राष्ट्रीय प्रौद्योगिकी संस्थान पटना / NATIONAL INSTITUE OF TECHNOLOGY PATNA
संगणक विज्ञान एंव अभियांत्रिकी विभाग / DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
अशोक राजपथ, पटना-८००००५, विहार / ASHOK RAJPATH, PATNA-800005, BIHAR
Phone No.: 0612-2372715, 2370419, 2370843, 2371929 Ext- 200, 202 Fax-0612-2670631 Website: www.nitp.ac.in

No:- **Date:**

CS55XX22 Malware Analysis **L-T-P-Cr: 2-0-2-3**

Pre-requisites: Brief knowledge of the subject Network Security, TCP/IP, Network programming skills.

Course Objectives: This course will introduce students to modern malware analysis techniques through readings and hands on interactive analysis of real-world samples. After taking this course students will be equipped with the skills to analyze advanced contemporary malware using both static and dynamic analysis and memory forensics.

Course Outcomes:
CO1 Learn to analyze various malicious file types
CO2 Learn to build and utilize a sandbox environment for malware analysis
CO3 Apply various tools to Identify the vulnerabilities and to perform Malware analysis
CO4 Apply malware classification and functionality & anti-reverse engineering techniques

COs	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	2	1	2	2	0	2	0	3	0	0	2	2
CO2	2	3	1	2	3	2	0	3	2	0	2	3
CO3	3	2	2	0	2	2	0	3	0	0	2	3
CO4	3	1	2	0	2	2	0	3	2	0	2	2

UNIT I: **Lectures: 2**
Introduction to Malware Analysis, . Setting up the Lab Environment

UNIT II **Lectures: 8**
Static Analysis: Determining the File Type, Fingerprinting the Malware, Multiple Anti-Virus Scanning, Extracting Strings, Determining File Obfuscation, Inspecting PE Header Information, Comparing and Classifying the Malware

Dynamic Analysis: Lab Environment Overview, System and Network Monitoring, Dynamic Analysis (Monitoring) Tools, Dynamic Analysis Steps, Analyzing a Malware Executable, Dynamic-Link Library (DLL) Analysis.

UNIT III **Lecture: 8**
Assembly Language and Disassembly Primer: Computer Basics, CPU Registers, Data Transfer Instructions, Arithmetic Operations, Bitwise Operations, Branching and Conditionals, Loops, Functions, Arrays and Strings, Structures, x64 Architecture, Reverse Engineering using Ghidra

UNIT III: **Lectures: 4**
Malware Functionalities and Persistence: Malware Functionalities, Malware Persistence Methods

Code Injection and Hooking: Virtual Memory, User Mode and Kernel Mode, Remote DLL Injection, Hooking Techniques

UNIT IV: **Lectures: 3**

Malware Obfuscation Techniques: Simple Encoding, Malware Encryption, Custom Encoding/Encryption, Malware Unpacking, Manual Unpacking

UNIT V: **Lectures: 3**

Hunting Malware Using Memory Forensics: Memory Forensics Steps, Memory Acquisition, Volatility Overview: Enumerating Processes, Listing Process Handles, Listing DLLs, Dumping an Executable and DLL, Listing Network Connections and Sockets, Inspecting Registry

Text/Reference Books:

1. Monnappa K A, Learning Malware Analysis, Packt Publishing Ltd.
2. Michael Sikorski and Andrew Honig, “Practical Malware Analysis”, No Starch Press,2012
3. Jamie Butler and Greg Hoglund, “Rootkits: Subverting the Windows Kernel”, Addison-Wesley, 2005
4. Dang, Gazet, Bachaalany, “Practical Reverse Engineering”,Wiley,2014
5. Reverend Bill Blunden, “The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System” SecondEdition, Jones & Bartlett, 2012.