SEMESTER 5

MALWARE DETECTION AND ANALYSIS

Course Code	**PEAIT528**	**CIE Marks**	**40**
Teaching Hours/Week (L: T:P: R)	**3:0:0:0**	**ESE Marks**	**60**
Credits	**3**	**Exam Hours**	**2 Hrs 30 Mins**
Prerequisites (if any)	**PEAIT528**	**Course Type**	**Theory**

Course Objectives:

1. To develop a good understanding of malware analysis.
2. To identify different malware detection techniques.
3. To gain knowledge about advanced static malware analysis environment.
4. To gain knowledge about advanced dynamic malware analysis environment.

SYLLABUS

Module No.	Syllabus Description	Contact Hours
1	INTRODUCTION: Introduction to Malware, Operating System Security Concepts, Malware Threats, Evolution of Malware, Malware Types - Viruses, Worms, Rootkits, Trojans, Bots, Spyware, Adwares, Logic Bombs, Malware Analysis, Static Malware Analysis, Dynamic Malware Analysis, Categories of Malware, Patterns of Malware Attack, Classification of Malware By Malicious Behaviors, Malware Attack Life Cycle.	9
2	MALWARE DETECTION TECHNIQUES: Signature-based techniques: malware signatures, packed malware signature, metamorphic and polymorphic malware signature Non-signature-based techniques: similarity-based techniques, machine-learning methods, invariant inferences.	9
3	ADVANCED STATIC ANALYSIS: X86 Disassembly: Levels Of Abstraction, Reverse-Engineering, X86 Architecture: Main Memory, Instructions, Opcodes And Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method And Offsets, Analyzing Malicious Windows Programs, Portable Executable File Format, Disassembling Malicious Executable Programs. Malware Components, Malware Distribution Mechanisms, YARA.	12

KTUSPECIAL

4	ADVANCED DYNAMIC ANALYSIS: Debugging Malware, Ollydbg, Kernel Debugging With Windbg, Setting Virtual Environments-Sandboxes, Emulators, Hypervisors, Virtual Machines, Live Malware Analysis, Dead Malware Analysis, Analyzing Traces Of Malware-Systemcalls, Api Calls, Registries, Network Activities. Debugging Tricks For Unpacking Malware.	10

Course Assessment Method
(CIE: 40 marks, ESE: 60 marks)

Continuous Internal Evaluation Marks (CIE):

Attendance	Assignment/ Microproject	Internal Examination-1 (Written)	Internal Examination- 2 (Written)	Total
5	**15**	**10**	**10**	**40**

End Semester Examination Marks (ESE)

In Part A, all questions need to be answered and in Part B, each student can choose any one full question out of two questions

KTU SPECIAL

Part A	Part B	Total
• 2 Questions from each module. • Total of 8 Questions, each carrying 3 marks **(8x3 =24marks)**	• Each question carries 9 marks. • Two questions will be given from each module, out of which 1 question should be answered. • Each question can have a maximum of 3 sub divisions. **(4x9 = 36 marks)**	**60**

Course Outcomes (COs)

At the end of the course students should be able to:

Course Outcome		Bloom's Knowledge Level (KL)
CO1	To develop a good understanding of malware analysis.	K2
CO2	To identify different malware detection techniques.	K2
CO3	To gain knowledge about advanced static malware analysis environment.	K3
CO4	To gain knowledge about advanced dynamic malware analysis environment.	K3

Note*: K1- Remember, K2- Understand, K3- Apply, K4- Analyse, K5- Evaluate, K6- Create*

CO-PO Mapping Table (Mapping of Course Outcomes to Program Outcomes)

	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12
CO1	√	√	√	√	-	-	-	-	-	-	-	√
CO2	√	√	√	√	√	-	-	-	-	-	-	√
CO3	√	√	√	√	-	-	-	-	-	-	-	√
CO4	√	√	√	√	√	-	-	-	-	-	-	√

Note: *1: Slight (Low), 2: Moderate (Medium), 3: Substantial (High), -: No Correlation*

Text Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Practical Malware Analysis: The hands-On Guide to Dissecting Malicious Software	Michael Sokorski, Andrew Honig	No Starch Press,	2/e, 2012
2	Malware Analysis and Detection Engineering: Comprehensive Approach to detect and Analyze Modern Malware.	Abhijith Mohanta, Anoop Saldanha	Apress	1/e, 2020
3	Malware Detection	Christodorescu, M, Jha, S. Maughan, D. Song, D. Wang,C	Springer US	1/e, 2007

KTU SPECIAL

Reference Books				
Sl. No	**Title of the Book**	**Name of the Author/s**	**Name of the Publisher**	**Edition and Year**
1	Practical Reverse Engineering	Dang, Gazet, Bachaalany	Wiley	2014
2	MalwareForensics: Investigating and Analyzing Malicious Code	Cameron H. Malin, Eoghan Casey, and James M. Aquilina	Syngress Publications	1st Edition, 2008

Video Links (NPTEL, SWAYAM…)	
Module No.	**Link ID**
3	https://www.cybrary.it/course/malware-analysis/
3	https://www.udemy.com/course/malware-analysis-and-reverse-engineering/