Faculty of Engineering & Technology
Master of Technology (M. Tech)
(W. E. F.: 2023-24)

Document ID: SUTEFETM-01

Name of Faculty	:	Faculty of Engineering & Technology
Name of Program	:	Master of Technology (M.Tech.) – Cyber Security
Course Code	:	2MCS02
Course Title	:	Malware Analysis & Network Security
Type of Course	:	Cyber Security
Year of Introduction	:	2023-24

Prerequisite	:	Basic knowledge of Computer Networks and various types of attacks
Course Objective	:	Gain expertise in malware analysis, including static and dynamic analysis, executable formats, Windows internals, and advanced anti-analysis techniques, while understanding the broader social and historical aspects of malware.
Course Outcomes	:	At the end of this course, students will be able to:
	CO1	Students with a specialist understanding of the nature of malware, its capabilities, and how it is combated through detection and classification
	CO2	Students will be able to apply the tools and methodologies used to perform static and dynamic analysis on unknown executables.
	CO3	Students will have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
	CO4	Students will able to apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples
	CO5	Furthermore, students would have a broad understanding of the social, economic, and historical context in which malware occurs

Teaching and Examination Scheme

Teaching Scheme (Contact Hours)			Credits	Examination Marks				
				Theory Marks		Practical Marks		Total Marks
L	**T**	**P**	**C**	**SEE**	**CIA**	**SEE**	**CIA**	
4	0	2	5	70	30	30	20	150

Legends: ***L****-Lecture;* ***T****–Tutorial/Teacher Guided Theory Practice;* ***P*** *– Practical,* ***C*** *– Credit,* ***SEE*** *– Semester End Examination,* ***CIA*** *- Continuous Internal Assessment (It consists ofAssignments/Seminars/Presentations/MCQ Tests, etc.))*

Course Content

Unit No.	Topics	Teaching Hours	Weightage	Mapping with CO
1	**INTRODUCTION:** Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis.	06	10%	CO1
2	**DYNAMIC ANALYSIS:** Live malware analysis, dead malware analysis, analyzing traces of malware-system-calls, api-calls, registries, network activities. Anti-dynamic analysis techniquesanti-vm, runtime- evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching	15	25%	CO2
3	**DYNAMIC ANALYSIS:** Live malware analysis, dead malware analysis, analyzing traces of malware-system-calls, api-calls, registries, network activities. Anti-dynamic analysis techniquesanti-vm, runtime- evasion techniques, , Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching	15	25%	CO3
4	**Malware Functionality:** Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching-Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection	06	15%	CO4
5	**Malware Detection Techniques**: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware	08	20%	CO5

	signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences.			
6	**Android Malware:** Malware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	10	20%	CO5

Suggested Distribution of Theory Marks Using Bloom's Taxonomy						
Level	Remembrance	Understanding	Application	Analyse	Evaluate	Create
Weightage	**20**	**30**	**30**	**20**	**0**	**0**

NOTE: This specification table shall be treated as a general guideline for the students and the teachers. The actual distribution of marks in the question paper may vary slightly from above table.

Suggested List of Experiments/Tutorials

Sr. No.	Name of Experiment/Tutorial	Teaching Hours
1	Set up a safe virtual environment to analyse malware	04
2	Quickly extract network signatures and host-based indicators	04
3	Use key analysis tools like IDA Pro, OllyDbg, and WinDbg.	02
4	Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques	04
5	Use your newfound knowledge of Windows internals for malware analysis	04
6	Develop a methodology for unpacking malware and get practical experience with five of the most popular packers	04
7	Analyze special cases of malware with shellcode, C++, and 64-bit code	04
8	Install Reanimator in your Windows machine and scan the system for Malware and prepare one report for the same.	04

Major Equipment/ Instruments and Software Required

Sr. No.	Name of Major Equipment/ Instruments and Software
1	IDA Pro,
2	OllyDbg,.
3	WinDbg.
4	Turbo C++
5	VMWare

Suggested Learning Websites

Sr. No.	Name of Website
1	https://www.geeksforgeeks.org/introduction-to-malware-analysis
2	https://intezer.com/blog/malware-analysis/the-role-of-malware-analysis-in

Reference Books

Sr. No.	Name of Reference Books
1	Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10
2	Computer viruses: from theory to applications by Filiol, Eric Springer Science &Business Media
3	Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0,
4	Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill