# CYBER SECURITY ASSIGNMENT QUESTION

## DAY 45

**1. Explain the difference between passive and active packet sniffing techniques and discuss their implications for network security.**

**2. Describe how packet sniffing can be used to discover network vulnerabilities and potential security risks.**

**3. Discuss the importance of encryption in defending against packet-sniffing attacks and explain how techniques like SSL/TLS can mitigate the risk of data interception.**

**4. Develop a Python script to detect packet-sniffing activities on a network using the Scapy library and ICMP (Internet Control Message Protocol) packets.**

**5. Design a comprehensive mitigation plan to defend against packet-sniffing attacks, including network segmentation, encryption, and intrusion detection systems.**