

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 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 Multiple object can be sent over a TCP connection between client and server in :

- (A) persistent http
- (B) nonpersistent http
- (C) both (A) and (B)
- (D) none of the mentioned

1.2 Which of the following layer is not present in TCP/IP model ?

- (A) application
- (B) presentation
- (C) transport
- (D) network

1.3 The Routing Information Protocol (RIP) is an intra domain routing based on which routing ?

- (A) distance vector
- (B) link state
- (C) path vector
- (D) distance code

1.4 Routers help in _____.

- (A) transmission of data between networks
- (B) connecting different devices using appropriate protocol
- (C) both (A) and (B)
- (D) neither (A) nor (B)

1.5 Packets in IPv4 layer are called _____.

- (A) datagrams
- (B) header length
- (C) code point
- (D) tunneling

1.6 Phishing is _____.

- (A) hacking a computer over internet
- (B) online theft
- (C) fraudulent attempt to obtain sensitive information
- (D) none of the above

1.7 What is malware ?

- (A) software that has some malicious purpose
- (B) software that is not functioning properly
- (C) software that damages your system
- (D) software that is not properly configured for your system

1.8 Security methods such as private encryption, VLANs and firewalls come under subject area :

- (A) accounting management
- (B) compliance
- (C) data privacy
- (D) all of the mentioned

1.9 In Which layer, vulnerabilities are directly associated with physical access to networks and hardware ?

- (A) physical
- (B) data-link
- (C) network
- (D) application

1.10 A Digital Signature is _____.

- (A) a bit string giving identity of a correspondent
- (B) a unique identification of a sender
- (C) an authentication of an electronic record by trying it uniquely to a key only a sender knows
- (D) an encrypted signature of sender

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 The Information Technology Act -2000 bill was passed by K. R. Narayanan.
- 2.2 Cyber forensics is an extracting data as digital evidence.
- 2.3 Accessing Wi-Fi dishonestly is a cyber-crime.
- 2.4 The Digital Signature Certificate under the IT Act, 2000 is issued by the Certifying Authority.
- 2.5 Unauthorized network access is a transport layer vulnerability.
- 2.6 Packet sniffers involve active receiver and passive receiver.
- 2.7 A cryptographic hash function must meet seven criteria.
- 2.8 A firewall protects denial of service attack.
- 2.9 A web server is a software program which serves the web pages requested by web users using a browser.
- 2.10 Non-persistent and persistent are the two primary classifications of cross-site scripting.

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	The most flexible network topology is	A.	128 bits
3.2	stream ciphers and block ciphers	B.	52 words
3.3	AES stands for	C.	RTT
3.4	In AES in which Round Sub keys are Generated from original key for each round	D.	Bus
3.5	What is the expanded key size of AES-192 ?	E.	key expansion
3.6	Which one is a type of cyber crime	F.	Abnormal Encryption Strategy
3.7	Which is security protocol based on digital certificates	G.	mitm
3.8	What type of attack uses a fraudulent server with a relay address ?	H.	Symmetric key cryptography
3.9	IPv6 addresses have a size of	I.	1024 bytes
3.10	The time taken by a packet to travel from client to server and then back to the client is called	J.	secure electronic transactions
3.11		K.	forgery
3.12		L.	Advance Encryption standard
		M.	Authorized Encryption Standard

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.	7	B.	67	C.	network layer	D.	1023
E.	16	F.	536	G.	256	H.	intrusion prevention system
I.	proxy ARP	J.	8-byte	K.	host-based intrusion detection system	L.	route
M.	virtual machines						

- 4.1 IDS and _____ are important tools in a computer security arsenal.
- 4.2 The OSI model has _____ layers.
- 4.3 _____ cloud computing delivery model.
- 4.4 A technique called _____ is used to create a subnetting effect.
- 4.5 In DES step both LPT and RPT undergoes in _____ key Rounds.
- 4.6 _____ command is used to manipulate TCP/IP routing table.
- 4.7 DHCP uses UDP port _____ for sending data to the server.
- 4.8 IPsec is designed to provide security at the _____.
- 4.9 _____ bytes of the secret key is generated using Diffie-Hellman encryption/decryption scheme.
- 4.10 An ICMP message has _____ header and a variable-size data section.

PART TWO

(Answer any FOUR questions)

5. (a) What is seizure in digital forensic ? List the different phases of Digital Forensics and explain in detail.
- (b) Discuss the importance of Cyber law in India with respect to Fraud, Copyright, Defamation, Harassment and Stalking.
(7+8)
6. (a) What is a cyber security assessment tool ? Explain the concept of Risk Assessment based on ISO27001.
- (b) List the Web Application Security Threats and explain any two in detail.
(7+8)
7. (a) List the Network security devices and explain any two devices in details.
- (b) Explain Cybersecurity Risk Mitigation in detail.
(8+7)
8. (a) What do you mean by cryptography ? What are the types of cryptography ? Explain the concept of symmetric key cryptography with suitable example.
- (b) What do you mean by public key infrastructure ? Explain the concept of Digital Certificates.
(8+7)

9. Differentiate between the following:

- (a) Static Routing vs. Dynamic Routing
- (b) TCP vs UDP
- (c) IPv4 vs IPv6 (5+5+5)

- o O o -

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK