

ASSIGNMENT -3

1. Describe the key differences between intrusion detection systems (IDS) and intrusion prevention systems (IPS).
2. Design a hypothetical network architecture for a medium-sized enterprise and outline how you would integrate both intrusion detection and prevention mechanisms. Consider factors such as placement of sensors, types of detection techniques (e.g., signature-based, anomaly-based), and strategies for blocking or mitigating identified threats.
3. Analyze the impact of social engineering attacks on individuals and organizations, considering factors such as financial losses, reputational damage, and compromised data security.
4. Compare and contrast the characteristics of malware and ransomware attacks, including their methods of propagation, objectives, and potential consequences for victims. Evaluate the effectiveness of proactive measures such as regular software updates, antivirus software, and user awareness training in preventing and mitigating the impact of these types of cyber threats.
5. How has the IT Act of 2000, along with its subsequent amendments, shaped the legal landscape for addressing cyber-crime and offenses in India? Discuss the key provisions of the Act related to cyber-security and examine their effectiveness in prosecuting cyber-criminals and protecting individuals and organizations from cyber threats.