COURSE SYLLABUS

1 ECE 8489 - Malware Analysis and Defense

2 Meeting Information

3 credits, 3 contact hours Example: (Two 75-minute lectures)

a. **Section 001:**
Lecture: Mfrom 06:10 pm to 08:50 pm Location: CEER 307,

b. **Section DL1:**
Lecture: Mfrom 06:10 pm to 08:50 pm Location: TBA,

3 Course Instructor(s), TA(s)

a. **Section 001:**

Class Instructor:	Hasshi L. Sudler
Office Hours:	, or by appt.
TA:	None

b. **Section DL1:**

Class Instructor:	Hasshi L. Sudler
Office Hours:	, or by appt.
TA:	None

4 Textbook

Monnappa K A., *Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware*, Packt Publishing, 2018. ISBN: ISBN 978-1-78839-250-1. OPTIONAL.

a. **Other Supplemental Materials:** The course will require you to either download or access web tools for exercises. Readings will be provided and should be read prior to class discussions.

5 Specific Course Information

a. **Catalog Description**
Malicious software detection and defenses including Static Analysis, Dynamics Analysis and other techniques such as using IDAPro, Viruses, worms and Trojan horses, logic bombs, malicious web server scripts and software. Anatomy of well-known viruses and worms. Methodologies used by the anti-virus/spyware vendors and freeware.

b. **Prerequisites:** None; **Co-requisites:** None

c.

6 Course-specific Goals

a. Course Objective: To provide an analysis of malicious software functionality and architecture, and to investigate the structure of various malware code. The course studies a variety of analysis tools and defense options, including basic static and dynamic analysis, advanced static and dynamic analysis, reverse engineering and memory forensics.

7 List of Covered Topics

1. Anonymous Researching
2. Designing a Lab for Malware Analysis
3. Basic Static Analysis
4. Basic Dynamic Analysis
5. Advanced Static Analysis
6. Using IDA Pro
7. Advanced Dynamic Analysis
8. Analyzing Malicious Programs and Files
9. Malware Behavior and Network Signatures
10. Reverse Engineering
11. Packers and Unpackers
12. Memory Forensics

8 Tentative Schedule

Tentative schedules for all sections follow. Be sure to refer to the schedule for your specific section, if more than one is provided.

Tentative Schedule for **All Sections**

Date	Topic	Assignment
Aug 26	Overview of Malware and Anonymous Researching, Designing a Lab for Malware Analysis	
Sept 2	Standing Up Physical and Virtual Machines for Malware Analysis	P-Set 1
Sept 9	Basic Static Analysis	
Sept 16	Basic Dynamic Analysis	P-Set 2
Sept 23	Advanced Static Analysis, Midterm Review	
Sept 30	Using IDA Pro , Midterm Review	
Oct 7	MIDTERM EXAM	Midterm
Oct 13	NO CLASSES – SPRING BREAK	
Oct 20	Advanced Dynamic Analysis, Students Declare Semester Design Projects	
Oct 27	Analyzing Malicious Programs and Files	
Nov 3	Malware Behavior and Network Signatures	P-Set 3
Nov 10	Reverse Engineering	
Nov 17	Packers and Unpackers	
Nov 24	Memory Forensics	Draft Paper
Dec 1	Research discussions	
Dec 8	Semester Design Presentation	Semester Presentation

9 Grading Policy

Grading policy here

Letter grade scale: A(94–100), A–(90–93), B+(87–89), B(83–86), B–(78–82), C+(74–77), C(70–73), F(<70)

10 HW Assignment and Laboratory Report Submission Policy

Homework and/or reading policies

All homework should be completed and uploaded to Blackboard by the due date. Unexcused late submissions are penalized. Assigned readings should be complete before attending class. All

students should be prepared to discuss readings in details.

11 Attendance Policy

Attendance is mandatory for the Midterm exam and for the Semester Design Presentation on the final day of the course. Both Midterm and Semester Presentations will be conducted fully online. All students should sign on 15 minutes before start of class to perform audio and video/screen sharing tests.

Whenever possible, students should inform the instructor if they plan to be late or absent from class. In all cases, documentation is required to petition for *excused* absences to the Associate Dean for Student and Strategic Programs, Dr. Stephen Jones. The excused absence form is posted at: https://www1.villanova.edu/villanova/engineering/resources/undergraduates.html.

