Jordan University of Science and Technology

Faculty of Computer & Information Technology

Network Engineering And Security Department

NES552 Reverse Engineering And Malware Analysis - JNQF Level: 7

First Semester 2023-2024

Course Catalog
3 Credit Hours. This course introduces the essential concepts, tools, and techniques for understanding, analyzing, and investigating binary programs, in general, and malicious programs, in specific. It begins with easy methods that can be used to get information from relatively unsophisticated programs, and proceeds with increasingly complicated techniques that can be used to tackle even the most sophisticated malicious programs. Particular topics include static analysis techniques, dynamic analysis, assembly language and disassembly, recognizing C code constructs in assembly, debugging, and obfuscation techniques.

Instructor	
Name	**Dr. Monther Al dwairi**
Office Location	M2L2
Office Hours	Sun : 08:30 - 09:30 Sun : 12:15 - 13:15 Mon : 11:30 - 13:30 Tue : 13:30 - 14:30 Wed : 11:30 - 12:30
Email	munzer@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Sun, Tue : 09:30 - 10:30 Room: M5126

Prerequisites		
Line Number	**Course Name**	**Prerequisite Type**
1754530	NES453 Network Security	Prerequisite / Study
1713512	CPE351 Microprocessor Systems	Prerequisite / Study
1714730	CPE473 Operating Systems	Prerequisite / Study

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Week 1	Introduction	
Weeks 2, 3	A Crash Course in x86 Assembly	
Weeks 4, 5, 6	Recognizing C Code Constructs in Assembly	
Week 7	Analyzing Malicious Windows Programs	
Week 8	Debugging	
Weeks 9, 10	Covert Malware Launching	
Weeks 11, 12	Data Encoding	
Weeks 13, 14	Malware-Focused Network Signatures	
Week 15	Packers and Unpacking	

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Learn and apply basic and advanced static analysis techniques [1SO1] [1L7S1]	40%	First Exam, Second Exam, Final Exam, Assignments and Projects
Learn and apply basic and advanced dynamic analysis techniques [1SO1] [1L7S1]	30%	First Exam, Second Exam, Final Exam, Assignments and Projects
Learn how to recognize and defeat the techniques of anti-disassembly, anti-debugging, anti-virtual machine analysis, and packing [1SO1] [1L7S3]	30%	Second Exam, Final Exam, Assignments and Projects

Relationship to Program Student Outcomes (Out of 100%)						
SO1	SO2	SO3	SO4	SO5	SO6	SO7
100						

Relationship to NQF Outcomes (Out of 100%)	
L7S1	L7S3
70	30

Evaluation	
Assessment Tool	**Weight**
First Exam	10%
Second Exam	10%

Final Exam	40%
Assignments and Projects	40%

Policy	
Essential Notes (Exams)	? May include: Definitions, True/False, Multiple-Choice, Analysis and Descriptive formats. ? Use only your own tools: calculator, pens and ruler ? Instructions on the first page of the exam are quite important. ? Not abiding by the rules is a reason for dismissal from the exam. ? Graded exam papers will be returned within a week.
Additional Notes	Makeups ? Makeup exam should not be given unless there is a valid excuse. Drop Date ? Last day to drop the course is before the 12th week of the current semester. Cheating ? Standard JUST policy will be applied. Attendance ? Excellent attendance is expected. ? According to the JUST policy, a student will receive the grade of ZERO (35%) ?failed for absence? if he misses more than 20% of the classes. ? Attendance will be taken by calling the names or passing a sign-up sheet. ? If you miss a class, it is your responsibility to find out about any announcements or assignments you may have missed. Workload ? Average workload student should expect to spend 8 hours/week. Participation ? Participation in the class will positively affect your performance. ? Disruption and side talks will possibly result in dismissal from class. ? No eating or chewing gums are allowed in class.

Date Printed: 2024-02-04