National Testing Agency

Question Paper Name: Cyber Security 09th November 2019 Shift 1
Subject Name: Cyber Security
Creation Date: 2019-11-09 18:35:15
Duration: 180
Total Marks: 130
Display Marks: Yes

Cyber Security

Group Number :	1
Group Id :	7077561
Group Maximum Duration :	0
Group Minimum Duration :	120
Revisit allowed for view? :	No
Revisit allowed for edit? :	No
Break time:	0
Group Marks:	130

Cyber Security-1

Section Id :	7077561
Section Number :	1
Section type :	Online
Mandatory or Optional:	Mandatory
Number of Questions:	70
Number of Questions to be attempted:	70
Section Marks:	70
Display Number Panel:	Yes
Group All Questions:	No

Sub-Section Number:	1
Sub-Section Id:	7077561
Question Shuffling Allowed :	Yes

Question Number : 1 Question Id : 7077561 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

People who are actively engaged in cyberspace are known as

1. Cyber criminals
2. Cybernauts
3. Insiders
4. Crackers

Question Number : 2 Question Id : 7077562 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This assures authorized access to the Information and resources.

1. Data confidentiality
2. Data integrity
3. System availability
4. System configuration

Question Number : 3 Question Id : 7077563 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Pinpoint the consequences of online communication.

1. Information loss
2. Extortion
3.
4. Theft
5. All the above

Question Number : 4 Question Id : 7077564 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Threats target these in an organization to compromise the Triad.

1. Assets
2. Vulnerabilities
3. Emails
4. Devices

Question Number : 5 Question Id : 7077565 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Choose the conditions that satisfy the properties of the extended cyberspace.

i. Extended cyberspace covers everything that surrounds the core

ii. Anybody can get access to core cyberspace through extended cyberspace

1. Only i.
2. Only ii.
3. Both i and ii.
4. Either i or ii.

Question Number : 6 Question Id : 7077566 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Predict the type of attack that floods the network bandwidth using high traffic.

1. Application
2. Volume-based
3. Protocol
4. Harmonized

Question Number : 7 Question Id : 7077567 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which attacks slow or stop the information flow between the nodes in a wireless network?

1. Adhoc
2. Man-In-The-Middle
3. Wireless Sensor Networks
4. Attacks on Mobile Adhoc Networks

Question Number : 8 Question Id : 7077568 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Ping of death attack can be avoided through this

1. Installing firewall
2. Using spyware
3. Using anti-malware
4. All the above

Question Number : 9 Question Id : 7077569 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This type of virus changes the last modified date and time of a file.

1. Macro virus
2. Stealth virus
3. Polymorphic virus
4. File infector virus

Question Number : 10 Question Id : 70775610 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Security compromise in a network is mainly due to

1. People

2. Devices

3. Internet

4. Intrusions

Question Number : 11 Question Id : 70775611 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This is the condition possessed by non-cooperative method for accessing the information in computer system vulnerability assessment.

1. Assume legal detection

2. Legal invasion

3. Illegal invasion

4. Assume illegal detection

Question Number : 12 Question Id : 70775612 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Detection of known attacks can be well handled using this technique.

1. Signature based IDS

2. Perimeter IDS

3. Anomaly based IDS

4. Virtual Machine based IDS

Question Number : 13 Question Id : 70775613 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following combination is active and passive in real-time?

1. Intrusion Prevention System and Intrusion Detection System

2. Network based Intrusion Detection System and Host based Intrusion Prevention System

3. Intrusion Detection System and Intrusion Prevention System

4. Host based Intrusion Detection System and Network based Intrusion Prevention System

Question Number : 14 Question Id : 70775614 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The type of Intrusion Detection System where the traffic is monitored only in a single host is

1.   Network Intrusion Detection System

2.   Network Node Intrusion Detection System

3.   Host Intrusion Detection System

4.   All the above

Question Number : 15 Question Id : 70775615 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Categorize various multi-biometric systems.