Excused absences do not count towards a failure in the course for first year students. Absence from class does not release the student from assigned work. Students who miss an in-class obligation such as an exam, a 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. In the case of illness or injury, the form must be submitted within 24 hours of missing a class. The University's list of excused absences for all students includes the following:

1. Participation in NCAA athletic competitions
2. Participation in special academic events such as: conferences, field trips, project competitions, etc., and in official university business such as student representatives attending meetings related to university governance
3. Attendance at significant events of the immediate family such as: funerals, weddings, etc.
4. Religious holidays - see the University's policy on Religious Holidays
5. College-approved participation in placement activities such as: job interviews, graduate school interviews, job fairs
6. Legally required absence such as: jury duty, court appearance, short-term military service
7. Documented serious illness or disability

12 Examination Policy

The College of Engineering has adopted the following general examination guidelines:

1. Students must arrive before the start of the examination. Under exceptional circumstances a student may need to arrive late, but he/she can enter the examination room no later than five (5) minutes after the start of the exam.
2. Cell phones must be turned off until the student exits the examination room.
3. The official Villanova class attendance policy must be followed when requesting excuses for absences or lateness to an examination.
4. Each student must write and sign the following statement, "I have neither given nor received any unauthorized assistance in the completion of this examination."
5. For online examinations, the instructor may implement video proctoring or other measures to ensure academic integrity. For consent purposes, the instructor will inform students in advance if (s)he plans to use any form of video-proctoring and whether the examination will be recorded.

13 Academic Integrity Policy

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 on the following web page:
https://www1.villanova.edu/villanova/provost/resources/student/policies/integrity.html.

14 Adherence to the Student Code of Conduct

Students are expected to act in a professional and respectful manner to their fellow students, faculty, and staff. Students should become acquainted with and understand the responsibilities set forth in the Student Handbook, especially those in the sections on Policy and Regulations. Adherence to university regulations is expected and required for successful completion of the program of studies. Enforcement within the classroom of policies regarding classroom behavior is the responsibility of the faculty member. All other discipline problems are to be referred to the Dean of Students.

15 Inclusive Classroom

This classroom is a place where you will be treated with respect; we welcome individuals of all ages, backgrounds, beliefs, ethnicities, gender, gender identities and expressions, sexual orientation, and other visible and non-visible differences. All members of this class are expected to contribute to a respectful, welcoming, and inclusive environment to allow all among us to learn and flourish.

16 Students with Disabilities

It is the policy of the university to make reasonable academic accommodations for qualified individuals with disabilities. If you are a person with a disability (non-physical) please register with the office of Learning Support Services (LSS) by emailing Learning.support.services@villanova.edu or by phoning 610-519-5176 as soon as possible. Registration is *required* in order to receive accommodations.

The Office of Disability Services (ODS) 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 at 610-519-3209 or visit the office on the second floor of the Connelly Center.

17 Tutoring Services

Villanova's tutoring services include The Writing Center, The Learner's Studio, and The Center for Speaking and Presentation. These services are offered free of charge to students. Drop in as-needed or book a regular weekly session to supercharge your academic success. Sessions can be 30 or 60 minutes in length.

Register for an account and book sessions in advance at villanova.mywconline.com. If you don't see your class listed, request a tutor for a missing subject at: tutorrequest.villanova.edu For more information, contact Juliana Struder at juliana.studer@villanova.edu or at 610-519-5862.

18 Online Expectations

Some or all sessions of this class may be recorded for educational purposes and for later playback. In order to foster a professional environment, please wear appropriate clothes and refrain from eating. If attending online, mute your microphone if you are not talking to cut down on background noise and select an appropriate setting for online class meetings. You may turn off your webcam for privacy reasons unless explicitly instructed not to do so by the instructor (such as during the conduct of online examinations).

19 Electronics Policy

The use of electronic devices, such as phones, laptops, tablets, calculators, etc., during class is generally allowed, unless their use causes a disturbance to others. During examinations, the use of any electronic device is prohibited, unless it is expressly authorized by the instructor.

Students are prohibited from making any audio or visual recordings (including taking photographs) of lectures, discussions, or other classroom activities, unless a student (1) has written permission in advance from the instructor, or (2) is permitted to record under terms and conditions as approved by the University's Office of Disability Services or Learning Support Services. Students who have received approval to record classes as an academic accommodation must provide supporting documentation from the Office of Disability Services or Learning Support Services in advance of any recording. Students may use authorized recordings only for the purposes of individual study in the course, and may not disseminate or share them with a wider audience without explicit permission.

20 Copyright Policy

The materials used in Villanova University courses ("Course Materials") generally represent the intellectual property of course instructors, third parties and/or the university which may not be disseminated or reproduced in any form for public distribution (e.g., sale, exchange, etc.) without the written permission of the course instructor. Course materials include all written or electronic documents and materials, including syllabi, current and past examination questions/answers, and presentations such as lectures, videos, slides, etc., provided by a course instructor. Course materials may only be used by students enrolled in the course for academic (course-related) purposes.

Published course readings (book chapters, articles, reports, etc.) available in "Blackboard" are copyrighted materials. These works are made available to students through licensed databases or fair use. They are protected by copyright law, and may not be further disseminated or reproduced in any form for distribution (e.g. uploading to websites, sale, exchange, etc.) without the permission of the copyright owner.

Follow these links for more information on Intellectual Property, Copyright, and Computer Acceptable Use.

21 Professorial Duties

It is important to note that teaching is one of the many duties that professors perform as part of their job responsibilities. In addition to teaching, professors perform research, advise graduate

students, edit journals and review journal articles, serve on committees for the university and professional societies, travel to conferences to remain abreast of current developments and to present their results... to name just a few commitments.