No. of Printed Pages : **8**

A10.3-R5.1 : 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 the 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 the instructions therein. (1x10)

1.1 Which OSI layer is responsible for establishing, managing and terminating sessions between two communicating hosts ?

(A) Physical (B) Data Link
(C) Session (D) Application

1.2 Which device operates at Layer 2 (Data Link layer) of the OSI model and is used to reduce collisions in a network by separating collision domains ?

(A) Hub (B) Switch
(C) Router (D) Repeater

1.3 In CIDR (Classless Inter-Domain Routing), what is the primary advantage compared to traditional classful addressing ?

(A) It increases the number of available IPv4 addresses
(B) It allows subnetting only within Class B networks
(C) It allows for more efficient allocation of IP addresses
(D) It reduces the number of routers required in a network

1.4 Which routing protocol uses the Administrative Distance value to choose between multiple routes to a destination ?

(A) RIP (B) OSPF
(C) BGP (D) EIGRP

1.5 Which cryptographic algorithm is a symmetric key encryption method that divides data into blocks and uses a 56-bit key for encryption ?

(A) AES (B) DES
(C) RSA (D) ECC

1.6 Which of the following is an example of a DDoS (Distributed Denial of Service) attack ?

(A) An attacker sends multiple malformed packets to a server
(B) An attacker uses multiple systems to flood a target server with traffic
(C) An attacker intercepts and modifies data in transit
(D) An attacker guesses a user's password and logs into their account

1.7 In IPv6, what is the main purpose of the Neighbor Discovery Protocol (NDP) ?

(A) To resolve MAC addresses from IP addresses
(B) To enable end-to-end communication in a mesh topology
(C) To discover routers, resolve IP addresses, and perform stateless address auto-configuration
(D) To authenticate packets using cryptographic signatures

1.8 Which of the following accurately describes Network Address Translation (NAT) overload or PAT (Port Address Translation) ?

(A) It assigns each internal device a unique public IP address

(B) It maps multiple private IP addresses to a single public IP address by using different port numbers

(C) It allows for the translation of IPv4 addresses to IPv6

(D) It requires static mapping between internal and external IP addresses

1.9 Which type of cyber-attack specifically targets vulnerabilities in web applications, such as by injecting malicious code into form fields ?

(A) Cross-site scripting (XSS)

(B) Buffer overflow

(C) Phishing

(D) Denial of Service (DoS)

1.10 Which of the following tools is commonly used for vulnerability scanning in network security, particularly for identifying known weaknesses in systems and applications ?

(A) Wireshark (B) Nessus

(C) Metasploit (D) Snort

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 the instructions therein. (1x10)

2.1 The OSI model has seven layers, and the Transport layer is responsible for error correction and flow control.

2.2 In a Class B IPv4 address, the first two octets represent the network portion, and the default subnet mask is 255.255.255.0.

2.3 RIP (Routing Information Protocol) uses a hop count metric and supports a maximum hop count of 15 before a route is considered unreachable.

2.4 The MD5 cryptographic hash algorithm generates a 256-bit hash value and is still widely recommended for cryptographic purposes.

2.5 Under the IT Act 2000 (amended in 2008), digital signatures are legally recognized, and any electronic document signed with a digital signature is admissible as evidence in Indian courts.

2.6 A VLAN (Virtual Local Area Network) can only operate within a single switch, and it cannot span multiple switches.

2.7 The Diffie-Hellman key exchange is a method used for securely exchanging cryptographic keys over a public channel without the need for prior shared secrets.

2.8 A Distributed Denial of Service (DDoS) attack uses multiple systems to overwhelm the target network or application with traffic, and this is classified as a "DoS" attack under the IT Act.

2.9 Cross-Site Scripting (XSS) is a web application vulnerability where malicious scripts are injected into a website and executed in the user's browser, often by passing Same-Origin Policy (SOP).

2.10 Section 66F of the IT Act 2000 deals with cyber terrorism, where unauthorized access to a computer resource leading to severe damage is treated as an offense.

