[This question paper contains 2 printed pages.]

Your Roll No.....

L

Sr. No. of Question Paper : 5320

Unique Paper Code : 2344000031

Name of the Paper : Information Security

Name of the Course : **B.Sc. (H) CS (GE)**

Semester : VIII

Duration : 3 Hours

Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **Section A** is compulsory.
3. Attempt any **Four** Questions from **Section B**.
4. Part of a question must be answered together.

Section A

1 (a) Consider the following code fragment: **(2)**

```
#include <stdio.h>
#include <string.h>

int main() {
    char buffer[10];
    printf("Enter a string: ");
    gets(buffer);
    printf("You entered: %s\n", buffer);
    return 0;
}
```

Can a buffer overflow occur in this program? Give suitable explanation.

(b) Define popular password attack and specific account attack. Suggest suitable countermeasures to prevent each. **(4)**

(c) Explain inband SQL injection attack. Also, discuss its types. **(4)**

(d) List the characteristics used by firewalls to enforce a security access control policy. **(4)**

(e) Explain the different phases of a computer virus. **(4)**

(f) What does disruption mean in the context of system security. Mention the types of threat actions that can cause disruption? **(4)**

(g) List any four major security concerns for mobile devices. **(4)**

P.T.O.

(h) Define a digital envelope. Describe the process of creating a digital envelope. **(4)**

Section B

2 (a) Compare and contrast Discretionary Access Control (DAC) and Role-Based Access Control (RBAC). Describe the various RBAC reference models. **(10)**

(b) Explain Public Key Infrastructure X.509 (PKIX) model. **(5)**

3 (a) Differentiate between the following: **(10)**

(i) Fixed database role and Fixed server roles
(ii) User mode rootkit and Kernel mode rootkit
(iii) SYN spoofing attack and SYN flooding attack
(iv) Public cloud and Private cloud
(v) Low interaction honeypot and High interaction honeypot

(b) Discuss any five fundamental security design principles. **(5)**

4 (a) Describe various types of network scanning strategies that a worm uses to locate vulnerable host. Also, discuss any two major computer worms from history. **(8)**

(b) Discuss the key principles of writing a safe program code. Explain how input validation, type safety, and memory management practices prevent common software vulnerabilities. Illustrate with a example code. **(7)**

5 (a) Describe any four cloud-specific security threats. Also, for each threat give its suitable countermeasures. **(8)**

(b) Define injection attack. Also, discuss its major variants with the help of suitable examples. **(7)**

6 (a) Describe the main components of Identity, Credential, and Access Management (ICAM). **(8)**

(b) Explain one way hash function. List the requirements for a secure hash function. **(7)**

7 (a) Differentiate between firewall and honeypot in network security. Also, discuss the various types of firewalls. **(8)**

(b) List the main components of a wireless network. Why is wireless security considered a major concern compared to wired security? **(7)**