1.   Multi-phase, multi-algorithmic, multi-capture

2.   Multi-sensorial, multi-algorithmic, multi-instance

3.   Multi-sensorial, multi-stage, multi-function

4.   Multi-phase, multi-instance, multi-function

Question Number : 16 Question Id : 70775616 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following is used to prevent password theft during online transactions?

1.   One-time password

2.   Pass phrase

3.   Pass codes

4.   All the above

Question Number : 17 Question Id : 70775617 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Surveillance systems make use of this type of Biometrics.

1.   Behavioral biometrics

2.   Physiological biometrics

3.   Physical biometrics

4.   Biological biometrics

Question Number : 18 Question Id : 70775618 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

1 → M (One to Many) matching occurs in this phase of biometric systems.

1. Verification mode
2. Identification mode
3. Authentication mode
4. Authorization mode

Question Number : 19 Question Id : 70775619 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following dictates the essential guidelines to be followed with reference to computer assets by the user and the organization?

1. Security mechanism
2. Computer security
3. Security model
4. Security policy

Question Number : 20 Question Id : 70775620 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This type of attack is easier to identify than other types of routing attacks.

1. Packet mistreating attack
2. Hit-and-run attack
3. Persistent attack
4. Routing table poisoning

Question Number : 21 Question Id : 70775621 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The threat that causes serious indirect consequences to an Operating System.

1. Security update
2. Malicious modification
3. Vulnerability
4. None of the above

Question Number : 22 Question Id : 70775622 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Secure Socket Layer protocol ensures the establishment of client/server connection through this.

1. Alert
2. Record
3. Handshake
4. ChangeCipherSpec

Question Number : 23 Question Id : 70775623 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Sensitive data sometimes become vulnerable to attacks due to

1. Security misconfiguration
2. Insecure cryptographic storage
3. Insufficient transport layer protection
4. Insecure direct object references

Question Number : 24 Question Id : 70775624 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This attack hacks individual's essential data stored in mobile when accessed through public network systems.

1. Phishing
2. Crypto-jacking
3. Network spoofing
4. Trojans

Question Number : 25 Question Id : 70775625 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Examine the ways to maintain a secured mail system.

1. Configure, protect, analyse log files
2. Backup data frequently
3. Perform periodic testing
4. All the above

Question Number : 26 Question Id : 70775626 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This is a pre-planned approach designed to keep track of cloud usage and recover from disaster.

1. Incident management
2. Configuration management
3. System integrity
4. Contingency planning

Question Number : 27 Question Id : 70775627 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Rearrange the workflow of Cyber Physical Systems in correct order.

1. Computing, Actuation, Monitoring, Networking
2. Monitoring, Networking, Actuation, Computing
3. Monitoring, Networking, Computing, Actuation
4. Monitoring, Computing, Networking, Actuation

Question Number : 28 Question Id : 70775628 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following attack averts response to valid data packets?

1. Jamming
2. Rushing
3. Repudiation
4. Traffic analysis

Question Number : 29 Question Id : 70775629 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This attack alters or exploits data through decryption process.

1. Eavesdropping
2. Compromised-key attack
3. Stealthy deception
4. Jamming

Question Number : 30 Question Id : 70775630 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The level of privacy in social media is

1. Good
2. Average
3. Unknown
4. Poor

Question Number : 31 Question Id : 70775631 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Choose the major attempt that can be followed to clear social media threat issues.

1. Limiting publishing rights
2. Social media strategy
3. Restricting installation of apps
4. All the above

Question Number : 32 Question Id : 70775632 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Identify the following statements that are true with respect to Virtual Currencies.

S1-Regulated money

S2-Unregulated money

S3-Issued and controlled by developers

S4-Accepted and used among members of virtual community

1. S1 and S4
2. S2 and S3
3. S1, S3 and S4
4. S2, S3 and S4

Question Number : 33 Question Id : 70775633 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

This is the primary motive behind selfish mining attack.

