| BCSE321L | MALWARE ANALYSIS | L | T | P | C |
|---|---|---|---|---|---|
| | | 2 | 0 | 0 | 2 |
| **Pre-requisite** | **NIL** | **Syllabus version** | | | |
| | | 1.0 | | | |

**Course Objectives**

1. To introduce the malware taxonomy and malware analysis tools.
2. To identify and analyze malware samples using static, dynamic analysis, and reverse engineering techniques.
3. To detect and analyze malicious documents and mobile malware.

**Course Outcome**

After completion of this course, the student shall be able to:

1. Possess the skills to carry out static and dynamic malware analysis on various malware samples.
2. Understand the executable formats, Windows internals, and APIs.
3. Apply techniques and concepts to unpack, extract, and decrypt malware.
4. Comprehend reverse-engineering of malware and anti-malware analysis techniques.
5. Achieve proficiency with industry-standard malware analysis tools.

| **Module:1** | **Fundamentals of Malware Analysis** | **5 hours** |
|---|---|---|

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, etc.

| **Module:2** | **Static Analysis** | **4 hours** |
|---|---|---|

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:3** | **Dynamic Analysis** | **4 hours** |
|---|---|---|

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:4** | **Reverse Engineering** | **4 hours** |
|---|---|---|

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

| **Module:5** | **Malicious Document Analysis** | **3 hours** |
|---|---|---|

PDF and Microsoft Office document structures – Identify PDF and office document vulnerabilities - Analysis of suspicious websites - Examining malicious documents: word, XL, PDF, and RTF files - Malware extraction and analysis tools.

| **Module:6** | **Anti-Reverse-Engineering** | **3 hours** |
|---|---|---|

Anti-Disassembly - Anti-Debugging - Anti-Forensic Malware - Packers and Unpacking – Shellcode Analysis - 64-Bit Malware

| **Module:7** | **Mobile Malware Analysis** | **5 hours** |
|---|---|---|

Mobile application penetration testing - Android and iOS Vulnerabilities - Exploit Prevention - Handheld Exploitation - Android Root Spreading and Distribution Android

| | | |
|---|---|---|
| Debugging - Machine learning techniques for malware analysis: Support Vector Machine (SVM), K-Nearest Neighbor (KNN), Random Forest (RF), Decision Trees (DT), Naïve Bayes (NB), and Neural Networks (NN). | | |
| **Module:8** | **Contemporary Issues** | **2 hours** |
| | **Total Lecture hours:** | **30 hours** |

| | |
|---|---|
| **Text Book** | |
| 1. | Abhijit Mohanta, Anoop Saldanha, Malware Analysis and Detection Engineering a Comprehensive Approach to Detect and Analyze Modern Malware, 2020, 1st edition, Apress (ISBN 978-1-4842-6192-7), United States. |
| 2. | M. Sikorski and A. Honig, Practical Malware Analysis: The Hands-on Guide to Dissecting Malicious Software. 2012, 1st edition, No Starch Press San Francisco, CA. (ISBN No.: 9781593272906), United States. |
| **Reference Books** | |
| 1. | Monnappa K A, Learning Malware Analysis- Explore the concepts, tools, and techniques to analyze and investigate Windows malware, 2018, 1st edition, Packt Publishing, (ISBN 978-1-78839-250-1), United Kingdom. |

| | | | |
|---|---|---|---|
| Mode of Evaluation: CAT / Assignment / Quiz / FAT / Seminar | | | |
| Recommended by Board of Studies | 04-03-2022 | | |
| Approved by Academic Council | No.65 | Date | 17-03-2022 |