COURSE CONTENT

MALWARE ANALYSIS AND REVERSE ENGINEERING								
II Semester: CSE								
Course Code	**Category**	**Hours / Week**			**Credits**	**Maximum Marks**		
BCSE27	**Elective**	**L**	**T**	**P**	**C**	**CIA**	**SEE**	**Total**
		3	0	0	3	40	60	100
Contact Classes:45	**Total Tutorials: Nil**	**Total Practical Classes: Nil**				**Total Classes: 45**		
Prerequisites: Computer Networks, Information security								

I. COURSE OVERVIEW:

This course typically aims to provide students or participants with a comprehensive understanding of malicious software, how it operates, and techniques to analyze and reverse engineer it.

II. COURSE OBJECTIVES:

The students will try to learn:

I The fundamentals of malware analysis
II The malware taxonomy and malware analysis tools.
III The malware samples using static, dynamic analysis, and reverse engineering techniques.

III. COURSE OUTCOMES:

After successful completion of the course, students should be able to

CO1 apply the skills to carry out static and dynamic malware analysis on various malware samples.
CO2 Comprehend reverse-engineering of malware analysis techniques.
CO 3 Apply techniques and concepts to unpack, extract, and decrypt malware
CO 4 Summarize the executable formats, Windows internals, and APIs and conduct malware forensics
CO 5 Apply reverse engineering to dissect malware, understand its code, and reconstruct its logic to comprehend how it works

IV. COURSE CONTENT:

MODULE-I: MALWARE TAXONOMY (9)

Malware taxonomy - Malware analysis techniques – Packed and Obfuscated Malware -Portable Executable File Format: Headers and Sections, Malware Analysis in Virtual Machines - Malware Analysis Tools: ProcMon/ ProcExplore, BinText, FileAlyzer, OllyDbg.

MODULE-II: MALWARE FORENSICS (9)

Using TSK for Network and Host Discoveries, Using Microsoft Offline API to Registry Discoveries, Identifying Packers using PEiD, Registry Forensics with Reg Ripper Plu-gins: Bypassing Poison Ivy's Locked Files, Bypassing Conficker's File System ACL Restrictions, Detecting Rogue PKI Certificates.

MODULE-III: STATIC ANALYSIS (9)

File signature analysis and Identifying file dependencies -Database of file hashes. String analysis - Local and online malware sandboxing - Levels of Abstraction - x86 Architecture -x86/x86_64 Assembly - Static Analysis Tools: PeiD, Dependency Walker, Resource Hacker.

MODULE-IV: DYNAMIC ANALYSIS (9)

Source level vs. Assembly level Debuggers - Kernel vs. User-Mode Debugging –Exceptions - Modifying Execution with a Debugger - Modifying Program Execution in Practice - DLL analysis - Dynamic Analysis Tools: Virustotal, Malware Sandbox, Windows Sysinternals

MODULE-V: REVERSE ENGINEERING (9)

Reverse engineering malicious code - Identifying malware passwords – Bypassing authentication - Advanced malware analysis: Virus, Trojan and APK Analysis – Reverse Engineering Tools: IDA Pro and OLLYDBG.

V TEXT BOOKS:

1. Abhijit Mohanta, Anoop Saldanha, "Malware Analysis and Detection Engineering a Comprehensive Approach to Detect and Analyze Modern Malware", Apress publications, 1st edition, 2020,

VI. REFERENCE BOOKS:

1. Michael Sikorski, Andrew Honig "Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software" publisher Williampollock.
2. Monnappa K A, Learning Malware Analysis- Explore the concepts, tools, and techniques to analyze and investigate Windows malware, 2018, 1st edition, Packt Publishing,

VII. WEB REFERENCES:

1. https://github.com/CyberSecurityUP/Awesome-Malware-and-Reverse-Engineering
2. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/malware-reverse-engineering/
3. https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/malware-reverse-engineering/

VIII. E-TEXTBOOKS:

1. https://ccdcoe.org/uploads/2020/07/Malware_Reverse_Engineering_Handbook.pdf
2. https://doc.lagout.org/security/Malware%20%26%20Forensics/Practical%20Malware%20Analysis.pdf
3. https://www.foo.be/cours/dess-20122013/b/Eldad_Eilam-Reversing__Secrets_of_Reverse_Engineering-Wiley(2005).pdf

VIII. MATERIALS ONLINE:

1. Course Outline Description
2. Tutorial question bank
3. Tech talk topics
4. Open-ended experiments
5. Definitions and terminology
6. Assignments
7. Model question paper – I
8. Model question paper – II
9. Lecture notes
10. PowerPoint presentation
11. E-Learning Readiness Videos (ELRV)