will include an analytic paper detailing your analysis on several command line protocol or traffic analysis tools. A short presentation detailing the results of your analysis and demonstrating your assigned tools will also be a requirement. The report and presentation are both due on the assigned class week. Twenty percent (20%) of the tool share grade will come from the presentation material forty percent (40%) will come from the information derived in the report and forty percent will come from the (40%) demonstration.

tcpdump	tshark	hping3	snort	Xplico	findsmtpinfo
splunk	cat	ngrep	tail	Nettool	intrace
chaos reader	p0f	arp	Bro	Paros	driftnet
foremost	tcptrack	pcapcat	tcpxtract	Yara	Web Scarb
dsniff	tcpflow	strings	whois	nfdump	clamscan
nftcracker	argus	tcppick	SiLK	iodine	tcptrace
chopshop	dshell	honey snap	fiddler	burp suite	***more tools***

Midterm

A midterm exam will be given during week seven and will cover information provided during lectures, required and supplemental readings, and any information derived from the tool share presentations and demonstrations.

PCAP Challenge

Most classes will include a PCAP challenge. The purpose of the PCAP challenge is to hone your command line skills. A PCAP file will be released during class, with associated challenge questions. The challenge can be completed separately or with a partner.Utilize tools from the tool share or from command line recipes. The PCAP challenge will be started during class, the answers should be submitted individually on Blackboard before the start of the following class.

Software Requirements

Students are to bring the following materials to class:

- ❏ Laptops with VMware, VM Fusion, or VMplayer
- ❏ Kali Linux 1.0.9 64-bit - http://www.kali.org/downloads/

Textbook

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

Supplemental Materials

http://packetlife.net - [Cheat Sheets and Sample Packet Captures]
http://packetstormsecurity.com/

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.

Disability Accommodations

If you have a documented learning disability or other condition that may affect academic performance you should: 1) make sure this documentation is on file with Office of Disability Services (SUB I, Rm. 4205; 993-2474;http://ods.gmu.edu) to determine the accommodations you need; and 2) talk with me to discuss your accommodation needs.

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.

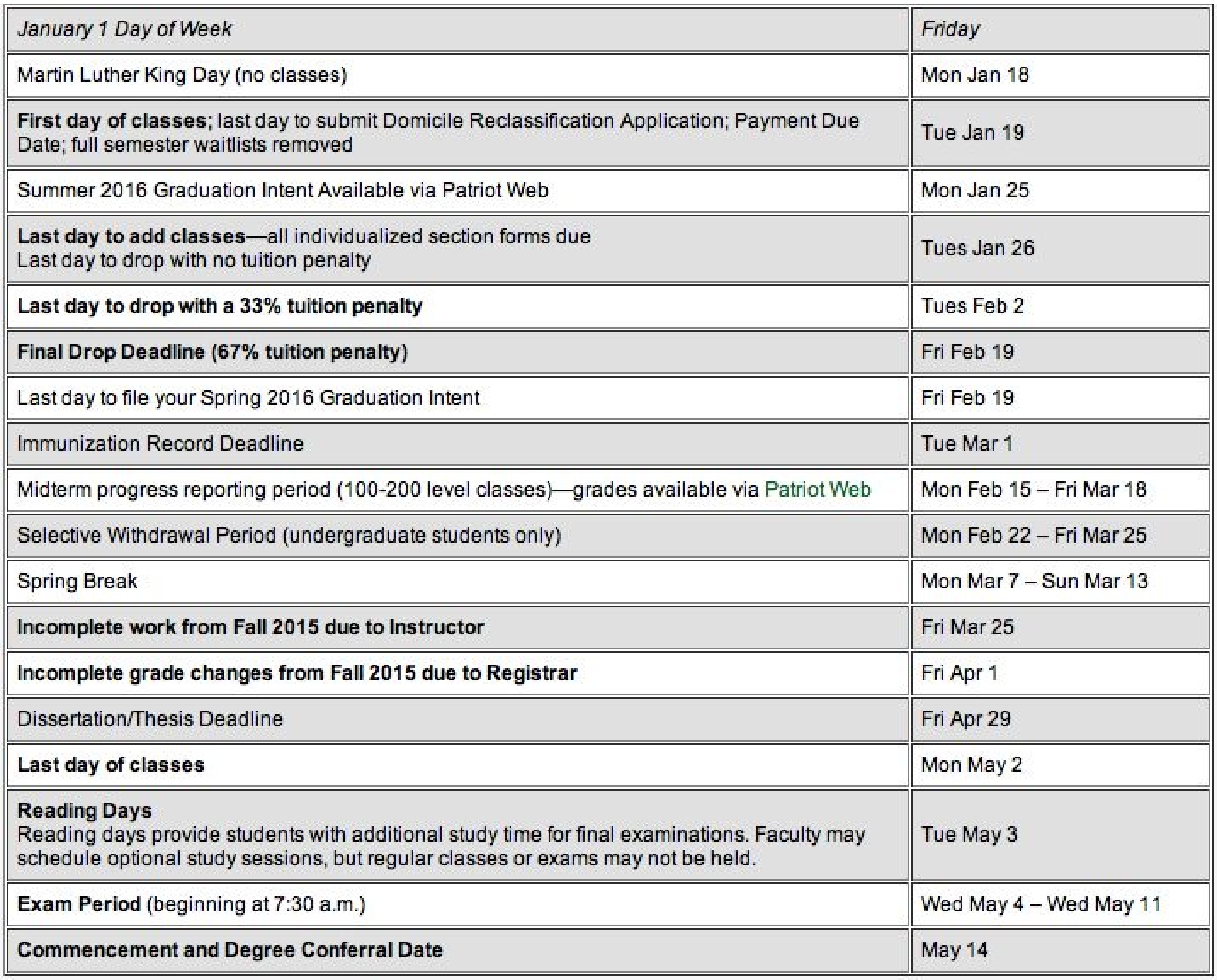
Violations of this policy may result in revocation of access, suspension of accounts, disciplinary action, or prosecution. Evidence of illegal activity will be turned over to the appropriate authorities. It is the responsibility of all users of Mason computing resources to read and follow this policy 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.

