COURSE TITLE	**MALWARE ANALYSIS AND REVERSE ENGINEERING**
COURSE CODE	**01CC0609**
COURSE CREDITS	**3**

Objective:

1 Students will be able to apply concepts of malware, its types, and static and dynamic analysis techniques, analyze malicious code behavior using reverse engineering tools such as IDA and OllyDbg along with debugging methodologies, and evaluate advanced malware techniques, document-based threats, and emerging cyber threats in modern computing environments.

Course Outcomes: After completion of this course, student will be able to:

1 Apply static and dynamic malware analysis techniques to identify and understand the behavior of malicious software in controlled environments

2 Utilize reverse engineering tools and debugging techniques to investigate and interpret malicious code and its execution flow.

3 Analyze assembly-level instructions, system calls, and execution patterns to determine the functionality and impact of malware.

4 Evaluate suspicious files, malicious documents, and attack patterns to assess threats and determine appropriate mitigation strategies.

5 Design and develop systematic approaches or tools for effective malware detection, analysis, and response.

Pre-requisite of course: Understanding of Operating Systems. Basic Computer Literacy. Programming Languages.

Teaching and Examination Scheme

Theory Hours	Tutorial Hours	Practical Hours	ESE	IA	CSE	Viva	Term Work
2	0	2	50	30	20	25	25

Contents : Unit	Topics	Contact Hours
1	**Introduction to Malware and Reverse Engineering** Introduction to Malware, Basics of Malware, Types of Malware, Basics of Static Analysis, Basics of Dynamic Analysis, Basic Analysis Methodology, Automated Malware Analysis, Introduction to Reverse Engineering: Basic of Reverse Engineering, Machine Code, Assembly Language: Assembly Basics, Registers, Operands, Instruction, Arithmetic Instructions, System and Code Level Reversing, Legality of Reverse Engineering, Reversing Tools, IDA, Debugging Concepts, Stepping, Breakpoints and Exceptions, Modifying Execution, Ollydbg	6

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Contents : Unit	Topics	Contact Hours
2	**Fundamentals of Malware Analysis &Reversing Malicious Code** Fundamentals of Malware Analysis: Creating a Toolkit for Effective Malware Analysis, Investigating Static Properties of Suspicious Programs, Conducting Behavioral Analysis and Dynamic Code Analysis of Malicious Windows Executables, Reversing Malicious Code: Understanding Core x86 Assembly Concepts for Malicious Code Analysis, Identifying Key Assembly Logic Structures Using a Disassembler, Following Program Control Flow to Analyze Decision Points During Execution, Recognizing Common Malware Characteristics at the Windows API Level (Registry Manipulation, Keylogging, HTTP Communications, Droppers), Extending Assembly Knowledge to Include x64 Code Analysis	8
3	**In-Depth Malware Analysis** Identifying Packed Malware and Initiating Unpacking Procedures, Utilizing Debuggers to Extract Packed Malware from Memory, Analyzing Obfuscated PowerShell Scripts, Examining Multi-Technology and Fileless Malware, Exploring Code Injection and API Hooking Techniques, Leveraging Memory Forensics for Malware Analysis, Implementing Malware Sandboxing for Testing and Analysis	6
4	**Malicious Web and Document Files** Studying Malicious Websites to Evaluate Threats, De obfuscating Malicious JavaScript Code, Analyzing Suspicious PDF Files, RTF Document Files, and Microsoft Office Documents	6
5	**Advanced Malware Analysis and Emerging Threats** Advanced Disassembly and Decompilation, Advanced Debugging Techniques, Network Traffic Analysis, Anti-Analysis Techniques and Countermeasures, Rootkit Analysis, Mobile Malware Analysis, Emerging Threats and Future Trends	6
Total Hours		**32**

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
1	**Practical 1** Set up a secure virtual lab environment for malware analysis using VirtualBox and FLARE VM. Configure network isolation and snapshots to ensure safe execution and analysis of suspicious files.	2
2	**Practical 2** Study destructive malware behaviors such as file deletion in a controlled environment. Analyze their impact on system resources and understand preventive and recovery mechanisms.	2
3	**Practical 3** Simulate worm-like behavior using safe scripts and analyze file/folder propagation patterns. Observe how such behavior spreads within a system and evaluate methods to contain it.	2

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)

Suggested List of Experiments:

Contents : Unit	Topics	Contact Hours
4	**Practical 4** Study USB-based attack vectors (e.g., shortcut attacks) and implement detection and prevention techniques. Understand how removable media can be exploited and how security policies can mitigate such risks.	2
5	**Practical 5** Perform memory forensics and malware analysis using Volatility. Extract and analyze running processes, network connections, and hidden artifacts from memory dumps.	2
6	**Practical 6** Study human interface device (HID) attack concepts (e.g., Rubber Ducky) and explore defense mechanisms. Understand how such attacks simulate user input and how systems can be protected against them.	2
7	**Practical 7** Analyze techniques used to conceal malicious code (e.g., steganography) within files such as images. Evaluate methods to detect hidden data and understand their implications in cybersecurity.	2
8	**Practical 8** Study keystroke logging concepts and implement detection and mitigation techniques. Understand how sensitive data can be captured and how security tools can prevent such threats.	2
9	**Practical 9** Install and explore Android emulation using Genymotion to understand its working mechanism. Analyze how emulators can be used for application testing and mobile security analysis.	2
10	**Practical 10** Perform malware analysis and reverse engineering using radare2. Understand binary analysis techniques to identify program behavior and potential security risks.	2
Total Hours		**20**

Textbook :

1 Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware, Monnappa K A, Packt Publishing, 2018

References:

1 Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, Michael Sikorski, No Starch Press, 2012

2 “Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, “Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code, Michael Hale Ligh, Matthew Richard, Blake Hartstein, Steven Adair, Wiley Publishing, Inc., 2010

References:

3 Reversing: Secrets of Reverse Engineering, Reversing: Secrets of Reverse Engineering, Eldad Eilam, Wiley Publishing, Inc., 2005

4 Reverse Engineering for Beginners, Reverse Engineering for Beginners, Dennis Yurichev, Self-Published, 2014

Suggested Theory Distribution:

The suggested theory distribution as per Bloom's taxonomy is as follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

Distribution of Theory for course delivery					
Remember / Knowledge	**Understand**	**Apply**	**Analyze**	**Evaluate**	**Higher order Thinking / Creative**
0.00	2.00	30.00	30.00	18.00	20.00

Instructional Method:

1 The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.

2 The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory or class-room.

Supplementary Resources:

1 https://www.nostarch.com/malware

2 https://malwareunicorn.org/workshops/re101.html

3 https://github.com/volatilityfoundation

4 https://remnux.org/

DR. MUNINDRA HASMUKHBHAI LUNAGARIA
Digitally signed by (Name of HOD)

DR. RAJENDRASINH BAHADURSINH JADEJA
Digitally signed by (Name of Dean/ Principal)