MALWARE ANALYSIS SYLLABUS

Module 1: Fundamentals of Malware Analysis

- 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

- 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

- 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

- 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

- PDF and Microsoft Office Document Structures
- Identifying PDF and Office Document Vulnerabilities
- Analysis of Suspicious Websites
- Examining Malicious Documents: Word, Excel, PDF, and RTF Files
- Malware Extraction and Analysis Tools

Module 6: Anti-Reverse-Engineering

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

Module 7: Mobile Malware Analysis

- 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: SVM, KNN, RF, DT, Naïve Bayes, NN