GUJARAT TECHNOLOGICAL UNIVERSITY
BRANCH: CYBER SECURITY (59)
SUBJECT NAME: MALWARE ANALYSIS
SUBJECT CODE: 2725908
SEMESTER: II

Type of course: Master of Engineering (Cyber Security)

Prerequisite: Basic knowledge of Computer Networks and various types of attacks.

Rationale:
This course introduces the fundamentals of malware and to set up a protected static and dynamic malware analysis environment. Learn various malware behaviour monitoring tools and actionable detection signatures from malware indicators. 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)		
						ESE	OEP	PA	RP	
3	0	2	4	70	30	20	10	10	10	150

Content:

Sr. No.	Contents	Hours	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.	6	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, c++ analysis, Analyzing Windows programs, Anti-static analysis techniques- obfuscation, packing, metamorphism, polymorphism.	15	25%
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	15	25%
4	**Malware Functionality:** Downloader, Backdoors, Credential	6	10%

	Stealers, Persistence Mechanisms, Privilege Escalation, Covert malware launching- Launchers, Process Injection, Process Replacement, Hook Injection, Detours, APC injection.		
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.	8	15%
6	**Android Malware**: Malware Characterization, Case Studies – Plankton, DroidKungFu, AnserverBot, Smartphone (Apps) Security	8	15%

Reference Books:

• 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

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.

Course Outcomes:

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 anti-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

Major Equipments:

The following are minimal requirements for your laptop:

- Intel-compatible 64-bit dual-core CPU i5 or higher (a faster processor is recommended)
- 8 GB RAM (more memory is recommended)
- 60 GB of available disk space (more space is recommended)
- USB port 2.0 or higher (USB port 3.0 is recommended)
- Ethernet network interface card (NIC) or adapter
- Wi-Fi card or adapter
- Virtualization support enabled in the BIOS; this is sometimes called Intel Virtualization Technology (also known as Intel VT) or AMD-V

List of open Source software/learning Websites:

- http://www.malware-analyzer.com
- http://resources.infosecinstitute.com/malware-analysis-basic-dynamic-techniques/#gref
- http:://www.remux.org