GUJARAT TECHNOLOGICAL UNIVERSITY
Syllabus for Integrated MSc, 8th Semester
Branch: Computer Science
Subject Name: Malware Analysis
Subject Code: 1380309

Teaching and Examination Scheme:

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

Content:

Sr. No.	Content	Teaching Hours	(%) Module Weightage
1	**INTRODUCTION:** Introduction to malware, OS security concepts, malware threats, evolution of malware, malware types viruses, worms, rootkits, Trojans, bots, spyware, adware, logic bombs, malware analysis, static malware analysis, dynamic malware analysis.	5	10
2	**STATIC ANALYSIS:** X86 Architecture- Main Memory, Instructions, Opcodes and Endianness, Operands, Registers, Simple Instructions, The Stack, Conditionals, Branching, Rep Instructions, C Main Method and Offsets. Antivirus Scanning, Fingerprint for Malware, 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,Anti-static analysis techniques obfuscation, packing, metamorphism, polymorphism.	8	20
3	**DYNAMIC ANALYSIS:** Live malware analysis, dead malware analysis, analyzing traces of malware- system-calls, api-calls, registries, network activities. Anti-dynamic analysis techniques anti-vm, runtime-evasion techniques, Malware Sandbox, Monitoring with Process Monitor, Packet Sniffing with Wireshark, Kernel vs. User-Mode Debugging, OllyDbg, Breakpoints, Tracing, Exception Handling, Patching.	8	20
4	**IN-DEPTH MALWARE ANALYSIS:** Recognizing packed malware, getting started with unpacking, using debuggers for dumping packed malware from memory, analyzing multi-technology and file-less malware, Code injection and API hooking, Using memory forensics for malware analysis	06	15
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	08	20
6	**ANDROID MALWARE:** Malware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	05	15

w.

Reference Books:

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
3. 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
4. Reverend Bill Blunden, "The Rootkit Arsenal: Escape and Evasion in the Dark Corners of the System" Second Edition, Jones & Bartlett.

Course Outcome:

1. Students with a specialist understanding of the nature of malware, its capabilities, and how it is combated through detection and classification
2. Students will be able to apply the tools and methodologies used to perform static and dynamic analysis on unknown executables.
3. Students will have an intimate understanding of executable formats, Windows internals and API, and analysis techniques.
4. Students will able to apply techniques and concepts to unpack, extract, decrypt, or bypass new ant analysis techniques in future malware samples.
5. Students will understand what are the underlying scientific and logical limitations on society's ability to combat malware
6. Furthermore, students would have a broad understanding of the social, economic, and historical context in which malware occurs

List of Experiments:

1. Set up a safe virtual environment to analyze malware
2. Quickly extract network signatures and host-based indicators
3. Use key analysis tools like IDA Pro, OllyDbg, and WinDbg
4. Overcome malware tricks like obfuscation, anti-disassembly, anti-debugging, and anti-virtual machine techniques
5. Use your newfound knowledge of Windows internals for malware analysis
6. Develop a methodology for unpacking malware and get practical experience with five of the most popular packers
7. Analyze special cases of malware with shellcode, C++, and 64-bit code
8. Install Reanimator in your Windows machine and scan the system for Malware and prepare one report for the same.

List of open Source software/learning Websites:

- http://www.malware-analyzer.com
- http://resources.infosecinstitute.com/malware-analysis-basic-dynamictechniques/#gref
- http:://www.remux.or