**CS MID-2 Descriptive Questions**

**UNIT-3**

1. Explain the countermeasures to be practiced for possible attacks on mobile/cell phones.
2. What kinds of cyber security measures an organization should have to take in case of portable storage devices? Prepare security guidelines which can be implemented in an organization.
3. Explain the various measures for protection of laptops through physical measures and logical access control measures.

**UNIT-4**

1. What are the different phases during an attack on the network, and why is understanding these phases crucial for network security?
2. What is the difference between a virus and a worm? Provide real-world examples of each and discuss the unique characteristics that distinguish them.
3. What is the difference between steganography and cryptography, and how do they contribute to data security?
4. Discuss SQL injection and the various countermeasures that organizations can implement to prevent such attacks. Emphasize the significance of database security.
5. Explain the different buffer overflow attacks that can be employed by cybercriminals. Provide examples and discuss the potential risks associated with these attacks.
6. What are the key components of a wireless network, and how can these components be secured against various threats?

**UNIT -5**

1. What is meant by "insider threat"? How does it affect organizations?
2. Are there costs associated with cybercrimes? What are the typical components of those costs? Do you see a "pattern" in those costs? Explain.
3. Describe incident response life cycle along with the typical activities involved in each of the phases.
4. Why should organization's media and information assets be protected?
5. What is an "endpoint" in a corporate network? Why is endpoint security important?
6. Can "cookies" impact data security and personal security? Explain how.