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



**PRESIDENCY UNIVERSITY**

**Bengaluru**

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

|  |  |  |
| --- | --- | --- |
| **School:** SOCSE | **Program:** B.Tech CDV | |
| **Course Code :**CSE3051 | **Course Name :** System Monitoring | |
| **Semester**: VII | **Max Marks**:100 | **Weightage**: 50% |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **CO - Levels** | **CO1** | **CO2** | **CO3** | **CO4** | **CO5** |
| **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 are the essential components of system monitoring? | **2 Marks** | **L1** | **CO1** |
| **2** | Mention any two tools used for system monitoring. | **2 Marks** | **L1** | **CO1** |
| **3** | What is the principle of "Build Once, Deploy Anywhere"? | **2 Marks** | **L1** | **CO2** |
| **4** | Name two common risks faced during software delivery. | **2 Marks** | **L2** | **CO2** |
| **5** | What is software configuration management? | **2 Marks** | **L1** | **CO3** |
| **6** | Define "build automation." | **2 Marks** | **L1** | **CO3** |
| **7** | Name two tools commonly used for implementing a testing strategy. | **2 Marks** | **L2** | **CO3** |
| **8** | What is the difference between unit testing and integration testing? | **2 Marks** | **L1** | **CO4** |
| **9** | Define the term "pipeline as code." | **2 Marks** | **L1** | **CO4** |
| **10** | What are the key stages of a development pipeline? | **2 Marks** | **L1** | **CO4** |

**Part B**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Answer the Questions Total 80 Marks.** | | | | | |
| **11.** | **a.** | Describe the steps involved in implementing a procedural approach to system monitoring, and why is this approach considered effective in ensuring proactive issue resolution, efficiency, scalability, and alignment with business goals? | **20 Marks** | **L2** | **CO1** |
| **Or** | | | | | |
| **12.** | **a.** | Classify the real-time data visualization be applied in a monitoring infrastructure to enhance system performance, and what are the best practices for designing effective dashboards? | **20 Marks** | **L3** | **CO1** |
|  |  |  |  |  |  |
| **13.** | **a.** | Compare the advantages and disadvantages of manual software deployment versus automated deployment. Additionally, discuss the key principles of effective software delivery and explain how they enhance the development process. | **20 Marks** | **L2** | **CO2** |
| **Or** | | | | | |
| **14.** | **a.** | Failure prevention in system monitoring involves strategies and practices designed to identify and address potential issues before they lead to system failures. By monitoring system behavior, performance metrics, and logs, early warning signs of problems can be detected, enabling teams to take corrective actions. Compare and contrast reactive and proactive failure prevention strategies in system monitoring. | **20 Marks** | **L2** | **CO2** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **15.** | **a.** | You are part of the IT security team responsible for monitoring the network and systems of a large financial institution. Your monitoring setup includes Prometheus for metrics collection, Grafana for visualization, and various exporters (e.g., Node Exporter, MySQL Exporter) to monitor different components.  One morning, you notice that Grafana dashboards are failing to load certain metrics, and several alerts are being missed. Upon investigating, you realize:  i. The MySQL Exporter (used to monitor database metrics) is crashing intermittently due to an outdated version that is incompatible with the latest version of Prometheus you upgraded last week.  ii.You also discover that the Prometheus upgrade introduced a breaking change in how it handles a certain query language function that some of your critical alerts depend on.  What dependency management processes would you implement to prevent similar issues from occurring during future updates to the monitoring stack? | **20 Marks** | **L3** | **CO3** |
| **Or** | | | | | |
| **16.** | **a.** | Explain the role of manual testing versus automated testing in a testing strategy. In what scenarios would each approach be more appropriate, and how can they complement each other to achieve optimal results? | **20 Marks** | **L2** | **CO3** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **17.** | **a.** | Describe how you would implement a security testing strategy for a web application. Discuss the various security testing techniques such as penetration testing, vulnerability scanning, and threat modeling, and explain how they contribute to securing the application. | **20 Marks** | **L2** | **CO4** |
| **Or** | | | | | |
| **18.** | **a.** | You are part of the cybersecurity team at a mid-sized organization. The company relies on continuous monitoring to detect security threats and vulnerabilities in its internal network. Your task is to maintain the security of the network through ongoing management of logs, alerts, and system behaviors. The organization uses a Security Information and Event Management (SIEM) system integrated with threat detection tools like IDS/IPS. Recently, there have been a series of suspicious activities and minor security alerts, but nothing significant enough to raise an immediate alarm. The goal of this exercise is to ensure that you can identify patterns in low-level alerts, correlate data from different sources, and respond quickly before these events escalate into major security incidents. In the given scenario, as a member of the cybersecurity team at a mid-sized organization, how do you contribute to the overall security management? What are your key responsibilities in ensuring a robust security posture, particularly in relation to detecting suspicious activities, managing logs, alerts, and system behaviors, and responding to minor security events before they escalate into major incidents? How do tools like SIEM and IDS/IPS aid in achieving these objectives? | **20 Marks** | **L3** | **CO4** |

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