3/31

0212N905

Candidate's Seat No :________

B.Sc Sem.-5 Examination

SE 305

Computer Science

Time : 2-30 Hours] **December-2024** **[Max. Marks : 70**

Q1(A) Explain the concept of "Defence in Depth" in computer security. (7)

Q1(B) What is the difference between symmetric and asymmetric encryption? Illustrate with examples. (7)

OR

Q1(A) Discuss the role of firewalls in network security. What are the different types of firewalls? (7)

Q1(B) What are the key principles of access control in computer security? Discuss each principle briefly. (7)

Q2(A) If a user's password is stored in an insecure manner and the database is compromised, what are the implications for the user, and what measures can be taken to prevent such a situation? (7)

Q2(B) Explain the principle of least privilege and its importance in computer security. (7)

OR

Q2(A) What are the common types of malware, and how do they differ from each other? (7)

Q2(B) Describe the role of firewalls in network security. What are the differences between hardware and software firewalls? (7)

Q3(A) Discuss the importance of encryption in data security. Provide examples of encryption standards used in practice. (7)

Q3(B) Can a system be secure if it is user-friendly? Discuss the relationship between usability and security in system design. (7)

OR

Q3(A) What are the three core principles of information security? Explain each principle in detail. (7)

Q3(B) What is social engineering in the context of cybersecurity? Provide examples of techniques used in social engineering attacks. (7)

Q4(A) A company implemented a new security protocol that requires all employees to change their passwords every month. However, they found that employees started using simpler passwords or writing them down. Discuss the potential security issues this could create and suggest alternative strategies for effective password management. (7)

Q4(B) Discuss the differences between symmetric and asymmetric encryption. (7)

OR

Q4(A) If a user has a strong password but shares it with a colleague, is the account still secure? Explain your answer. (7)

Q4(B) If a company has implemented robust security measures such as firewalls, encryption, and employee training, can it be considered fully secure? Discuss the concept of "security is a process, not a product." and explain why it's

N905-2

critical for organizations to continuously assess and improve their security posture. (7)

Q5 MCQ Attempt any seven out of twelve.(2 Marks each) **(14)**

1) What is the primary goal of cyber security?
A) To prevent all cyber attacks
B) To manage risks associated with cyber threats
C) To eliminate all malware
D) To enforce legal penalties for cyber crimes

2) Which of the following is considered a form of social engineering?
A) Phishing B) SQL Injection C) Denial of Service D) Firewall Breach

3) In the context of cyber security, what does the acronym "CIA" stand for?
A) Central Intelligence Agency
B) Confidentiality, Integrity, Availability
C) Cyber Information Awareness
D) Critical Infrastructure Assurance

4) Which of the following is NOT a characteristic of a strong password?
A) Contains both uppercase and lowercase letters
B) Is at least 8 characters long
C) Includes personal information such as a birthdate
D) Has a mix of letters, numbers, and symbols

5) What type of malware is designed to replicate itself and spread to other computers?
A) Virus B) Worm C) Trojan Horse D) Ransomware

6) Which of the following practices is most effective in preventing unauthorized access to sensitive data?
A) Regularly changing passwords
B) Using a firewall
C) Implementing two-factor authentication
D) Encrypting data

7) What is the purpose of a Denial of Service (DoS) attack?
A) To steal sensitive information
B) To gain unauthorized access to systems
C) To disrupt services and make them unavailable
D) To install malicious software on a victim's computer

8) Which of the following describes a “zero-day vulnerability”?
A) A security flaw that has been publicly disclosed
B) A vulnerability that is patched on the same day it is discovered
C) A newly discovered vulnerability that has no available fix
D) A vulnerability that exists for more than a year

9) In cyber security, what is "phishing"?
A) Sending emails that appear to be from reputable sources to steal personal information
B) Hacking into a network to steal data
C) Overloading a server with requests
D) Using spyware to monitor user activity

10) Which type of attack involves intercepting and altering communications between two parties without their knowledge?
A) Man-in-the-Middle (MitM)
B) Ransomware
C) Phishing
D) SQL Injection

11) What is the function of a VPN (Virtual Private Network)?

N905-3

A) To protect against viruses
B) To encrypt internet traffic and provide anonymity
C) To create backups of data
D) To manage firewall settings

12) Which of the following is a common indicator of a phishing attempt?
A) A request for urgent action
B) An email from a known contact
C) A misspelled website URL
D) Both A and C

ALL THE BEST