No. of Printed Pages : **8**

A10.3-R5 Information Security Management

DURATION : 03 Hours **MAXIMUM MARKS : 100**

OMR Sheet No. :						

Roll No. : | | | | | | |

Answer Sheet No. : | | | | | | |

Name of Candidate : _____ **; Signature of Candidate :** _____

INSTRUCTIONS FOR CANDIDATES :

- Carefully read the instructions given on Question Paper, OMR Sheet and Answer Sheet.
- Question Paper is in English language. Candidate has to answer in English language only.
- There are **TWO PARTS** in this Module/Paper. **PART ONE** contains **FOUR** questions and **PART TWO** contains **FIVE** questions.
- **PART ONE** is Objective type and carries **40** Marks. **PART TWO** is Subjective type and carries **60** Marks.
- **PART ONE** is to be answered in the **OMR ANSWER SHEET** only, supplied with the question paper, as per the instructions contained therein. **PART ONE** is **NOT** to be answered in the answer book for **PART TWO**.
- Maximum time allotted for **PART ONE** is **ONE HOUR**. Answer book for **PART TWO** will be supplied at the table when the Answer Sheet for **PART ONE** is returned. However, Candidates who complete **PART ONE** earlier than one hour, can collect the answer book for **PART TWO** immediately after handing over the Answer Sheet for **PART ONE** to the Invigilator.
- **Candidate cannot leave the examination hall/room without signing on the attendance sheet and handing over his/her Answer Sheet to the invigilator. Failing in doing so, will amount to disqualification of Candidate in this Module/Paper.**
- After receiving the instruction to open the booklet and before answering the questions, the candidate should ensure that the Question Booklet is complete in all respects.

DO NOT OPEN THE QUESTION BOOKLET UNTIL YOU ARE TOLD TO DO SO.

PART ONE

(Answer ALL Questions; each question carries ONE mark)

1. Each question below gives a multiple choice of answers. Choose the most appropriate one and enter in the "OMR" answer sheet supplied with the question paper, following instructions therein. **(1x10)**

1.1 Which of the following function is not performed by network layer of OSI model ?

(A) Congestion Control

(B) Routing

(C) Inter-networking

(D) Error control

1.2 Which transport protocol is connection-oriented ?

(A) TCP

(B) UDP

(C) Both TCP and UDP

(D) Neither TCP nor UDP

1.3 Which of the following cyber attacks typically employs a network of compromised devices to flood a target system with a high volume of traffic, causing it to become inaccessible to legitimate users ?

(A) Phishing attack

(B) SQL Injection attack

(C) DDoS attack

(D) Ransomware attack

1.4 Which encryption method involves using two keys, one for encryption and another for decryption, and is commonly employed in secure communication protocols like HTTPS ?

(A) Symmetric Encryption

(B) Asymmetric Encryption

(C) Hashing

(D) Transposition Encryption

1.5 Which type of firewall operates at the application layer of the OSI model ?

(A) Packet Filtering Firewall

(B) Proxy Firewall

(C) Stateful Inspection Firewall

(D) Next-Generation Firewall

1.6 In SQL injection attacks, what is the primary objective of injecting malicious SQL code into a vulnerable database ?

(A) Stealing encrypted passwords

(B) Extracting sensitive information

(C) Modifying server configuration files

(D) Generating fake log entries

1.7 The Information Technology Act of 2000 in India primarily deals with which of the following aspects ?

(A) Data Protection and Privacy

(B) Cyber crime and Electronic Commerce

(C) Intellectual Property Rights

(D) Telecommunication Regulations

1.8 In cyber forensics, what is the main objective of evidence preservation ?

(A) To prevent unauthorized access to the crime scene

(B) To ensure the integrity and authenticity of digital evidence

(C) To gather evidence for use in civil litigation

(D) To expedite the investigation process

1.9 In the context of cybersecurity, what does a buffer overflow vulnerability typically involve ?

(A) Unauthorized access to a system's administrator privileges

(B) Interception of network traffic between a client and a server

(C) Execution of arbitrary code by overwriting memory beyond the bounds of a buffer

(D) Manipulation of cryptographic algorithms to weaken encryption

1.10 What does NIDS stand for in the context of cyber security ?

(A) Network Interface Detection System

(B) Network Intrusion Detection System

(C) Network Information Discovery System

(D) Network Infiltration Defense System

2. Each statement below is either TRUE or FALSE. Choose the most appropriate one and enter your choice in the "OMR" answer sheet supplied with the question paper, following instructions therein. **(1x10)**

2.1 Subnetting allows a network administrator to divide an IP network into smaller sub-networks for better organization and efficiency.

