# A10.3-R5 : INFORMATION SECURITY MANAGEMENT

| | |
|---|---|
| अवधि : 03 घंटे<br>DURATION : 03 Hours | अधिकतम अंक : 100<br>MAXIMUM MARKS : 100 |

ओएमआर शीट सं. :
OMR Sheet No. :

रोल नं. :
Roll No. :

उत्तर-पुस्तिका सं. :
Answer Sheet No. :

परीक्षार्थी का नाम :
Name of Candidate : ____________________;

परीक्षार्थी के हस्ताक्षर :
Signature of Candidate : ____________

| परीक्षार्थियों के लिए निर्देश : | Instructions for Candidate : |
|---|---|
| कृपया प्रश्न-पुस्तिका, ओएमआर शीट एवं उत्तर-पुस्तिका में दिये गए निर्देशों को ध्यानपूर्वक पढ़ें। | Carefully read the instructions given on Question Paper, OMR Sheet and Answer Sheet. |
| प्रश्न-पुस्तिका की भाषा अंग्रेजी है। परीक्षार्थी केवल अंग्रेजी भाषा में ही उत्तर दे सकता है। | Question Paper is in English language. Candidate can answer in English language only. |
| इस मॉड्यूल/पेपर के **दो भाग** हैं। **भाग एक** में **चार** प्रश्न और **भाग दो** में **पाँच** प्रश्न हैं। | There are **TWO PARTS** in this Module/Paper. **PART ONE** contains **FOUR** questions and **PART TWO** contains **FIVE** questions. |
| **भाग एक** ''वैकल्पिक'' प्रकार का है जिसके कुल अंक 40 है तथा **भाग दो** ''व्यक्तिपरक'' प्रकार का है और इसके कुल अंक 60 है। | **PART ONE** is Objective type and carries 40 Marks. **PART TWO** is Subjective type and carries 60 Marks. |
| **भाग एक** के उत्तर, **ओएमआर उत्तर-पुस्तिका** पर ही दिये जाने हैं। **भाग दो** की उत्तर-पुस्तिका में **भाग एक** के उत्तर **नहीं** दिये जाने चाहिए। | **PART ONE** is to be answered in the **OMR ANSWER SHEET** only. **PART ONE** is **NOT** to be answered in the answer book for **PART TWO**. |
| **भाग एक** के लिए अधिकतम समय सीमा **एक घण्टा** निर्धारित की गई है। **भाग दो** की उत्तर-पुस्तिका, **भाग एक** की उत्तर-पुस्तिका जमा कराने के पश्चात् दी जाएगी। तथापि, निर्धारित एक घंटे से पहले **भाग एक** पूरा करने वाले परीक्षार्थी **भाग एक** की उत्तर-पुस्तिका निरीक्षक को सौंपने के तुरंत बाद, **भाग दो** की उत्तर-पुस्तिका ले सकते हैं। | 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. |
| **परीक्षार्थी, उपस्थिति-पत्रिका पर हस्ताक्षर किए बिना और अपनी उत्तर-पुस्तिका, निरीक्षक को सौंपे बिना, परीक्षा हॉल/कमरा नहीं छोड़ सकते हैं। ऐसा नहीं करने पर, परीक्षार्थी को इस मॉड्यूल/पेपर में अयोग्य घोषित कर दिया जाएगा।** | **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.** |
| प्रश्न-पुस्तिका को खोलने के निर्देश मिलने के पश्चात् एवं उत्तर लिखना आरम्भ करने से पहले उम्मीदवार जाँच कर यह सुनिश्चित कर लें कि प्रश्न-पुस्तिका प्रत्येक दृष्टि से संपूर्ण है। | After receiving the instruction to open the booklet and before starting to answer the questions, the candidate should ensure that the Question Booklet is complete in all respect. |

