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

Introduction-Definition of Malware Analysis-Goals-Malware Analysis Techniques-Types of Malware-General Rules for Malware Analysis-Basic static Techniques-Malware Analysis in Virtual Machine-Basic Dynamic Analysis.

Unit II: Advanced Static Analysis

Levels of Abstraction-The x86 Architecture-The IDA Pro Interface-Using Cross-References -Using Graphing Options-Enhancing Disassembly-Extending IDA with Plug-ins -Recognising the code constructs in assembly-The Windows API-The Windows Registry-Networking APIs-Running Malware.

Unit III: Advanced Dynamic Analysis

Debugging-OllyDbg-Loading Malware-The OllyDbg Interface-Viewing Threads and Stacks- Breakpoints-Loading DLL-Tracing-Exception Handling-Patching-Analyzing Shellcode-Plug-ins – Scriptable Debugging-Kernel Debugging with WinDbg.

Unit IV:Malware Functionality

Malware Behavior-Backdoors-Credential Stealers-Persistence Mechanisms-Privilege Escalation-IAT and Inline Hooking-Launchers-Process Injection and Replacement-Hook Injection-APC Injection.

Unit V: Data Encoding and Malware focused Network Signatures

Goal of Analyzing Encoding Algorithms-Common Cryptographic Algorithms-Custom Encoding and Decoding-Network Countermeasures-Combining Dynamic and Static Analysis Techniques-Understanding the Attacker's Perspective.

References:

1. Sikorski, M., & Honig, A. (March 3, 2012). Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco, CA: No Starch Press. (ISBN-13: 978-1593272906, ISBN-10: 1593272901).
2. Computer Viruses and Malware, John Aycock, Springer 2006.
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
5. Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code by Michael Ligh,Steven Adair,Blake Hartstein,Matthew Richard