EEL 4804
Introduction to Malware & Reverse Engineering

Department of Electrical & Computer Engineering
Florida International University
Fall 2018

Classroom	**:**	EC 1104
Class Time	**:**	8:00 am—12:30 pm
Faculty	**:**	Dr. Alexander Pons
Office Hours	**:**	T & R 10:00-12:00 am or by Appointment
Office	**:**	EC – 3145
Phone	**:**	305.348.7253
Email	**:**	apons@fiu.edu
Prerequisite	**:**	Basic knowledge about computer and windows operating system or Successful completion of a Programming language course Or permission from the instructor

Textbook

- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Adrew Honig (Feb, 2012), ISBN: 1593272901
- The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle (Jul, 2011), ISBN: 1593272898

Course Description

The objective of this course is to familiarize students with the practice of performing reverse engineering on suspicious files and firmware by utilizing static and dynamic techniques and procedures. The student will gain an understanding of how firmware is compromised and how to validate and restore its integrity. Analytical information such as environment changes (file, system, network, and process), communication with the rest of the network and the malware's impact on mobile devices will be closely observed and analyzed for actionable information.

Course Objectives

1. To give the student an understanding of Malware Reverse Engineering approaches.
2. To give the students a hands-on exposure to the latest tools and techniques to find, extract, and analyze malicious code from various types of hardware.
3. To provide analysis on the way the malware interacts with any associated networks, identifying the type of information being targeted.

Topics Covered

1. Ethical Issues in Security
2. Sandboxing executable and extracting information by performing runtime analysis.
3. Static /dynamic analysis of malware.
4. Packers, Compression and Obfuscation techniques
5. Analysis malware using IDA Pro Disassembler
6. Analyzing malicious browser based exploits.

Relationship of course to program objectives

In this course, the student will have to show:

1. An ability to apply knowledge of mathematics, science, and engineering,
2. an ability to design and conduct experiments, as well as to analyze and interpret data,
3. an ability to design a system, component, or process to meet desired needs within realistic constraints such as economic, environmental, social, political, ethical, health and safety, manufacturability, and sustainability,
4. an ability to identify, formulate, and solve engineering problems (homework),
5. the broad education necessary to understand the impact of engineering solutions in a global, economic, environmental, and societal context
6. an ability to communicate effectively (through teamwork),
7. an ability to use the techniques, skills, and modern engineering tools necessary for engineering practice,
8. a knowledge of contemporary issues,
9. a knowledge of advanced mathematics.

Tentative Grading Scale

Grading Scale:		
A	**95-100**	**"Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook."**
A-	**90-94**	
B+	**86-89**	
B	**82-85**	
B-	**78-81**	
C+	**74-77**	
C	**70-73**	
D	**60-69**	
F	**< 59**	

Grading Scheme

Quizzes	**10%**
Group Project	**15%**
Classwork and Homework	**15%**
Midterm Exam	**30%**
Final Exam	**30%**
Total	**100%**

Group Project

1. A group of maximum 3 students per group.
2. Develop a functioning malware for Windows or Linux that demonstrates its activity. You must state the ground truth of the malware and demonstrate its adherence to it.
3. The group must submit a working malware, a description of the malware's behavior and actions and a short video showing (10-15 mins) how the malware performs its activity.

University's Code of Academic Integrity

Florida International University is a community dedicated to generating and imparting knowledge through excellent teaching and research, the rigorous and respectful exchange of ideas, and community service. All students should respect the right of others to have an equitable opportunity to learn and honestly to demonstrate the quality of their learning. Therefore, all students are expected to adhere to a standard of academic conduct, which demonstrates respect for themselves, their fellow students, and the educational Mission of the University. All students are deemed by the University to understand that if they are found responsible for academic misconduct, they will be subject to the Academic Misconduct procedures and sanctions, as outlined in the Student Handbook.
More information can be found at http://academic.fiu.edu/academic_misconduct.html

Department Regulations Concerning Incomplete Grades

To qualify for an Incomplete, a student:

