EGR 8489: Malware Analysis and Defense

Class Meetings

Section 001 and DL1: Tuesdays, 6:10pm – 8:50pm, CEER 208

Instructor

Professor Hasshi Sudler

Adjunct Professor (office through ECE)

Tel: 267-322-8352

email: hasshi.sudler@villanova.edu

Web: http://www.homepage.villanova.edu/hasshi.sudler

Office Hours

Office hours are available by appointment. Please contact the instructor to arrange a meeting time.

Course Objectives

To enhance professionals with the ability to:

- To provide an analysis of malicious software functionality and architecture,
- To investigate the structure of various malware code.
- To study a variety of analysis tools and defense options, including basic static and dynamic analysis, advanced static and dynamic analysis, reverse engineering and memory forensics.

Grading Policy

Your final grade will be determined from the following:

- Exams: 20%
- Homework: 30%
- Participation: 20%
- Final Exam: 30%

The scale used to assign letter grades is:

Numerical Grade	Letter Grade	Numerical Grade	Letter Grade
A	94 to 100	C	73 to 76
A-	90 to 93	C-	70 to 72
B+	87 to 89	D+	67 to 69
B	83 to 86	D	63 to 66
B-	80 to 82	D-	60 to 62
C+	77 to 79	F	Less than 60

Attendance

Class and laboratory attendance for first-year students is mandatory. A first-year student will receive a grade of "Y" (failure) whenever the number of unexcused absences in a course exceeds twice the number of weekly class meetings for the course.

State here if attendance is mandatory or not for your class. Provide a description of what it means to be present (seated and ready to go or just in the room, be explicit).

Where possible, students should inform their instructors if they plan to be late or absent from class. In all cases, students should be prepared to provide documentation to petition for *excused* absences to the appropriate Associate Dean. The form for requesting an *excused* absence can be found here (http://www1.villanova.edu/villanova/engineering/resources/policies/forms/studentAbsence.html). Excused absences do not count toward a failure in the course for first year students. Absence from class does not release the student from work assigned. Students who miss an in-class obligation (exam, presentation, etc.) due to an excused absence will not be penalized - the instructor may offer a make-up test, arrange an alternative time for a presentation, exempt a student from the assignment, or provide another arrangement.

The University's list of excused absences for all students includes the following:

- participation in NCAA athletic competitions
- participation in special academic events (e.g., conferences, field trips, project competitions)
- participation in official university business (e.g., student representatives attending meetings related to university governance)
- attendance at significant events involving the immediate family (e.g., funerals, weddings)
- religious holidays - see the University's policy on Religious Holidays
- college-approved participation in placement activities (e.g., job interviews, graduate school interviews, attending job fairs)
- documented serious illness or disability (see below how to document)

Course Materials

The course will require you to either download or access web tools for ethical hacking exercises.

Readings will be provided and should be read prior to class discussions.

Academic Integrity

The College of Engineering is committed to creating an environment of academic integrity and ethical decision-making that we hope is reflected in the actions of our students and graduates. As Villanova students, integrity is central to the University mission. As engineers, our code of conduct requires us to place honor and integrity at the forefront of everything we do. As engineering students, it is expected that you will begin to adopt these values and instill them into your work habits. Students violating the academic integrity policy will receive a zero on that assignment or exam and the violation will be reported to the Associate Dean for Academic Affairs.

The University's academic integrity policy can be found here: https://www1.villanova.edu/villanova/provost/resources/student/policies/integrity.html.

The College of Engineering has adopted the following exam guidelines:

- Students must arrive before the start of the exam. Under exceptional circumstances a student may need to arrive late, but he/she can enter the exam no later than 5 minutes after the start of the exam.
- All cell phones must be turned off and stored away until the student exits the exam room.
- The official Villanova class attendance policy must be followed when requesting excuses for absences or lateness to an exam.
- Each student must write and sign the following statement, "*I have neither given nor received any unauthorized assistance in the completion of this exam.*"

Students with Disabilities

It is the policy of Villanova to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability please contact me after class or during office hours to make arrangements.

If you have a non-physical disability you need to register with the Learning Support Office by contacting 610-519-5176 or at learning.support.services@villanova.edu as soon as possible. Registration is needed to receive accommodations.

The Office of Disability Services collaborates with students, faculty, staff, and community members to create diverse learning environments that are usable, equitable, inclusive and sustainable. The ODS provides Villanova University students with physical disabilities the necessary support to successfully complete their education and participate in activities available to all students. If you have a diagnosed disability and plan to utilize academic accommodations, please contact and register with Gregory Hannah, advisor to students with disabilities @ 610-519-3209 or visit the office on the second floor of the Connelly Center.

Schedule

You should include a course schedule that includes all major deadlines, including exams.

Lectures	**Date**	**Descriptions**
1	16-Jan	Overview of Malware and Anonymous Researching
2	23-Jan	Designing a Lab for Malware Analysis
3	30-Jan	Standing Up Physical and Virtual Machines for Malware Analysis
4	6-Feb	Basic Static Analysis

5	13-Feb	Basic Dynamic Analysis
6	20-Feb	Advanced Static Analysis
7	27-Feb	Using IDA Pro (WEEK OF MIDTERM EXAM)
8	6-Mar	NO CLASSES – SPRING BREAK
9	13-Mar	Advanced Dynamic Analysis
10	20-Mar	Analyzing Malicious Programs and Files
11	27-Mar	Malware Behavior and Network Signatures
12	3-Apr	Reverse Engineering
13	10-Apr	Packers and Unpackers
14	17-Apr	Memory Forensics
15	24-Apr	Presentations of Market Products (WEEK OF FINAL EXAM)
16	1-May	Research Presentation

Course Management

Distance Learners:

To help facilitate a dynamic learning environment, all Distance Learning students are invited to attend classroom lectures in person if time and travel permits.