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



January 1 Day of Week	*Friday*
Martin Luther King Day (no classes)	Mon Jan 18
First day of classes; last day to submit Domicile Reclassification Application; Payment Due Date; full semester waitlists removed	Tue Jan 19
Summer 2016 Graduation Intent Available via Patriot Web	Mon Jan 25
Last day to add classes—all individualized section forms due Last day to drop with no tuition penalty	Tues Jan 26
Last day to drop with a 33% tuition penalty	Tues Feb 2
Final Drop Deadline (67% tuition penalty)	Fri Feb 19
Last day to file your Spring 2016 Graduation Intent	Fri Feb 19
Immunization Record Deadline	Tue Mar 1
Midterm progress reporting period (100-200 level classes)—grades available via Patriot Web	Mon Feb 15 – Fri Mar 18
Selective Withdrawal Period (undergraduate students only)	Mon Feb 22 – Fri Mar 25
Spring Break	Mon Mar 7 – Sun Mar 13
Incomplete work from Fall 2015 due to Instructor	Fri Mar 25
Incomplete grade changes from Fall 2015 due to Registrar	Fri Apr 1
Dissertation/Thesis Deadline	Fri Apr 29
Last day of classes	Mon May 2
Reading Days Reading days provide students with additional study time for final examinations. Faculty may schedule optional study sessions, but regular classes or exams may not be held.	Tue May 3
Exam Period (beginning at 7:30 a.m.)	Wed May 4 – Wed May 11
Commencement and Degree Conferral Date	May 14

*Schedule

Week	Date	Tools or Topics	Readings	Due Date
1	01/19/2016	Introduction	Tracking Hackers - Chapter 1	
2	01/26/2016	Evidence, Network Evidence Sources, OSI Model, Linux Commands, Ports	Tracking Hackers - Chapter 2	
3	02/02/2016	Tool Share 1	Tracking Hackers - Chapter 3	PC 1
4	02/09/2016	Tool Share 2	Tracking Hackers - Chapter 4	PC 2
5	02/16/2016			PC 3
6	02/23/2016	Tool Share 3 & **Midterm Review**	Tracking Hackers - Chapter 5	PC 4
7	**03/01/2016**	**MIDTERM**		
8	**03/08/2016**	**CLASS DOES NOT MEET**		
9	03/15/2016	Tool Share 4 Guest - *Penetration testing on car infotainment systems*	Violent Python Chapter 4 - Network Traffic Analysis with Python	
10	03/29/2016	Tool Share 5 **python scripting**	Supplemental reading	PC 5
11	04/05/2016	Tool Share 6	Supplemental reading	PC 6
12	04/12/2016	Looking Under SSL	Supplemental reading	PC 7
13	04/19/2016	python scripting - scapy	Supplemental reading	PC 8
14	04/26/2016	Web Proxies	Chapter 10	
15	04/28/2016	Netwitness [Dan Mitchell]	Supplemental reading	PC 9
16	**05/03/2016**	**Reading Day/CLASS DOES NOT MEET**		
17	**05/10/2016**	**FINAL**		

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

PC = Packet Challenge