**जब तक आपसे कहा न जाए, तब तक प्रश्न-पुस्तिका न खोलें।**

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

## PART ONE

**(Answer all the questions)**

**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** Compromising confidential information comes under _________.

(A) Bug

(B) Threat

(C) Vulnerability

(D) Attack

**1.2** Which of the following information security technology is used for avoiding browser-based hacking ?

(A) Anti-malware in browsers

(B) Remote browser access

(C) Adware remover in browsers

(D) Incognito mode in a browser

**1.3** From the options below, which of them is **not** a threat to information security ?

(A) Disaster

(B) Eavesdropping

(C) Information leakage

(D) Unchanged default password

**1.4** Which of the following is **not** a vulnerability of the Data Link Layer ?

(A) MAC Address Spoofing

(B) VLAN circumvention

(C) Switches may be forced for flooding traffic to all VLAN ports

(D) Overloading of Transport Layer mechanisms

**1.5** Which of the following is an example of Data Link Layer vulnerability ?

(A) MAC Address Spoofing

(B) Physical Theft of Data

(C) Route spoofing

(D) Weak or non-existent authentication

**1.6** Which of the following is **not** a Software Firewall ?

(A) Windows Firewall

(B) Outpost Firewall Pro

(C) Endian Firewall

(D) Linksys Firewall

**1.7** ACL stands for __________.

(A) Access Condition List

(B) Anti-Control List

(C) Access Control Logs

(D) Access Control List

1.8 Which of the following is **not** an attack done in the Network Layer of the TCP/IP model ?

(A) MITM attack

(B) DoS attack

(C) Spoofing attack

(D) Shoulder surfing

1.9 DNS stands for __________.

(A) Data Name System

(B) Domain Name Server

(C) Domain Name System

(D) Distributed Naming System

1.10 Plain text are also called __________.

(A) cipher-text

(B) raw text

(C) clear-text

(D) encrypted text

**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 Computer Security is protection of the integrity, availability and confidentiality of information system resources.

2.2 Computer Security is essentially a battle of wits between a perpetrator who tries to find holes and the administrator who tries to close them.

2.3 The procedure to add bits to the last block is termed as hashing.

2.4 The full form of Malware is Malicious Software.

2.5 Tailgating is also termed as piggybacking.

2.6 Banker A is a remote Trojan.

2.7 TLS vulnerability is also known as Return of Bleichenbacher's Oracle Threat.

2.8 Using VPN, we can access sites that are blocked geographically.

2.9 Antivirus masks your IP address.

2.10 TCP flooding is not a type of application layer DoS.

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 instructions therein.** **(1x10)**

| X | | Y | |
|---|---|---|---|
| **3.1** | OSI Layer 3 | **A.** | Internet Layer |
| **3.2** | Private key | **B.** | Type of output |
| **3.3** | TCP/IP layer 2 | **C.** | RSA |
| **3.4** | Public key algorithm | **D.** | Network layer |
| **3.5** | MD5 | **E.** | Voice+phishing |
| **3.6** | Vishing | **F.** | Session layer |
| **3.7** | Space filler virus | **G.** | cryptography |
| **3.8** | Sniffing also known as | **H.** | Message Digest algorithm |
| **3.9** | Circuit level gateway | **I.** | Cavity virus |
| **3.10** | NTA | **J.** | Generic solutions to recurring problems |
| | | **K.** | Wire tapping |
| | | **L.** | Network Traffic analysis |
| | | **M.** | SHA-1 |

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 attached to the question paper, following instructions therein.** **(1x10)**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **A** | agile | **B** | router to router VPN | **C** | illegitimate | **D** | Hacktivism |
| **E** | DNS | **F** | ethical hacking | **G** | non resident virus | **H** | system development life cycle |
| **I** | IM trojan | **J** | first generation firewall | **K** | cryptography | **L** | Brute force attack |
| **M** | Asymmetric | | | | | | |

**4.1** Direct Action Virus is also known as __________.

**4.2** __________ is a means of storing and transmitting information in a specific format so that only those for whom it is planned can understand or process it.

**4.3** A/an __________ is a program that steals your logins and passwords for instant messaging applications.

**4.4** Site-to-site VPNs are also known as __________.

**4.5** A __________ attack one of the simplest process of gaining access to any password protected system.

**4.6** __________ is the technique used in business organizations and firms to protect IT assets.

**4.7** RSA is a __________ Algorithm.

**4.8** Phishers often develop __________ websites for tricking users & filling their personal data.

**4.9** Packet filtering firewalls are also called __________.

**4.10** The __________ matches and maps to the user friendly domain name.

## PART TWO

**(Answer any FOUR questions)**

5. (a) What is difference between "MD5" and "SHA-l Algorithm" ?

(b) What is Email Security ?

(c) Explain various modes of risk analysis. **(5+5+5)**

6. (a) Explain use of digital signature.

(b) Explain various security threats and write their solution.

(c) Explain the use of firewall. **(4+5+6)**

7. (a) Explain TCP/IP model in detail.

(b) Why UDP is faster than TCP ? **(7+8)**

8. (a) Differentiate between private key and public key encryption.

(b) What is cryptography ? **(7+8)**

9. (a) What is Internet Law ?

(b) Why is Cyber Law important ? Also explain the different Cyber Threats. **(8+7)**

**- o O o -**

SPACE FOR ROUGH WORK

SPACE FOR ROUGH WORK