

Branch Name:	Cyber Security
Program Code:	ET207
Course Title:	Malware Analysis and Reverse Engineering Practical
Course Code:	2ET2070302P
Pre-requisite Course:	Basic knowledge of Computer Networks and various types of attacks

Course Objective:

This course introduces fundamentals of malware and to set up a protected static and dynamic malware analysis environment. It teaches various malware behavior monitoring tools and actionable detection signatures from malware indicators. You can learn how to trick malware into exhibiting behaviors that only occur under special conditions

Teaching and Examination Scheme:

Credit	Teaching Scheme Hours per week				Evaluation Scheme (Marks)								
					Theory (Marks)				Practical (Marks)				Total (Marks)
	SEE		CCA		SEE		CCA						
	Min.	Max.	Min.	Max.	Min.	Max.	Min.	Max.					
1	-	-	2	2	-	-	-	-	10	25	10	25	50

List of Experiments:

Sr.No	List of Practical	Total Hour
1	Identify and Unpack the Malware: Obtain a sample of a packed malware executable. Determine the packing technique (e.g., UPX). Use UPX to unpack the executable (upx -d packed_malware.exe).	2
2	Static Analysis: - Load the unpacked executable into IDA Pro. - Analyze the disassembled code to understand the malware's structure, entry points, and key functions. Identify any obfuscated code, anti-analysis techniques, or suspicious API calls.	2
3	Dynamic Analysis - Initial Execution: - Execute the unpacked malware in a controlled environment (e.g., VM). - Use a debugger (e.g., OllyDbg, x64dbg) to monitor the malware's behavior. Capture API calls, file system modifications, and registry changes.	2
4	Network Analysis: Use Wireshark to capture and analyze network traffic generated by the malware. Identify any command-and-control (C&C) communications, data exfiltration attempts, or other malicious network activities.	2
5	Behavioral Analysis: Use Process Monitor to capture runtime activities such as process creation, DLL loading, and system service interactions. Document any suspicious behaviors observed during runtime, such as attempts to inject code into other processes or modify system configurations.	2
6	Reverse Engineering Challenges: Identify and overcome any anti-debugging or anti-analysis techniques employed by the malware. Analyze encrypted strings or payloads using static and dynamic decryption techniques.	2
7	Documentation and Reporting: Compile a comprehensive report detailing the malware's behavior, capabilities, and potential impact on systems. Include analysis findings, screenshots of key moments in the execution, and recommendations for mitigation or further investigation.	2

Review Presentation:

- The student is expected to refer at least two peer reviewed journal papers related to this domain/subject.
- The student is expected to identify issues/challenges and emerging trends in the domain/subject.
- Student is supposed to explore various video lectures (E.g. NPTEL) available in the domain/subject.
- Student is required to make a review-presentation on the work carried out for the same.

List of References:

1. 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, 2012
2. Computer viruses: from theory to applications by Filiol, Eric Springer Science & Business Media, 2006
3. Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005
4. Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis,
5. Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
6. Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

Course Learning Outcomes (CLO): On completion of this course, the students will be able to:

CLO	Description	Bloom's Taxonomy Level
CLO1	Understand the concept of secure operating system & virtualization and Understand the nature of malware, its capabilities, and how it is combated through detection and	1 Remembering, 2 Understanding
CLO2	To apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples	2 Understanding, 3 Applying
CLO3	Understand what are the underlying scientific and logical limitations on society's ability to combat malware?	1 Remembering, 2 Understanding
CLO4	To have a broad understanding of the social, economic, and historical context in which malware occurs	2 Understanding, 3 Applying

Mapping of CLOs with POs & PSOs:

Course Learning Outcomes	Program Outcomes (POs)												Program Specific Outcomes(PSOs)			
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3	PSO4
CLO1	H	L	L	L	M							M	L	L		
CLO2	M	M	H	L	M							M	M	M		
CLO3	L	L	M	M	M							M	L	M		
CLO4	L	L	H	L	M							M	M	M	M	

H: High, M: Medium, L: Low