

**GYANMANJARI INNOVATIVE UNIVERSITY**  
**GYANMANJARI INSTITUTE OF TECHNOLOGY**  
**B.Tech. - Mid Semester Examination (MSE) - W2026**

**Enrollment No.:** \_\_\_\_\_  
**Subject Code:** BETCE16407  
**Subject Name:** Intrusion Detection and Prevention System  
**Time:** 2:30 PM to 4:30 PM

**Date:** 24-09-2026  
**Semester:** 7  
**Total Marks:** 60

**Instructions:**

1. Question No. 1 is compulsory.
2. Make suitable assumptions wherever necessary.
3. Figures to the right indicate full marks.

|                                                                                                                                  | Marks |
|----------------------------------------------------------------------------------------------------------------------------------|-------|
| Q.1 (a) Define Intrusion Detection System (IDS).                                                                                 | 05    |
| (b) Compare signature-based and anomaly-based detection techniques in terms of detecting known versus unknown attacks.           | 05    |
| (i) Explain the concept and need of an Intrusion Prevention System (IPS) in modern networks.                                     | 10    |
| (ii) Explain the role of a firewall in network security.                                                                         |       |
| Q.2 (a) Evaluate the reliability of an IDS that produces a high number of false positives.                                       | 05    |
| (b) Compare the roles of IDS, IPS, and firewall in a layered security architecture.                                              | 05    |
| <b>OR</b>                                                                                                                        |       |
| (b) Analyse the impact of not having an IDS/IPS deployed in an organization's network.                                           | 05    |
| (c) (i) Demonstrate how statistical approaches can be used to detect an unusual spike in network traffic.                        | 10    |
| (ii) Apply the concept of false positive and false negative to a scenario where a legitimate user login triggers an alert.       |       |
| <b>OR</b>                                                                                                                        |       |
| (c) (i) Illustrate how a machine-learning based IDS would classify an incoming packet as malicious or benign.                    | 10    |
| (ii) Give an example of a rule that could be used for rule-based detection of repeated failed login attempts.                    |       |
| Q.3 (a) Evaluate the challenges an organization might face while selecting an appropriate IDS classification for its network.    | 05    |
| (b) Analyse how the choice of performance evaluation metric affects the assessment of an IDS's real-world effectiveness.         | 05    |
| (c) (i) Evaluate the effectiveness of a firewall compared to an IDS/IPS in preventing sophisticated, multi-stage cyberattacks.   | 10    |
| (ii) Propose a basic IDS/IPS architecture suitable for a small organization's network.                                           |       |
| <b>OR</b>                                                                                                                        |       |
| Q.3 (a) Analyse because a hybrid detection approach may achieve better accuracy than a single detection technique.               | 05    |
| (b) Examine the relationship between security threats and vulnerabilities in the context of the cyberattack lifecycle.           | 05    |
| (c) (i) Justify the use of behaviour analysis over rule-based detection in an environment with rapidly evolving attack patterns. | 10    |
| (ii) Design a simple rule-based detection logic to identify a brute-force login attempt.                                         |       |