2.2 Phishing is a type of social engineering attack that exploit any programmable device, service or network.

2.3 Digital Signature hashes the document or message and encrypts the hash with the sender's private key.

2.4 The AES Encryption algorithm is a symmetric block cipher algorithm with a block size of 128 bits.

2.5 Cross-Site Scripting is a security vulnerability that allows attackers to gain unauthorized access to various sites.

2.6 Cyber forensics is a process of extracting data as proof for a crime which involves electronic devices.

2.7 Eramba is a cloud-based file storage service.

2.8 Host-based Intrusion Prevention System (HIPS) protects your system from malware and unwanted activity attempting affect your computer.

2.9 The primary role of SSL (Secure Sockets Layer) is to provide a secure and encrypted communication channel between a client and a server over the internet.

2.10 The Microsoft Security Baseline is a platform for managing user authentication and access control in Microsoft environments.

3. **Match words and phrases in column X with the closest related meaning / words(s) / phrase(s) in column Y. Enter your selection in the "OMR" answer sheet supplied with the question paper, following instructions therein.** **(1x10)**

X		Y	
3.1	VLAN	**A.**	network diagnostics
3.2	ICMP	**B.**	Virtual Local Area Network
3.3	hash function	**C.**	connects two or more packet-switched networks
3.4	router	**D.**	converts a numerical input value into another compressed numerical value
3.5	NIPS	**E.**	preventing intrusion attempts in real-time
3.6	HIPS	**F.**	Analyzing network traffic for suspicious activities or security breaches.
3.7	non-profit organization to help protecting web applications from cyber attacks	**G.**	Nessus
3.8	remote security scanning tool	**H.**	*OWASP*
3.9	Domain name disputes are resolved by	**I.**	Volatile Local Area Network
3.10	volatile evidence	**J.**	Data that is easily tampered
		K.	evidence that may be lost when a system is powered off or restarted.
		L.	Monitoring unauthorized access or malicious behavior.
		M.	UDRP

4. Each statement below has a blank space to fit one of the word(s) or phrase(s) in the list below. Choose the most appropriate option, enter your choice in the "OMR" answer sheet supplied with the question paper, following instructions therein. (1x10)

A.	two-octet number	**B.**	session hijack	**C.**	Chain of Custody	**D.**	Host ID
E.	four-octet number	**F.**	SNMP	**G.**	Static routing	**H.**	cipher
I.	Apache Server	**J.**	IDS	**K.**	ICMP	**L.**	UTMTMG
M.	HMAC						

4.1 _____ is used to track the physical and digital evidence collected during an investigation.

4.2 Intercepting and taking control of an ongoing session between a user and a server is called as _____.

4.3 The _____ is used to detect and mitigate security threats such as malware, viruses, and intrusion attempts.

4.4 _____ are used to monitor and analyze network traffic for suspicious activities or security breaches.

4.5 Many communication and transfer protocols use _____ including HTTPS, SFTP and FTPS to check data integrity and authentication of parties.

4.6 A _____ is a method used in cryptography for performing encryption or decryption.

4.7 The broadcast address of a subnet is determined by setting all the remaining bits of the _____ to '1'.

4.8 A subnet mask is a _____ used to identify the network ID portion of a 32-bit IP address.

4.9 _____ organizes and sends data from various devices for network monitoring with fault identification and isolation.

4.10 _____ is a method where network administrators manually configure the routing table with fixed routes.

PART TWO

(**Answer any FOUR questions**)

5. (a) Explain the concept of subnetting. Do mention its advantages and disadvantages.

(b) Discuss the significance of following protocols with respect to OSI model- TCP, UDP, ICMP and SNMP. **(7+8)**

6. (a) Differentiate between the following types of cyber attacks - DDOS, Phishing, SQL Injection, Cross Site Scripting.

(b) Explain RSA algorithm in detail with example. **(8+7)**

7. (a) Explain the role of hash function. Discuss any two popular hash algorithms.

(b) Write short notes on the following :

(i) Digital Signature

(ii) Role of Cyber Forensics **(8+7)**

8. (a) What is the purpose of security auditing ? How it helps in avoiding security risks ?

(b) Explain the purpose of X.500, X.509 standards.

(c) Differentiate between Inter Domain Routing, Inter VLAN routing and Static Routing. **(5+5+5)**

9. (a) Differentiate between SSL and TLS. Explain their significance with respect to cryptography.

(b) Discuss the significance of firewalls. Explain its various types and its usage areas. **(7+8)**

- o O o -

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK