

|                              |                                                                   |
|------------------------------|-------------------------------------------------------------------|
| <b>Branch Name:</b>          | Cyber Security                                                    |
| <b>Program Code:</b>         | ET207                                                             |
| <b>Course Title:</b>         | Malware Analysis and Reverse Engineering                          |
| <b>Course Code:</b>          | 2ET2070302T                                                       |
| <b>Pre-requisite Course:</b> | Basic knowledge of Computer Networks and various types of attacks |

**Course Objective:**

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

**Teaching and Examination Scheme:**

| Credit | Teaching Scheme<br>Hours per week |   |   |       | Evaluation Scheme (Marks) |      |      |      |                   |      |      |      | Total<br>(Marks) |
|--------|-----------------------------------|---|---|-------|---------------------------|------|------|------|-------------------|------|------|------|------------------|
|        |                                   |   |   |       | Theory (Marks)            |      |      |      | Practical (Marks) |      |      |      |                  |
|        | L                                 | T | P | Total | SEE                       |      | CCA  |      | SEE               |      | CCA  |      |                  |
|        |                                   |   |   |       | Min.                      | Max. | Min. | Max. | Min.              | Max. | Min. | Max. |                  |
| 3      | 3                                 | - | - | 3     | 24                        | 60   | 16   | 40   | -                 | -    | -    | -    | 100              |

**Course Contents:**

| Sr. No | Topic                                                                                                                                                                                                                                                                                                                                                                              | Total Hours | Weight (%) |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|------------|
| 1      | <b>Introduction:</b> Types of Malware, Malware attack Life Cycle, Malware Business model, Malware Analysis setup, Operating Systems Files and File formats, Intrusion into IT and operational network (OT) and their signs, signature-based malware detection and classification – pros and cons, and need for machine learning-based techniques.                                  | 7           | 20%        |
| 2      | <b>Advanced Techniques Malware Analysis:</b> Static Analysis, Dynamic Analysis, and Hybrid Analysis of Windows Malware, Linux Malware, and Android Malware, Virtual memory and Portable Executable Files, Windows Internals – Win32 API, Registry, Directories, Processes, and services.                                                                                           | 8           | 20%        |
| 3      | <b>Static and Dynamic Malware Analysis:</b><br>Fingerprinting the Malware - PE: File types, header analysis, Extracting Strings - Classifying Malware using YARA - Tools: PEid and TrID, MASTIFF, PE executables.<br>Behavior Events Analysis using ProcMon and Autoruns - Detecting Code Injection - Automated dynamic analysis - Sandboxing: Tools and Techniques - Virus Total. | 8           | 20%        |
| 4      | <b>Purpose of Reverse Engineering:</b> Malware Components: Malware Components, Distribution mechanisms, Malware Packers, Persistence mechanism, Network Communication, Detecting Network Communication, Code Injection, Process Hollowing, API Hooking, Stealth techniques and Rootkits                                                                                            | 6           | 20%        |
| 5      | <b>Malware Reverse Engineering:</b> Debuggers and disassembly, Debugging for unpacking malware and code injections, Armoring Techniques<br>Detection Engineering : Device Analysis, Anti Virus Engines, IDS/IPS and Snort /Suricata rule writing, Malware Sandbox Internals, DBI for Malware analysis                                                                              | 6           | 20%        |

**Review Presentation:**

1. 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.
2. 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.
3. Recommended sites for journal papers are (1) dl.acm.org (2) springer.com (3) sciencedirect.com (4) elsevier.com (5) ieeexplore.ieee.org (6) scholar.google.co.in (7) scopus.com or others of similar repute.

**List of References:**

1. nces 1. Product Design: Techniques in Reverse Engineering and New Product Development by K. Otto and K. Wood Prentice Hall, 2001.
2. 2. Reverse Engineering: An Industrial Perspective by Raja and Fernandes. Springer-Verlag 2008
3. 3. RE as necessary phase by rapid product development by Sokovic and Kopac. Journal of Materials Processing Technology 2005
4. 4. Reversing: Secrets of Reverse Engineering by Eldad Eilam Publisher: Wiley (April 15, 2005)
5. 5. The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler by Chris Eagle

**Course Outcome:**

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

| CLO  | Description                                                                                   | Bloom's Taxonomy Level         |
|------|-----------------------------------------------------------------------------------------------|--------------------------------|
| CLO1 | Basic Malware Analysis and Learning to analyze various malicious file types.                  | 1 Remembering, 2 Understanding |
| CLO2 | Advanced Techniques Malware Analysis with the use of sandbox environment for malware analysis | 2 Understanding, 3 Applying    |
| CLO3 | Advanced Reverse Engineering Techniques                                                       | 1 Remembering, 2 Understanding |
| CLO4 | Remediation of Advanced Persistent Threats                                                    | 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**