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

X		Y	
3.1	Firewall	**A.**	Manipulating individuals to gain confidential info
3.2	RIP	**B.**	Unauthorized access to a secure system
3.3	Malware	**C.**	Authorized simulated attack on a system
3.4	Bridging	**D.**	Converts data into a coded format
3.5	Hash Function	**E.**	Ensures data integrity and authenticity
3.6	Social Engineering	**F.**	Protocol for secure email
3.7	Data Encryption	**G.**	Connects multiple networks at Layer 2
3.8	Penetration Testing	**H.**	Software designed to harm or exploit devices
3.9	Tokenization	**I.**	Malicious attempt to steal sensitive information
3.10	Breach	**J.**	Determines best path for data
		K.	Measures network traffic flow
		L.	Produces a fixed-size output from input data
		M.	Replaces sensitive data with unique identifiers

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

A.	Stateful	**B.**	Network Address Translation (NAT)	**C.**	Advanced Encryption Standard (AES)	**D.**	Conduit
E.	Neighbor Discovery Protocol (NDP)	**F.**	Steganography	**G.**	Diffie-Hellman	**H.**	Unauthorized access
I.	SQL Injection	**J.**	RSA	**K.**	Denial of Services (DoS)	**L.**	Subnet
M.	authorized access						

4.1 Under the IT Act, an intermediary is not liable for third-party information, data, or communication if the intermediary acts as a mere _____ and does not initiate the transmission.

4.2 The primary purpose of _____ is to translate private IP addresses to public IP addresses in order to conserve global IP address space.

4.3 A _____ firewall filters traffic based on connection state and tracks the state of network connections.

4.4 _____ is a symmetric encryption algorithm that operates on fixed-size blocks of data and uses a key size of 128, 192, or 256 bits.

4.5 In a sub netted network, a _____ mask is used to divide an IP address into network and host portions.

4.6 The Diffie-Hellman algorithm is used for _____ key exchange over an insecure channel.

4.7 _____ is a cyber-attack in which an attacker inserts malicious SQL queries into input fields, leading to unauthorized access to a database.

4.8 _____ is an example of a network-layer protocol used in IPv6 to handle address resolution and neighbour discovery.

4.9 Section 43 of the IT Act penalizes individuals who cause damage to a computer or computer system by _____ without the owner's permission.

4.10 _____ is a process of hiding data within other non-secret data to prevent detection of the hidden information.

PART TWO

(Answer any FOUR questions)

5. (a) Explain the working principles of Layer 2 (Data Link Layer) and Layer 3 (Network Layer) devices, such as bridges, switches, and routers. Compare their functions, particularly in relation to VLANs, inter-VLAN routing, and Network Address Translation (NAT).

(b) Explain the principles of error detection and correction techniques, including parity checks, Hamming code, and Cyclic Redundancy Check (CRC). For each technique, illustrate with examples how errors are detected and corrected during data transmission.

(7+8)

6. (a) Discuss the importance of web and mobile application security in modern IT infrastructures. Explain the fundamental principles of web and mobile application security, focusing on common vulnerabilities (e.g., SQL injection, cross-site scripting, insecure mobile APIs) and how organizations can secure their applications through secure coding practices, regular vulnerability scanning, and penetration testing.

(b) Discuss the Diffie-Hellman key exchange protocol and its importance in secure communication. Explain the mathematical principles behind it, how it enables two parties to securely exchange cryptographic keys over an insecure channel, and how it is combined with other cryptographic techniques in modern protocols like TLS (Transport Layer Security).

(7+8)

7. (a) Explain the mechanisms behind Buffer overflow and session hijacking attacks, focusing on how buffer overflow exploits memory management and how session hijacking manipulates session IDs. Discuss secure coding practices and mitigation techniques (e.g., memory management safeguards, secure session handling) to protect against these vulnerabilities.

(b) Explain the difference between Network-based Intrusion Detection Systems (NIDS) and Host-based Intrusion Detection Systems (HIDS). How do Intrusion Prevention Systems (IPS) differ from Intrusion Detection Systems (IDS) ?

(10+5)

8. (a) Describe the audit planning process, including the scope, pre-audit planning, and data gathering techniques. How does defining the audit scope impact the overall audit process, and what are the key considerations when gathering evidence for an IT/IS audit ?

(b) Explain the key provisions of the Information Technology Act 2000, as amended in 2008, focusing on the legal recognition of electronic records, digital signatures, and cybercrimes. Discuss how the amendments have strengthened the legal framework for handling cybercrimes, such as hacking and identity theft, and the protection of digital information in India.

(7+8)

9. (a) Explain the CIA Triad (Confidentiality, Integrity, Availability) and its role in maintaining the security of information systems. For each component, provide real-world examples of threats that can compromise it (e.g., data breaches, ransomware, DDoS attacks) and the counter measures that can be implemented to mitigate those threats.

(b) Discuss the processes involved in the identification, preservation, and seizure of digital evidence in a cybercrime investigation. How do investigators ensure the integrity and authenticity of digital evidence during acquisition ?

(7+8)

- o O o -

SPACE FOR ROUGH WORK