GUJARAT TECHNOLOGICAL UNIVERSITY

Master of Engineering
Subject Code: 3725908
Semester II
Mal-Ware Analysis

Type of course: Master of Engineering

Prerequisite: Undergraduate courses in logic and discrete mathematics, assembly, and imperative programming, OS fundamentals, fundamentals of c language

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

Teaching and Examination Scheme:

Teaching Scheme			Credits	Examination Marks				Total Marks
				Theory Marks		Practical Marks		
L	T	P	C	ESE (E)	PA (M)	ESE (V)	PA (I)	
3	0	2	4	70	30	20	10	150

Content:

Sr. No.	Contents	Hours
1	**INTRODUCTION:** Introduction to Mal-ware, OS security concepts, Mal-ware threats, evolution of Mal-ware, Mal-ware types- viruses, worms, root-kits, Trojans, bots, spy-ware, ad-ware, logic bombs, Mal-ware analysis, static Mal-ware analysis, dynamic Mal-ware analysis.	6
2	**Virtual Machines and Emulators:** Benefits Of Virtualization, Oracle Virtual Box, VMware Player, Virtual PC, Open source Alternatives:Bochs, QEMU, KVM	04
3	**Vulnerability Scanning:** Overview of Vulnerability Scanning, Open Port Service Identification, Banner/Version Check,Traffic Probe,Vulnerability Probe,Vulnerability Examples	03
4	**STATIC ANALYSIS:** X86 Architecture- Main Memory, Instructions, Opcodes and Endian-ness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets. Anti-virus Scanning, Fingerprint for Mal-ware, Portable Executable File Format, The PE File Headers and Sections, The Structure of a Virtual Machine, Reverse-Engineering- x86 Architecture, recognizing c code constructs in assembly, c++ analysis, Analyzing Windows programs, Anti-static analysis techniques- obfuscation, packing, metamorphism, polymorphism.	08
5	**DYNAMIC ANALYSIS:** live Mal-ware analysis, dead Mal-ware analysis, analyzing traces of Mal-ware- System-calls, API-calls, registries, network activities. Anti-dynamic analysis techniques- anti-vm, runtime-evasion techniques, , Mal-ware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wire-shark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching	06
6	**Mal-ware Functionality:** Down-loaders, Back-doors, Credential Stealer's,	5

	Persistence Mechanisms, Privilege Escalation, Covert Mal-ware launching-Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.	
7	**Mal-ware Detection Techniques:** Signature-based techniques: Mal-ware signatures, packed Mal-ware signature, metamorphic and polymorphic Mal-ware signature Non-signature based techniques: similarity-based techniques, machine-learning methods, invariant inferences.	5
8	**Android Mal-ware**: Mal-ware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	5
		42

Reference Books:

- Practical malware analysis by Sikorski, Michael, and Andrew Honi Netw. Secur 2012.12 (2012)
- Anti-Hacker Tool kit by Mike Shema,Mcgraw Hill Education (India) Fourth Edition,2014
- 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
- Android Malware by Xuxian Jiang and Yajin Zhou, Springer ISBN 978-1-4614-7393-0, 2005
- Hacking exposed™ malware & rootkits: malware & rootkits security secrets & Solutions by Michael Davis, Sean Bodmer, Aaron Lemasters, McGraw-Hill, ISBN: 978-0-07-159119-5, 2010
- Windows Malware Analysis Essentials by Victor Marak, Packt Publishing, 2015

Course Outcome:

Sr. No.	CO statement	Marks % weightage
CO-1	Understand the concept of secure operating system & virtualization and Understand the nature of malware, its capabilities, and how it is combated through detection and classification	20
CO-2	To apply the tools and methodologies used to perform static and dynamic analysis on unknown executables. To have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.To apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.	20
CO-3	To apply techniques and concepts to unpack, extract, decrypt, or bypass new anti-analysis techniques in future malware samples.	25
CO-4	Understand what are the underlying scientific and logical limitations on society's ability to combat malware?	20
CO-5	To have a broad understanding of the social, economic, and historical context in which malware occurs	15

List of Experiments:

1. Set up a safe virtual environment to analyze Mal-ware.
2. Quickly extract network signatures and host-based indicators.
3. Use key analysis tools like IDA Pro, OllyDbg, and WinDbg.

4. Overcome Mal-ware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques.
5. Use your newfound knowledge of Windows internals for Mal-ware analysis.
6. Develop a methodology for unpacking Mal-ware and get practical experience with five of the most popular packers.
7. Analyze special cases of Mal-ware with shell-code, C++, and 64-bit code.