1. Publish mined block
2. Obtain unfair reward
3. Combine components
4. Separate blocks

Question Number : 34 Question Id : 70775634 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The duties of a computer security auditor

1.   Conduct Vulnerability scans
2.   Examine Operating System settings
3.   Prepare historical data
4.   All the above

Question Number : 35 Question Id : 70775635 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which is the basis for the project plan?

1.   Statement of Work
2.   Application
3.   Network
4.   Statement of Proof

Question Number : 36 Question Id : 70775636 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Pinpoint the consequences of cyber-crime incidents.

1.   Financial loss
2.   Disruption of operational services
3.   Erosion of shareholder value and trust
4.   All the above

Question Number : 37 Question Id : 70775637 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The cyber security incidents and threats encountered in India are perceived by

1.   Cyber Security Team
2.   Indian Computer Emergency Response Team
3.   Computer Audit Response Team
4.   Incident Response Team

Question Number : 38 Question Id : 70775638 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The act of Cybercriminals indulging in dumping company secrets for sheer entertainment value is known as

1. Stealing IP
2. Information theft
3. Internet Griefing
4. Social badgering

Question Number : 39 Question Id : 70775639 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

This modifies data prior to or during input to a computer

1. Data diddling
2. Computer sabotage
3. Cyber trespass
4. War-dialer

Question Number : 40 Question Id : 70775640 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

The attitude of an individual about to commit an illegal activity comes under this element of fraud triangle.

1. Economic demands
2. Rationalization
3. Opportunity
4. Forces

Question Number : 41 Question Id : 70775641 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

These features are based on the analysis of essential keywords and phrases on specific topics.

1. Content-specific features
2. Lexical features
3. Structural features
4. Syntactic features

Question Number : 42 Question Id : 70775642 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

This is one of the functions of Incident Response Team

1. Safeguard incident data
2. Give access to data
3. Expose incident data
4. All the above

Question Number : 43 Question Id : 70775643 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Match the following in correct sequence

1. Data collection- Adds meaning to collected data
2. Data collation - Develops recognizable patterns
3. Data Analysis - Gathers raw data

1. 3 1 2
2. 1 3 2
3. 2 1 3
4. 2 3 1

Question Number : 44 Question Id : 70775644 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Crime Analysis units support various department functions like

1. Patrol deployment
2. Crime prevention
3. Carry out investigations
4. All the above

Question Number : 45 Question Id : 70775645 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The primary stage in a criminal proceeding is

1. Inquiry
2. Trail
3. Analysis
4. Investigation

Question Number : 46 Question Id : 70775646 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This helps the examiners in identifying the victims and their links to other victims.

1. Signatures
2. Trial
3. Crime type
4. Criminal profiling

Question Number : 47 Question Id : 70775647 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

The rationale behind psychological profiling

1. Biology
2. Antisocial personality
3. Environment
4. All the above

Question Number : 48 Question Id : 70775648 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Indicate the virtual version of a signature left at a crime scene.

1. Crime scene actions
2. Cybertrail
3. Thematic classification
4. Criminal profile

Question Number : 49 Question Id : 70775649 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Rearrange the following stages of Behavior Evidence Analysis framework in correct sequence.

1. Assessment of crime scene, Criminal characteristics, Equivocal forensic analysis, Victimology
2. Assessment of crime scene, Victimology, Equivocal forensic analysis, Criminal characteristics
3. Equivocal forensic analysis, Victimology, Assessment of crime scene, Criminal characteristics
4. Victimology, Equivocal forensic analysis, Criminal characteristics, Assessment of crime scene

Question Number : 50 Question Id : 70775650 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Which is the most commonly identified crime object at the cybercrime scenes?

