CLO # 1 (Questions 1): Evaluate the computer and data security needs of an organization, and be able to assess the current security landscape, including the nature of threats, the status of common vulnerabilities, and the likely consequences of security failures..

Question #1 Provide precise and short answers to the following questions. [2 x 4 =8 Marks]

A. How do cryptographic protocols such as SSL/TLS use cryptographic techniques to secure online communications?

B. If Bob receives a message encrypted with his public key, can he be sure it came from Alice?

C. If a message is encrypted using the recipient's public key, who can decrypt it and what does that guarantee about the message?

D. Describe a real-world scenario where combining both symmetric and asymmetric encryption (i.e., hybrid encryption) would be necessary.

CLO # 2 (Questions 2): Understand the flow of information in the modern world and be able to recognize and mitigate threats at every stage, e.g. network, coding and software layers; to this end, setting up and running appropriate tools and environments.

Question # 2: Read the given scenario carefully and identify the appropriate web application security risk from the OWASP Top 10 (2021). **Identify** and write the exact name of the risk as listed by OWASP. **[1x8=8 Marks]**

A. A web application uses weak passwords, and a user's account is compromised. What are the potential risks, and how can this vulnerability be addressed?

B. A web server's default configuration includes a directory that contains sensitive configuration files. What are the potential risks, and how can this vulnerability be addressed?

C. A web application allows users to enter product names and descriptions in a search box. An attacker enters a malicious script in the search box, and when another user uses the search box, the malicious script executes in their browser. What type of vulnerability is this, and how can it be prevented?

D. A web application allows users to view their own orders and edit their profile information. However, an attacker discovers that by manipulating the URL, they can access other users' order details and modify their profiles. What type of vulnerability is this, and how can it be mitigated?

E. A web application uses an outdated encryption algorithm to protect sensitive data. What are the potential risks, and how can this vulnerability be addressed?

F. A banking application uses session tokens to track logged-in users. These tokens are stored in the URL and can be intercepted or guessed easily. The application also does not expire sessions promptly after logout or timeout.

G. An API endpoint used by a mobile app accepts JSON input and uses an insecure deserialization method to convert data into objects. An attacker manipulates the input to execute arbitrary code on the server.

H. The application integrates several third-party libraries, including one with a known vulnerability that hasn't been updated in two years. No dependency scanning is in place.

CLO # 4 (Question 3 and 4): Identify security tools and hardening techniques.

Question # 3. Read each of the following scenarios carefully. For each one, identify the function (e.g., Govern , Identify, Protect, Detect, Respond, Recover), the exact name of category it belongs to and the subcategory code from the NSIT CSF 2.0 framework. **[1 x 8 = 8 Marks]**

A. A startup conducts an internal review to document and classify all IT assets and their roles within the organization. Identify

B. An enterprise develops and enforces a policy requiring strong passwords, screen lockouts, and automatic logoff features. Protect

C. An organization updates its supplier contracts to include specific cybersecurity requirements and right-to-audit clauses.

D. A hospital maintains cloud backups and regularly tests restoration processes to ensure business continuity during disasters. Protect detect

E. An IT administrator configures access permissions, so employees only have access to systems relevant to their roles.

F. After detecting unusual system behavior, the IT team isolates the affected system and notifies stakeholders within 15 minutes.

G. An organization regularly evaluates its internal capabilities and resources to understand if it can meet emerging cybersecurity threats and operational demands. detect

H. A university's IT department has configured their systems to automatically flag unusual data transfer patterns, such as a sudden spike in outbound traffic late at night. protect

Question# 4: Answer the following questions with reference to Nmap tool. **[1x 6 = 6 Marks]**

A. How can you reduce the likelihood that a standard firewall/IDS would detect your Nmap activity?

B. Which command is used to tell Nmap explicitly which network interface to use and not to expect to receive a ping reply.

C. You're scanning a network where you don't have root privileges. Which TCP scan type should you use and why?

D. You use a NULL scan on a network and receive many "open|filtered" results. What does this tell you?

E. You're scanning a system that logs all connection attempts. Which scan should you avoid?

F. Which type of scan is likely to go undetected by most IDS systems?