

CCY4305 Advanced Malware Analysis and Reverse Engineering**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY3102	4	7/8	2	--	2	3

COURSE AIM

To get the students to:

- Understand different attack methods used by malicious actors and how they map to attack frameworks
- Learn how malware authors dynamically construct import tables for function calls
- Gain a deeper understanding of binary file formats and how to analyze them to learn more about malware behavior (Portable Executable- PE file format)
- Leverage static and dynamic tools to develop a hybrid approach for effectively analyzing malware including assembly level debuggers, disassemblers, decompilers and sandboxes.
- Learn how to interact in crucial dialogue around critical software program protection and forensics.

COURSE WEEKLY CONTENTS

- 1 Course Aim, Course outline, understanding what is reverse engineering Malware and Malware Analysis
- 2 Static Analysis
- 3 Dynamic Analysis
- 4 Assembly Language and Disassembly Primer
- 5 Disassembly Using IDA
- 6 Debugging Malicious Binaries.
- 7 Malware Functionalities and Persistence.
- 8 7th week Assessment
- 9 Reversing malware that uses Autolt ransomware,
- 10 Code Injection and Hooking
- 11 Malware Obfuscation Techniques
- 12 12th week Assessment
- 13 Hunting Malware Using Memory Forensics
- 14 Detecting Advanced Malware Using Memory Forensics
- 15 Exploring posted studies papers related to malware behavior analysis.

STUDENT GRADING & ASSESSMENT

Weeks	Exams	Assign.	Quizzes	Reports	Present.	Lab.	Total
1 to 7	←		30	MARKS		→	30
8 to 12	←		20	MARKS		→	20
1 to 15	←		10	MARKS		→	10
16 or 17			Final Exam				40

REFERENCES

Textbook	Monnappa K A, Learning Malware Analysis: Explore the Concepts, Tools, and Techniques to Analyze and Investigate Windows Malware, Packet Publisher
-----------------	---