UE15CS417
PRACTICAL MALWARE ANALYSIS (4-0-0-0-4)

Course Objectives:
The objective(s) of this course is to:
1. Make familiar with basic and advanced malware analysis techniques to provide sufficient information to respond appropriately to a network intrusion.
2. To analyse malicious Windows executables and documents and develop professional quality malware analysis reports.
3. To identify common indicators of infection and characteristics of different types of malware.
4. To develop host- and network-based signatures to detect malware within a network.

Course Outcomes:
At the end of the course, the student will be able to:
1. Understand the types of malware, including rootkits, Trojans, and viruses.
2. Perform basic static analysis with antivirus scanning and strings.
3. Perform basic dynamic analysis with a sandbox.
4. Understand about X86 Architecture and perform advanced static analysis with IDA Pro interface.
5. Perform advanced dynamic analysis with a debugger and OllyDbg.
6. Operate a kernel debugger with WinDbg.
7. Analyse malware behavior, including launching, encoding, and network signatures.

Course Content:

Unit I: Introduction

Unit II: Advanced Static Analysis
Unit III: Advanced Dynamic Analysis

Unit IV: Malware Functionality

Unit V: Data Encoding and Malware focused Network Signatures

References:

3. Learning Malware Analysis: Explore the concepts, tools, and techniques to analyze and investigate Windows malware by Monnappa K A
4. Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly by Dennis Andriesse