Seat No.	

SW-339

Total No. of Pages : 03

B.C.A. (Part-III) (Semester-V) (CBCS)

Examination, March 2024.

I.T. Security

Sub. Code : 88234

Day and Date: Thursday, 28-03-2024 **Total Marks: 70**

Time: 10.30 a.m. to 01.30 p.m.

Instructions:
1) **Q.1 and Q.6 are compulsory.**
2) **Attempt ANY THREE questions from Q.2 to Q.5.**
3) **Figures to the right indicate full marks.**

Q.1 a) Choose the correct answer in each of the following questions. **(10)**

1) Which of the following is NOT a common security threat to IT systems?
   (A) Malware
   (B) Social engineering
   (C) Frequent software updates
   (D) Phishing attacks

2) How does spoofing differ from phishing?
   (A) Spoofing involved flooding a system or network with traffic, while phishing involves intercepting network traffic.
   (B) Spoofing involves impersonating legitimate users, while phishing involves sending fraudulent emails or messages.
   (C) Spoofing involves creating fake websites, while phishing involves monitoring network traffic.
   (D) Spoofing involves modifying data packets, while phishing involves creating fake websites.

3) What is the primary motivation behind most cyber-attacks?
   (A) Financial gain
   (B) Personal entertainment
   (C) Academic research
   (D) Political activism

4) What is the purpose of implementing data backup and recovery procedures in IT security?
   (A) To prevent unauthorized access to IT systems and networks
   (B) To encrypt sensitive data transmissions
   (C) To ensure that data can be restored in the event of data loss or corruption
   (D) To control access to IT resources based on user roles and permissions

5) What is the primary function of a malware detector?
   (A) To create and spread malware across networks
   (B) To analyze and identify malicious software on a system or network
   (C) To encrypt sensitive data transmissions
   (D) To limit access to specific IP addresses

6) Which of the following is a proactive approach to malware detection?
   (A) Signature-based detection
   (B) Heuristic analysis
   (C) Behavior-based detection
   (D) Limiting access to specific IP addresses

7) What is the primary purpose of biometric verification in IT security?
   (A) To encrypt sensitive data transmission
   (B) To limit access to specific IP addresses
   (C) To authenticate individuals based on unique biological characteristics
   (D) To monitor physical access to IT facilities

8) Which of the following biometric characteristics is NOT commonly used for verification purposes?
   (A) Hair color
   (B) Retina scan
   (C) Iris pattern
   (D) Voice recognition

9) What dimension of information security focuses on ensuring that security measures are compliant with laws, regulations and industry standards?

(A) Compliance (B) Confidentiality

(C) Integrity (D) Availability

10) Which of the following is NOT a common type of malware detected by malware detectors?

(A) Viruses (B) Trojans

(C) Encryption algorithms (D) Ransomware

b) Attempt ANY TWO questions. **(10)**

1) Explain challenges of IT Act.

2) What is Trojan horse?

3) Describe malware in detail.

Q.2 Describe need and significance of IT security. **(10)**

Q.3 What is security threat? Explain different types of security threats. **(10)**

Q.4 What is IT security control measure? Explain biometric verification in detail. **(10)**

Q.5 Explain IT Act, 2000 along with its features. **(10)**

Q.6 Write notes. (Any four) **(20)**

a) Challenges of IT Security

b) Cyber-crimes under Information Technology Act, 2000

c) Digital signature and certificate

d) IT assets

e) Sources of threat

f) Multilevel authentication