|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Roll No. |  |  |  |  |  |  |  |  |  |  |  |  |



 **PRESIDENCY UNIVERSITY**

  **Bengaluru**

|  |
| --- |
| **End - Term Examinations – JANUARY 2025** |
| **Date:** 04 - 01-2025 **Time:** 09:30 am – 12:30 pm |

|  |  |
| --- | --- |
| **School:** SOCSE | **Program:** B.Tech – CCS |
| **Course Code :** CSE3102 | **Course Name :** Malware Analysis |
| **Semester**: VII | **Max Marks**:100 | **Weightage**:50% |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** |
| **Marks** | **24** | **24** | **26** | **26** |

**Instructions:**

1. *Read all questions carefully and answer accordingly.*
2. *Do not write anything on the question paper other than roll number.*

**Part A**

|  |
| --- |
| **Answer ALL the Questions. Each question carries 2marks. 10Q x 2M=20M** |
| **1** | What is Malware Analysis. | **2 Marks** | **L1** | **CO1** |
| **2** | Compare Vulnerability and Malware | **2 Marks** | **L2** | **CO1** |
| **3** | Write a short note on DLLs with examples. | **2 Marks** | **L1** | **CO2** |
| **4** | Define Backdoors | **2 Marks** | **L1** | **CO2** |
| **5** | What is the purpose of Debugging in Malware Analysis. | **2 Marks** | **L1** | **CO3** |
| **6** | Demonstrate the use of breakpoint in the context of assembly-level debugging? | **2 Marks** | **L2** | **CO3** |
| **7** | List any two tools used for Advanced Dynamic Analysis | **2 Marks** | **L1** | **CO3** |
| **8** | How Hook injection process impacts the malware Analysis. | **2 Marks** | **L1** | **CO4** |
| **9** | Define APC Injection. | **2 Marks** | **L1** | **CO4** |
| **10** | Compare Malware Analysis and Malware Detection | **2 Marks** | **L2** | **CO4** |

**Part B**

|  |
| --- |
| **Answer the Questions Total 80 Marks.** |
| **11.** | **a.** | Explain* Adware,
* spyware,
* virus,
* worm,
* Trojan horse,

With suitable examples. | **10 Marks** | **L2** | **CO1** |
|  | **b.** | While conducting Malware Analysis, Explain the guidelines to be followed for Static Analysis and Dynamic Analysis. | **10 Marks** | **L2** | **CO1** |
| **Or** |
| **12.** | **a.** | Explain the different types of malware analysis, including static, dynamic, and hybrid analysis along with the procedures used in each analysis techniques. | **10 Marks** | **L2** | **CO1** |
|  | **b.** | Interpret the OS Security Concepts used for Malware Analysis in suitable case study. | **10 Marks** | **L2** | **CO1** |
|  |  |  |  |  |  |
| **13.** | **a.** | Explain the concept of reverse engineering in the context of malware investigation.  | **10 Marks** | **L2** | **CO2** |
| **b.** | Explain, How malware investigators can benefit from reverse engineering to understand the behaviour, intent, and functionality of malware. | **10 Marks** | **L2** | **CO2** |
| **Or** |
| **14.** | **a.** | Compare the challenges and limitations of static and Advanced Static malware analysis. | **10 Marks** | **L2** | **CO2** |
| **b.** | Illustrate the effectiveness of advanced tools and techniques, including binary analysis, in addressing these challenges and improving the accuracy and efficiency of malware analysis. | **10 Marks** | **L2** | **CO2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **15.** | **a.** | Demonstrate the detailed Dynamic Analysis Procedure for Process Monitoring using ProcMon Tool. | **10 Marks** | **L2** | **CO3** |
| **b.** | Explain the Procedure for packet sniffing using iNetSim and Wireshark Tools. | **10 Marks** | **L2** | **CO3** |
| **Or** |
| **16.** | **a.** | Explain the process of analyzing a program using OllyDbg. | **10 Marks** | **L2** | **CO3** |
| **b.** | Demonstrate the process of Setting Different Breakpoints in Ollydbg and windbg. | **10 Marks** | **L2** | **CO3** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **17.** | **a.** | Identify Process injection methods used by malware launchers. | **10 Marks** | **L3** | **CO4** |
| **b.** | Choose suitable Malware launchers which are applicable to bypass host-based firewall. | **10 Marks** | **L3** | **CO4** |
| **Or** |
| **18.** | **a.** | Develop a real time science to prove that behavioural-based detection would be more effective than signature-based detection? | **10 Marks** | **L3** | **CO4** |
| **b.** | Identify the machine learning-based systems used in accurately identifying malware? | **10 Marks** | **L3** | **CO4** |

**\*\*\*\*\* BEST WISHES \*\*\*\*\***