GANPAT UNIVERSITY									
FACULTY OF ENGINEERING AND TECHNOLOGY									
Programme	Bachelor of Technology					Branch/ Spec.	Computer Science & Engineering (CS)		
Semester	VII					Version	1.0.0.1		
Effective from Academic Year			2022-23			Effective for the batch Admitted in			June 2019
Subject code	2CSE713		Subject Name			MALWARE ANALYSIS			
Teaching scheme						Examination scheme (Marks)			
(Per week)	Lecture (DT)		Practical (Lab.)		Total		CE	SEE	Total
	L	TU	P	TW					
Credit	0	0	2	0	2	Theory	-	-	-
Hours	0	0	4	0	4	Practical	60	40	100

Pre-requisites:

Basic Understanding of Windows and Linux operating systems, Malware and Networking, Web and OS security attacks, High Level & Low Level Programming.

Objectives of the Course:

After learning the course the students will be able to:

- Learn to analyze various malicious file types
- Learn to build and utilize a sandbox environment for malware analysis
- Apply various tools to Identify the vulnerabilities and to perform Malware analysis
- Apply malware classification and functionality & anti-reverse engineering techniques

Theory syllabus

Unit	Content
1	**Malware Analysis Fundamentals:** Assembling a toolkit for effective malware analysis, examining static properties of suspicious programs, performing behavioral analysis of malicious Windows executable, performing static and dynamic code analysis of malicious Windows executables, interacting with malware in a lab to derive additional behavioral characteristics.
2	**Malicious Web and Document Files:** Interacting with malicious websites to assess the nature of their threats, Deobfuscating malicious JavaScript using debuggers and interpreters, analyzing suspicious PDF files, examining malicious Microsoft Office documents, including files with macros, Analyzing malicious RTF document files
3	**Reversing Malicious Code:** Understanding core x86 assembly concepts to perform malicious code analysis, Identifying key assembly logic structures with a disassembler, following program control flow to understand decision points during execution, recognizing common malware characteristics at the Windows API level (registry manipulation, key logging, HTTP communications, droppers), Extending assembly knowledge to include x64 code analysis
4	**In-Depth Malware Analysis:** Recognizing packed malware, Getting started with unpacking, using debuggers for dumping packed malware from memory, analyzing multi-technology and file-less malware, Code injection and API hooking, Using memory forensics for malware analysis
5	**Examining Self-Defending Malware:** How malware detects debuggers and protects embedded data, unpacking malicious software that employs process hollowing, Bypassing the attempts by malware to detect and evade the analysis toolkit, Handling code misdirection techniques, including SEH and TLS Callbacks, unpacking malicious executable by anticipating the packer's actions

Text Books:

1.	Practical Malware Analysis The Hands-on guide to Dissecting Malicious Software
Reference Books:	
1.	Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley
2.	Dang, Gazet and Bachaalany, “Practical Reverse Engineering”,Wiley
3.	Reverend Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” Second Edition,Jones& Bartlett
Course Outcomes:	
COs	Description
CO1	Learn to analyze various malicious file types
CO2	Learn to build and utilize a sandbox environment for malware analysis
CO3	Apply various tools to Identify the vulnerabilities and to perform Malware analysis
CO4	Apply malware classification and functionality & anti-reverse engineering techniques

Mapping of CO and PO:

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	2	2	0	2	0	3	0	0	2	2
CO2	2	3	1	2	3	2	0	3	2	0	2	3
CO3	3	2	2	0	2	2	0	3	0	0	2	3
CO4	3	1	2	0	2	2	0	3	2	0	2	2