Reg. No. \_\_\_\_\_\_\_\_\_\_\_\_\_



**End Semester Examination – Nov / Dec – 2019**

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
| **Code :** | **17CA2051** | **Duration :** | **3hrs** |
| **Sub. Name :** | **MALWARE ANALYSIS AND SECURITY** | **Max. Marks :** | **100** |

**ANSWER ALL QUESTIONS (5 x 20 = 100 Marks)**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Q. No.** | **Sub Div.** | **Questions** | **Course**  **Outcome** | **Marks** |
| 1. | a. | Evaluate the propagation methods of Malware. | CO1 | 10 |
| b. | Describe the role of tools such as process explorer and virus total in identifying malware infection. | CO1 | 10 |
| **(OR)** | | | | |
| 2. | a. | Distinguish malware and virus in detail with suitable example. | CO2 | 7 |
| b. | Outline the categories of malicious software. | CO2 | 4 |
| c. | Describe worm and discuss the effect of worm. | CO2 | 4 |
| d. | Enumerate Malware Evolution. | CO1 | 5 |
|  |  |  |  |  |
| 3. | a. | Explain the following: (Each 2 Marks)  i) Boot Sector viruses ii) Program Viruses  iii) Macro viruses iv) Email Viruses  v) Resident Viruses vi) Non Resident viruses  vii) Stealth viruses | CO3 | 14 |
|  | b. | Write a short note on Logic bomb and the prevention mechanism. | CO3 | 6 |
| **(OR)** | | | | |
| 4. | a. | Explain Dictionary attack and its methodology. | CO3 | 10 |
| b. | Discuss the functions of the components such as replicator, concealer and dispatcher in a malware. | CO3 | 10 |
|  |  |  |  |  |
| 5. | a. | Discuss in detail the polymorphic viruses, its propogation and the defense mechanism. | CO3 | 14 |
| b. | Explain the ways in which the known threats and the unknown threats can be prevented. | CO3 | 4 |
| c. | Distinguish Compiled virus and Interpreted virus. | CO3 | 2 |
| **(OR)** | | | | |
| 6. |  | List the various damages caused by malware when infects a system. | CO3 | 20 |
|  |  |  |  |  |
| 7. | a. | Write a short note on Static Analysis. | CO4 | 7 |
| b. | Discuss the Portable Executable (PE) file format. | CO4 | 5 |
| c. | Explain the String Analysis and Basic Analysis in detail. | CO4 | 8 |
| **(OR)** | | | | |
| 8. | a. | Explain the infection methods of Ransomware Attack. | CO5 | 10 |
| b. | Explain the following: (each 5 marks)  i) Happy worm 99 ii) Sassar Virus. | CO5 | 10 |
|  | | **Compulsory**: |  |  |
| 9. | a. | Illustrate the precautions taken by a security administrator in Anti-malware mitigation. | CO6 | 10 |
| b. | Write a short note on overt and covert channels. | CO6 | 10 |