1. Computer
2. Physical weapons
3. Criminal profile
4. Mobile device

Question Number : 51 Question Id : 70775651 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This service model is established to solve cloud-associated crimes.

1. Cloud-as-a-service
2. Software-as-a-service
3. Platform-as-a-service
4. Forensics-as-a-service

Question Number : 52 Question Id : 70775652 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The forensics that focuses on cross-examining the unsuccessful databases systematically.

1. Cloud forensics
2. Database forensics
3. Digital image forensics
4. Digital audio forensics

Question Number : 53 Question Id : 70775653 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Analyse the following statements and answer them as TT, TF, FT or FF with respect to different types of forensics.(T-True, F-False)

i. Database forensics and database recovery have similar functions.

ii. Digital Image forensics gathers, analyses and assesses audio-visual footages.

A   TT
B   FF
C   TF
D   FT

Question Number : 54 Question Id : 70775654 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Rearrange the steps involved in the process of conducting evidence examination.

1. Locating Evidence, Extracting Evidence, Reconstruction of Extracted data and Preparation
2. Locating Evidence, Preparation, Extracting Evidence and Reconstruction of Extracted data
3. Preparation, Locating Evidence, Extracting Evidence and Reconstruction of Extracted data
4. Locating Evidence, Reconstruction of Extracted data, Extracting Evidence and Preparation

---

Question Number : 55 Question Id : 70775655 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The extraction of data in bitwise form from the electronic devices is referred to as

1. Seizure
2. Acquisition
3. Isolation
4. Preparation

Question Number : 56 Question Id : 70775656 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The integrity of the computer forensics investigator is determined based on

1. Tools used
2. Professional conduct
3. Chain of custody
4. Countering to cyber threats

Question Number : 57 Question Id : 70775657 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The forensic report must be in this form.

1. Non-transmissible
2. Exposable
3. Contagious
4. Encrypted

Question Number : 58 Question Id : 70775658 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

These are the procedures used to hide or mask investigated data.

1. Steganography
2. Hidden partitions
3. File name anomalies
4. All the above

Question Number : 59 Question Id : 70775659 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This domain name issue is based on the illegal copying of legitimate website content to another website design.

1. Cyber squatting
2. Typo squatting
3. File carving
4. Pagejacking

Question Number : 60 Question Id : 70775660 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The Act that charges Penalty for publishing digital signature certificate without the knowledge of the certified authority.

1. Section 73
2. Section 71
3. Section 72
4. Section 80

Question Number : 61 Question Id : 70775661 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

One person is liable for the actions of another when engaged in joint or collective activity. This is called as

1. Vicarious liability
2. Corporate bodies
3. Computer source code
4. Reporting power

Question Number : 62 Question Id : 70775662 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Determine which of the following statements are true with respect to the salient features of the Information Technology Act 2000.

S1-Electronic signatures are replaced by Digital Signatures

S2- Limited scope on punishments and penalties based on the type of offenses and breaches

S3- cybercrime Justice Dispensation System's frameworks was provided

1.	S1, S2
2.	S2,S3
3.	S1, S3
4.	All the above

Identify the privileges protected under Intellectual Property.

1.	Trademarks
2.	Biological diversity
3.	Farmer's rights
4.	All the above

This value shows the quality of the record thereby providing a legal proof according to cyber law.

1.	Information
2.	Evidential
3.	Primary
4.	Data

The Act that governs specific functions of Reserve Bank of India Act.

1.	Negotiable Instruments Act
2.	FEMA Act
3.	National Housing Bank Act
4.	Transfer to Public Ownership Act

Question Number : 66 Question Id : 70775666 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The section of Patents Act that provides compulsory licensing of patents related to the manufacture of pharmaceutical products.

1.   Section 92A
2.   Section 82
3.   Section 84
4.   Section 94

Question Number : 67 Question Id : 70775667 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Any kind of information treated secretly in commercial applications include.

