

CCY3102 Malware Analysis and Reverse Engineering**COURSE INFORMATION**

Prerequisites	Academic Year & Level		Teaching Methods			Credit Hrs.
	Year	Semester	Lecture	Tutorial	Laboratory	
CCY2001 and CCS2103	3	6	2	--	2	3

COURSE AIM

To get the students to:

- Develop a good understanding of Malware Analysis
- Use various static and dynamic malware analysis tools
- Learn skills used to analyze and stop breaches to networks.
- Use a Malware Analysis-based approach in order to resolve real world problems.
- Explore the different techniques of reverse engineering principles.

COURSE WEEKLY CONTENTS

- 1 Course Aim, Course outline, malware identification and Malware types and behaviors.
- 2 Malware Components and Analysis, and Reverse Engineering and assembly
- 3 Malware Analysis and Classification including Different techniques of binary files, including static analysis and decomposition analysis
- 4 Automated techniques for dynamic and static analysis.
- 5 Ethical considerations, Senior Managers How to Write a Good Report,
- 6 Conducting a reverse engineering analysis.
- 7 7th week Assessment
- 8 Obfuscation schemes.
- 9 Analyzing hostile malware
- 10 How to build signatures to stop malware.
- 11 12th week Assessment
- 12 How to use artificial intelligence and machine learning in malware analysis
- 13 Reverse engineering tools which demonstrate anti-analysis techniques
- 14 Malware obfuscation, and packaging techniques
- 15 revision

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	Abhijit Mohanta and Anoop Saldanha, Malware Analysis and Detection Engineering: A Comprehensive Approach to Detect and Analyze Modern Malware, Apress
-----------------	---