**Subject Code:** 01CY0207

**Subject Name: Malware Analysis and Network Security**

**MTech. Year – 1 (Semester – 2)**

**Objective:**

|  |
| --- |
| To familiarize with the practice of Malware Analysis suspicious files by utilizing static and dynamic tactics, techniques, and procedures in order to gain an understanding as to what impact the suspicious file may have on a particular computer system when executed. |

**Credits Earned:** 4 Credits

**Course Outcomes:** After completion of this course, student will be able to

* Understand Information Gathering Methodology.
* Understand Active and Passive Attacks.
* To identify suspicious files and Trends of Malware Analysis.
* Understand Classifications of Malware, Threats of Malware.
* Apply Reverse Engineering Concept.

**Pre-requisite of course:** Information Security and Reverse Engineering

**Teaching and Examination Scheme**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Teaching Scheme (Hours) | | | Credits | Theory Marks | | | Tutorial/ Practical Marks | | Total Marks |
| Theory | Tutorial | Practical | ESE (E) | Mid Sem (M) | Internal (I) | Viva (V) | Term work (TW) |
| 3 | 0 | 2 | 4 | 50 | 30 | 20 | 25 | 25 | 150 |

**Contents:**

|  |  |  |
| --- | --- | --- |
| **Unit** | **Topics** | **Contact Hours** |
| 1 | **Introduction:**   |  |  | | --- | --- | | |  | | --- | | Malware Trends, Naming and Characteristics of Malware, Classification by attack areas, Boot Sectors, Files, Macros, Classification by self – concealment ways, Encryption, Stealth, Oligomorphic, Polymorphism, Metamorphism.  Reconnaissance: Information Gathering Methodology, Locate the Network Range, Active and Passive reconnaissance. | | | 6 |
| 2 | **Understanding the Malware Threats:**  Malware indicators, Malware Classification, Insider and Outsider threats, countermeasures, Side channel analysis, Power analysis, Differential power attacks, Timing attacks, Physically unclonable functions | 7 |
| 3 | **Fundamentals of Malware Analysis:**  Revere Engineering Malware (REM) Methodology, Introduction to key MA tools and techniques, Behavioural Analysis Vs. Code Analysis | 8 |
| 4 | |  | | --- | | **Scanning:**  Scanning, Elaboration phase, active scanning, scanning tools NMAP, hping2. Enumeration, DNS Zone transfer. Detecting live systems on the target network, discovering services running /listening on target systems, understanding port scanning techniques, Identifying TCP and UDP services running on the target network, Understanding active and passive fingerprinting  **Trojans and Backdoors:**  Effect on Business, Trojan, Overt and Covert Channels, Working of Trojans, Different Types of Trojans, Different ways a Trojan can get into a system, Indications of a Trojan Attack, some famous Trojans and ports used by them. | | 10 |
| 5 | |  | | --- | | **Resources for Reverse-Engineering Malware (REM):**  Initial Infection Vectors and Malware Discovery, Sandboxing Executables and Gathering Information from Runtime Analysis, The Portable Executable (PE32) File Format, Identifying Executable Metadata, Executable Packers and Compression, and Obfuscation, Techniques. Utilizing Software Debuggers to Examine Malware, triggering exploits by Emulating Browser DOM Elements. Triggering Exploits by Faking PDF Software Versions, Analysing Microsoft Office File, Debugging Office Shellcode. | | 9 |
|  | **Total Hours** | **40** |

**References:**

|  |  |
| --- | --- |
| 1. Malware Analyst’s Cookbook: Tools and Techniques for Fighting Malicious Code, Michael Ligh, Steven Adair, Blake Hartstein, and Matthew Richard ,Wiley,1st Edition,2010. 2. Practical Malware Analysis, Michael Sikorski and Andrew Honig, No Starch Press, 1st edition,2012 3. Network Security Essentials, William Stallings, Prentice hall, 5th Edition, 2013  |  | | --- | |  | |

**Suggested Theory distribution:**

The suggested theory distribution as per Bloom’s taxonomy is as per follows. This distribution serves as guidelines for teachers and students to achieve effective teaching-learning process

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Distribution of Theory for course delivery and evaluation | | | |  |
| Remember | Understand | Apply | Analyze | Evaluate | Create |
| 5% | 10% | 15% | 30% | 20% | 30% |

**Suggested List of Experiments:**

**Instructional Method:**

1. The course delivery method will depend upon the requirement of content and need of students. The teacher in addition to conventional teaching method by black board, may also use any of tools such as demonstration, role play, Quiz, brainstorming, MOOCs etc.
2. The internal evaluation will be done on the basis of continuous evaluation of students in the laboratory and class-room.
3. Practical examination will be conducted at the end of semester for evaluation of performance of students in laboratory.
4. Students will use supplementary resources such as online videos, NPTEL videos, e-courses, Virtual Laboratory