1.   Undisclosed information
2.   Trade secret
3.   Both 1 and 2
4.   Industrial secret

Question Number : 68 Question Id : 70775668 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Identify the tips to be followed to keep one's identity, personal information and data securely.

1.   Dispose of information properly
2.   Adhere to copyright restrictions
3.   Choosing strong passwords
4.   All the above

Question Number : 69 Question Id : 70775669 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Determine the techniques used to classify and cluster the intrusions.

1.   Data Mining
2.   Fuzzy logic
3.   Genetic algorithm
4.   Bayesian approach

Question Number : 70 Question Id : 70775670 Question Type : MCQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

If multiple accounts of a mail server are targeted, the impact is known as

1. Spamming
2. Junk email
3. Phishing
4. Denial of Service

Cyber Security-2

Section Id :	7077562
Section Number :	2
Section type :	Online
Mandatory or Optional:	Mandatory
Number of Questions:	60
Number of Questions to be attempted:	60
Section Marks:	60
Display Number Panel:	Yes
Group All Questions:	No

Sub-Section Number:	1
Sub-Section Id:	7077562
Question Shuffling Allowed :	Yes

Question Number : 71 Question Id : 70775671 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Application threats and vulnerabilities arise during these processes of a system

1. Upgradation
2. Design
3. Deployment
4. Planning

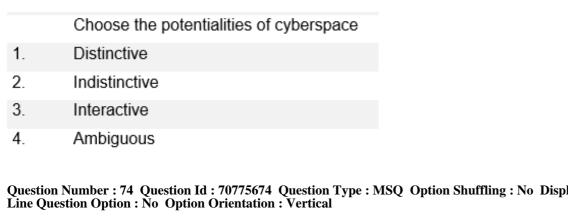**Question Number : 72 Question Id : 70775672 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical**

Correct Marks : 1 Wrong Marks : 0

A multi-layered security mechanism includes the following

1. Information security
2. Network security
3. Firewalls
4. Anti-virus software

Question Number : 73 Question Id : 70775673 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Choose the potentialities of cyberspace

1. Distinctive
2. Indistinctive
3. Interactive
4. Ambiguous

Question Number : 74 Question Id : 70775674 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Which of the following are interlinked?

1. Vulnerability
2. Threat
3. Risk
4. Actions

Question Number : 75 Question Id : 70775675 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Security policy weaknesses are caused due to

1. Misconfigured default settings
2. Lack of written security policy
3. Politics
4. Non-applied logical access control

Question Number : 76 Question Id : 70775676 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

These forms of messages are used in Black hole attack

1. RRER
2. RREP
3. RREQ
4. RRES

Question Number : 77 Question Id : 70775677 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Access attack types include

1. Port redirection
2. Phishing
3. Man-in-the middle
4. Port scanning

Question Number : 78 Question Id : 70775678 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Guessing the password in a random or systematic manner is the act of

1. Birthday attack
2. Replay attack
3. Brute force attack
4. Dictionary attack

Which of the following platforms allow the implementation of Sagan Intrusion detection tool?

1. Unix
2. Linux
3. Mac OS
4. Windows

The duties and responsibilities of vulnerability assessment include

1. Conducting asymmetrical assessment
2. Check report findings
3. Train staff
4. Security audits and scans

Select the primary components of Wireless Intrusion Prevention System.

1. Network
2. Administration
3. Sensors
4. Console

The advantages of using the system and the service banner in vulnerability assessment based on rules and models are

1. Simple
2. Fast
3. Efficient
4. Accuracy

Question Number : 83 Question Id : 70775683 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Judge the mechanisms that are essential to authenticate individuals.

1. Reliability
2. User-friendly
3. Dependency
4. Uniformity

Question Number : 84 Question Id : 70775684 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Identify the factors used in two-factor authentication.

1. Biometric feature
2. Password
3. Verification code
4. Object

Question Number : 85 Question Id : 70775685 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Select the levels where the multimodal biometrics fusion can be done.

