GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering Syllabus

Subject Code : 3174506

Subject Name : Malware Analysis

WEF Academic Year :	2021 - 22
Semester :	7
Category of the Course :	Professional Elective

Prerequisite :	Basic knowledge of computer Network and operating system fundamentals.
Rationale :	The course will focus on the fundamentals of malware and different environments like static and dynamic malware analysis environment. The course will focus on the learning of various malware detection techniques with the latest trends used in malware analysis.

Course Scheme :

Teaching Scheme			Total Credits	Assessment Pattern and Marks				Total Marks
				Theory		Practical		
L	T	PR	C	ESE (E)	PA(M)	ESE (V)	PA (I)	
3	0	2	4	70	30	30	20	150

Course Content :

Sr. No.	Course Content	No. of Hours	% of Weightage
1	**Unit 1 : Introduction to Malware** Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types-viruses, worms, ransomware, rootkits, Trojans, bots, spyware, adware, logic Bombs, malware analysis, Malware analysis and its significance in digital forensics.	7	15
2	**Unit 2 : Static Analysis and Dynamic Analysis** Static Analysis-Determining the File Type, Fingerprinting the Malware, Extracting Strings, Determining File Obfuscation, Inspecting PE Header Information, Dynamic Analysis- System and Network Monitoring, Dynamic Analysis (Monitoring) Tools, Dynamic Analysis Steps, Dynamic-Link Library (DLL) Analysis.	8	20
3	**Unit 3 : Malware Obfuscation Techniques** Simple Encoding, Malware Encryption, Custom Encoding/Encryption, Malware Unpacking, Code Analysis Tools, Static Code Analysis (Disassembly) Using IDA, Disassembling Windows API, Patching Binary Using IDA, IDA Scripting and Plugins.	7	15

4	**Unit 4 : 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, Investigating Service, Extracting Command History.	7	15
5	**Unit 5 : 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.	7	15
6	**Unit 6 : Android Malware** Malware Characterization, Case Studies – Plankton, DroidKungFu, Smartphone (Apps) Security.	3	10
7	**Unit 7 : Latest trends in Malware Analysis** MITRE ATT&CK framework, Case study of ransomware attacks, use of Artificial Intelligence for malware attacks.	3	10
	Total	**42**	**100**

Reference Book :

- Learning Malware Analysis, Packthub, By Monnappa K A.
- Practical malware analysis The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski and Andrew Honig ISBN-10: 159327-290-1, ISBN-13: 978-1-59327-290-6,20122.
- Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006.

Course Outcome :

After Completion of the Course, Student will able to :

No.	Course Outcomes
01	To remember the basic concepts of windows operating system libraries, android operating system, and malware.
02	To understand the different methods for malware analysis and latest trends in malware analysis.
03	To apply different tools and techniques to detect malwares in windows and android using MITRE ATT&CK.

Suggested Course Practical List :

- The practical work will be carried out based on the content covered during the academic sessions.

List of Laboratory/Learning Resources Required :

- Course-related online MOOCs on NPTEL/SWAYAM platform
- Recently Published papers/articles in reputed journals
- https://www.packtpub.com/product/learning-malware-analysis/9781788392501

* * * * * * *