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 the instructions therein. (1x10)

1.1 The private key is used to _____.

(A) Decrypt only

(B) Encrypt only

(C) Decrypt as well as encrypt

(D) None of the above

1.2 The intent of a _____ is to overkill the targeted server's bandwidth and other resources of the target website.

(A) DoS attack

(B) Phishing attack

(C) Website attack

(D) MiTM attack

1.3 A Denial of Service (DoS) attack meant to shut :

(A) A machine only.

(B) A network only.

(C) A machine or network.

(D) None of the above.

1.4 The role of a VPN is to create a _____ connection between two computers over a _____ network.

(A) Secure, Private

(B) Un-secure, Private

(C) Secure, Public

(D) Un-secure, Public

1.5 Class 'C' IP addresses use _____ bits for host ID.

(A) 8

(B) 16

(C) 24

(D) 32

1.6 Which of the following is the range of class A public IPv4 ?

(A) 0.0.0.0 to 223.255.255.255

(B) 0.0.0.0 to 192.0.0.0

(C) 0.0.0.0 to 127.255.255.255

(D) 0.0.0.0 to 128.0.0.0

1.7 If end to end connections, is done at a network or IP level, and if there are N hosts, then what is the number of keys required ?

(A) N

(B) N/2

(C) N(N-1)/2

(D) N(N+1)/2

1.8 Communication between end systems is encrypted using a key, often termed as _____.

(A) Session key

(B) Section key

(C) Line key

(D) Temporary key

1.9 SSL stands for _____.

(A) Secure Sockets Layer

(B) Socket Secure Layer

(C) Session Secure Layer

(D) Socket Session Layer

1.10 Machine that places the request to access the data, is generally termed as _____.

(A) Resource Machine

(B) Intelligent Machine

(C) Server Machine

(D) Client Machine

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 In addition to being a data sublanguage, SQL is also a programming language, like COBOL.

2.2 The SQL keyword MODIFY is used to change the structure, properties or constraints of a table.

2.3 ANSI standard SQL uses the symbol "%" to represent a series of one or more unspecified characters.

2.4 In an SQL query, FROM SQL keyword is used to specify the names of tables to be joined.

2.5 Intrusion Prevention System (IPS) instantly blocks or allows network traffic, based on the nature of traffic.

2.6 An Intrusion Detection System (IDS) only identifies potential threats, while an Intrusion Prevention System (IPS) not only identifies but also takes action.

2.7 FTP is used to receive email.

2.8 POP3 protocol is used to fetch e-mail from a mailbox.

2.9 UDP is an unreliable, connectionless transport layer protocol.

2.10 A TCP transmitter normally interprets three duplicate ACKs to mean that, while data packets have been received out of order, all data is successfully being delivered.

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	PDU	**A.**	Bloodstain
3.2	Session key is used for electronic funds transfer and point of sale applications	**B.**	File-Server system
3.3	Divide (HAPPY)26 by (SAD)26. We get quotient	**C.**	Microsoft-IIS
3.4	Dividing (11001001) by (100111) gives remainder	**D.**	110
3.5	The estimated computations required to crack a password of 6 characters from the 26 letter alphabet is	**E.**	8031810176
3.6	_____ provides an interface to which a client can send a request to perform an action, in response, to server executes the action and sends back results to the client.	**F.**	Topology
3.7	_____is not an open source web server.	**G.**	Bus
3.8	Physical Forensics Discipline includes	**H.**	Protocol Data Unit
3.9	Physical or logical arrangement of network is _____	**I.**	Computer - Server System
3.10	_____ topology requires a multipoint connection.	**J.**	308915776
		K.	111
		L.	KD
		M.	PIN-encrypting key

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.	Software	**B.**	Hardware	**C.**	Ring	**D.**	HTTP Flooding
E.	TCP, UDP	**F.**	Trash	**G.**	N(N-1)/2	**H.**	N(N+1)/2
I.	UDP Flooding	**J.**	Frames	**K.**	N+1	**L.**	Firewall
M.	WAN						

4.1 Data communication system spanning states, countries or the whole world is _____.

4.2 In TDM, slots are further divided into _____.

4.3 _____ links are there for N nodes in the mesh topology.

4.4 _____topology uses the token passing algorithm.

4.5 _____ lines are required for the bus topology.

4.6 Deleted E-mails are stored in _____.

4.7 In computing, _____ is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.

4.8 A Computer virus is a _____.

4.9 Dynamic packet filter firewalls are the fourth-generation firewalls that work at _____.

4.10 _____ do not comes under network layer DoS flooding.

PART TWO

(Answer any FOUR questions)

5. (a) How does the risk-based auditing approach help in minimizing overall audit risk, and what are the key steps involved in performing risk assessments using open-source tools like Eramba or Simple Risk ?

(b) Explain how ISO27001 security toolkits aid in risk analysis and audit planning, and what role does a prepared audit questionnaire play in conducting a successful audit for ISO27001 standards ? **(7+8)**

6. (a) Explain the working of subnetting and how Classless Inter-Domain Routing (CIDR) is used in IP address management for IPv4 and IPv6, including the role of routing protocols like OSPF and EIGRP.

(b) How do the OSI and TCP/IP models differ in terms of their layers and associated protocols, and what roles do devices like switches, routers, and UTMs play in managing traffic across these layers ? **(7+8)**

7. (a) What are the key steps involved in the identification, preservation, and acquisition of digital evidence in cyber forensics, and how does the chain of custody process ensure the integrity of evidence during an investigation ?

(b). How do forensic tools assist in generating report findings related to disk imaging, email analysis, and tracing internet access, and what is the importance of proper documentation and report writing in the overall cyber forensics process ? **(7+8)**

8. (a) What are the common web application attacks, such as SQL injection and cross-site scripting, and how do mitigation techniques differ when addressing threats in web versus mobile applications and cloud environments ?

(b) How do hash functions like MD5, SHA-1, and HMAC contribute to data integrity in cryptographic systems, and what role do Public Key Infrastructures (PKI) and digital certificates play in securing communication protocols such as SSL, TLS and IPsec ? **(7+8)**

9. (a) How can wireless networks including Bluetooth and 802.11 standards, be secured against common vulnerabilities, and what role do network security tools like scanners and sniffers play in detecting and mitigating wireless threats ?

(b) How has the Information Technology Act 2000, as amended in 2008, addressed cyber crimes and data protection, and what are the legal implications for intermediaries regarding liability and harmful content on the internet ? **(7+8)**

- o O o -

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK