MALWARE ANALYSIS & REVERSE ENGINEERING

Subject Code: CS34322CS	Subject Type: Elective
Evaluation Scheme: MSE(30), TA(20), ESE(50)	L-T-P: 3-0-0

Pre-Requisites: Computer Networks, Operating System, Programming Skills, Computer Architecture.

Course Objective: To understand the fundamentals of reverse engineering and malware analysis techniques. Additionally, this study aims to analyze and detect malware behavior, evasion techniques, and appropriate countermeasures.

Course Outcomes: At the end of the course, the student will be able to

CO-1	Understand reverse engineering principles and malware classification
CO-2	Perform static analysis of executable files and identify suspicious behavior
CO-3	Apply dynamic analysis techniques using debugging and monitoring tools
CO-4	Analyze malware techniques such as persistence, obfuscation, and evasion
CO-5	Design detection and mitigation strategies for modern malware attacks

Course Articulation Matrix:

CO/PO	PO-1	PO-2	PO-3	PO-4	PO-5	PO-6
CO-1	3	3	3	2	3	2
CO-2	3	2	3	-	3	3
CO-3	3	3	3	1	3	3
CO-4	3	3	3	-	3	2
CO-5	3	3	3	1	3	1

1 - Slightly; 2 - Moderately; 3 – Substantially

Syllabus:

Unit-1: Foundations of Malware Analysis

Introduction to Malware and Reverse Engineering, Malware types: Virus, Worm, Trojan, Ransomware, Rootkits, Reverse Engineering methodology and workflow, Static vs Dynamic analysis concepts, Malware analysis lab setup (VMs, sandboxing), Overview of tools (strings, PE tools, debuggers, disassemblers)

Unit-2: Static Analysis & PE Structure

Portable Executable (PE) file format. Static analysis techniques (strings, signatures, hashing), Disassembly and decompilation basics, Assembly language fundamentals (x86 architecture), Packers and obfuscation techniques, Signature-based detection (YARA rules, antivirus signatures)

Unit-3: Dynamic Analysis & Debugging

Dynamic malware analysis (behavioral analysis), Debugging tools (OllyDbg, x64dbg, GDB), API monitoring and system call tracing, Memory analysis and process injection techniques, Network analysis (packet capture, C2 communication), Anti-debugging and anti-analysis techniques

Unit-4: Advanced Malware Persistence Techniques & Case Studies

Malware persistence mechanisms (registry, services, DLL injection), Privilege escalation techniques, Rootkits and kernel-level malware concepts, Malware evasion and anti-forensics, Malware detection and mitigation strategies, Case studies and real-world malware analysis

Learning Resources:

Text and Reference Books:

1. Eilam, Eldad. Reversing: secrets of reverse engineering. John Wiley & Sons, 2011.
2. Botwright, Rob. Malware Analysis: Digital Forensics, Cybersecurity, And Incident Response. Rob Botwright, 2023.
3. The Ghidra Reverse Engineering Black Book – Boris Larin, 2019.
4. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software – Michael Sikorski & Andrew Honig, 2012.
5. Mohanta, Abhijit, and Anoop Saldanha. Malware analysis and detection engineering: a comprehensive approach to detect and analyze modern malware. New York, NY, USA: Apress, 2020.