1. Must contact (e.g., phone, email, etc.) the instructor or secretary before or during missed portion of class.
2. Must be passing the course prior to that part of the course that is not completed
3. Must make up the incomplete work through the instructor of the course
4. Must see Instructor. All missed work must be finished before last two weeks of the next term

University policies on sexual harassment, and religious holidays, and information on services for students with disabilities
Please visit the following websites: http://academic.fiu.edu/ and http://drc.fiu.edu

Course Policies

- **Attendance:** Attendance in the course is **mandatory** and student is not allowed to miss any class during the semester. There will be a **penalty** for missing classes and it may affect your final grade.
- **Academic Misconduct:** For work submitted, it is expected that each student will submit their own original work. Any evidence of duplication, cheating or plagiarism will result at least a failing grade for the course.
- **Unexcused Absences:** Two unexcused absences are permitted during the term. More than two will result in the loss of points from your final grade. (1 point per absence above two, 3 points per absence above 5).
- **Excused Absences:** Only emergency medical situations or extenuating circumstances are excused with proper documentation. After reviewing documentation you are required to email a description of the excuse and absence dates as a written record to apons@fiu.edu.
- **On Time:** As in the workplace, on time arrival and preparation are required. Two "lates" are equivalent to one absence. (Leaving class early is counted the same as tardy.)
- **Deadlines:** Assignments are due at the beginning of the class period on the date specified. Assignments submitted late (within 1 week) will receive half credit.
- To get assistance try to see me by an appointment.
- Students are encouraged to ask questions and to discuss course topics with the instructor and with each other.
- **Any work submitted should display Panther ID number and should be signed, as the students' own work, and that no unauthorized help was obtained.**
- Cell phones, communicators, MP3 players, head sets are not allowed to be used in the class.
- **DO NOT** send assignments by email.
- Instructor reserves right to change course materials or dates as necessary.

Exam policy

1. Make sure to complete the assigned homework in order to do well in the exam.
2. All exams are closed book and closed notes.
3. Use of any electronic device with keyboard is prohibited. This also applies to cellphones with messaging system.
4. No discussion is permitted during the exams.
5. Instructor is not compelled to give credit for something he cannot read or follow logically.
6. Cheating is considered as a serious offense. Students who are caught will receive the appropriate consequences.

Class Schedule

Once a week, 240 minutes each session: Wednesday

Class Schedule:

Week	Date	Weekly Topic
1	10/15 (10/17)	Chapter 0 - Malware Analysis Primer Chapter 1: Basic Static Techniques How to access VM for labs
2	10/22 (10/24)	Chapter 2: Malware Analysis in Virtual Machines Chapter 3: Basic Dynamic Analysis Proposed Group Project (Malware) Complete in Class Lab1a Quiz 1 (Chapter 0 and 1)
3	10/29 (10/31)	Chapter 4: A Crash Course in x86 Disassembly Chapter 5: IDA Pro Submit out of Class Lab1b Complete in Class Lab2a Quiz 2 (Chapters 2 and 3)
4	11/5 (11/7)	**Midterm** Chapter 6: Recognizing C Code Constructs in Assembly Quiz 3 (Chapters 4 and 5) taken before class Submit out of Class Lab2b
5	11/12 (11/14)	Chapter 7: Analysing Malicious Windows Programs Chapter 8: Debugging Submit out of Class Lab 3a and Lab3b Complete in Class Lab4a Project – Ground Truth Quiz 4 (chapter 6)
6	11/19 (11/21)	Chapter 9: OllDbg Chapter 11: Malware Behaviour Submit out of Class Lab4b Complete in Class Lab5a Quiz 5 (Chapter 7 and 8)
7	11/26 (11/28)	Chapter 12: Covert malware Lunching Submit out of Class Lab5b Complete in Class Lab6a Quiz 6 (chapter 9 and 11)
8	12/3 (12/5)	**Final Exam** Group Presentation Quiz 7 (Chapter 12) taken before class Submit out of Class Lab6b
	12/5	**Group Project is due**