GUJARAT TECHNOLOGICAL UNIVERSITY

Bachelor of Engineering Syllabus

Subject Code : 3154803

Subject Name : Malware Analysis

WEF Academic Year :	2022 - 23
Semester :	5
Category of the Course :	Professional Core

Prerequisite :	Basic knowledge of Computer organization and file system.
Rationale :	This course introduces the fundamentals of malware and sets up a protected static and dynamic malware analysis environment. Learn various malware behavior monitoring tools and actionable detection signatures from malware indicators. Covers the latest trends 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)	
4	0	2	5	70	30	30	20	150

Course Content :

Sr. No.	Course Content	No. of Hours	% of Weightage
1	**Unit 1 : Introduction to Malware Analysis** Introduction to malware, OS security concepts, malware threats, Terminologies related to Malware Analysis, Need of Malware Analysis.	4	10
2	**Unit 2 : Virtual Machines and Emulators** Benefits of virtualization, Oracle Virtual Box, SANS malware analysis OS/platform, VMware Player, Virtual PC, Open-source Alternatives: Bochs, QEMU, KVM.	4	10
3	**Unit 3 : Static Analysis** 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.	7	15
4	**Unit 4 : Dynamic Analysis** Dynamic Analysis-Lab Environment Overview, System and Network Monitoring, Dynamic Analysis (Monitoring) Tools, Dynamic Analysis Steps, putting it All Together: Analyzing a Malware Executable, Dynamic-Link Library (DLL) Analysis.	7	15

5	**Unit 5 : Malware Functionality** Downloader, Backdoors, Credential Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.	7	15
6	**Unit 6 : 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
7	**Unit 7 : Latest trends in Malware Analysis** Latest trends and challenges in malware analysis like ransomware detection and mitigation, AI based malware attacks, MITRE ATT&CK Framework, Tactics ID, Techniques ID, Enterprise Level Matrix, Case study of Malware attacks.	10	20
	Total	**46**	**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	RBT Level*
01	To remember the concept of malware and concepts of the virtual environment of the operating system.	RM
02	To understand the different types of malware analysis methodology.	UN
03	To apply different tools and techniques to detect malwares in windows and android.	AP

*RM: Remember, UN: Understand, AP: Apply, AN: Analyze, EL: Evaluate, CR: Create

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

******