1. Identification
2. Feature
3. Decision
4. Match

Question Number : 86 Question Id : 70775686 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The properties of facial biometric trait are

1. Low Security Level
2. High Level of Accuracy
3. High user acceptance
4. Ease of security

Question Number : 87 Question Id : 70775687 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Decide the places where Sensitive information can be obtained with the help of dumpster diving process.

1. Hard disk
2. Discarded paper
3. DVD
4. CD

Question Number : 88 Question Id : 70775688 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Data Loss Prevention techniques prevent users from these actions during unsafe conditions.

1. Replay
2. Upload
3. Forward
4. Print

Question Number : 89 Question Id : 70775689 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The security architecture of an Open Source Intelligence system pays attention to

1. Model
2. Attacks
3. Mechanisms
4. Services

Question Number : 90 Question Id : 70775690 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Determine the mechanisms used in employing network security.

1. Decipherment
2. Routing control
3. Data availability
4. Access control

Question Number : 91 Question Id : 70775691 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Frequent updations in Operating System help to

1. Improve functionality
2. Brand Marketing
3. Fix vulnerabilities
4. Ensure System stability

Question Number : 92 Question Id : 70775692 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The purpose of web security is to prevent these from cyber attacks.

1. Websites
2. Web servers
3. Web applications
4. Web storage

Question Number : 93 Question Id : 70775693 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

This may risk the organizations and force them to face indirect consequences due to non-compliance.

1. Bring Your Own Device
2. Security configurations
3. Malwares
4. Bring Your Own Computer

Question Number : 94 Question Id : 70775694 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The most common threats to e-mail security are

1. Botnets
2. Virus
3. Malicious links
4. Worms

Question Number : 95 Question Id : 70775695 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Software as a Service supports multiple users and data sharing through this model.

1. Single-tenancy
2. Multi-tenancy
3. Multi-instance
4. Single-instance

Question Number : 96 Question Id : 70775696 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Pinpoint the major issues faced by Internet of Things (IoT) devices.

1. Security
2. Availability
3. Privacy
4. Usability

Question Number : 97 Question Id : 70775697 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Identify the factors that minimize IoT security vulnerabilities.

1. Avoid Wi-Fi auto connect
2. Reconstruction of default password
3. Encrypting IoT devices
4. Regular updates

Question Number : 98 Question Id : 70775698 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Deception attack can be described as integrity breach in

1. Packet data
2. Sensor data
3. Packet controls
4. Nodes

Question Number : 99 Question Id : 70775699 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Imposter accounts are created to gain profit through fake

1. Games
2. Posts
3. Messages
4. Calls

Question Number : 100 Question Id : 707756100 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The properties of bitcoin are

1. Variable
2. Fixed
3. Transparent
4. Immutable

Question Number : 101 Question Id : 707756101 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The features of closed virtual currency are

1. Exists only in virtual community
2. Openly available
3. Cannot be exchanged
4. No link to real economy

Question Number : 102 Question Id : 707756102 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The resources in an Organization can be maintained safely by tracking the

1. Occurrence of threat
2. Strategy Development
3. Impact of threat
4. Implementation of strategy

Question Number : 103 Question Id : 707756103 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In the distributed network of a blockchain architecture, each participant has some of the responsibilities like

1.	Maintain
2.	Approve
3.	Update new entries
4.	Delete

Question Number : 104 Question Id : 707756104 Question Type : MSQ Option Shuffling : No Display Question Number : Yes
Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Determine the motives of cyber-crime.

1.	Activities due to emotions
2.	Political issues
3.	Entertainment purpose
4.	Badgering

Question Number : 105 Question Id : 707756105 Question Type : MSQ Option Shuffling : No Display Question Number : Yes
Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Cyber stalker pursues victims through

1.	Discussion forums
2.	Cloud
3.	Chat-rooms
4.	Network

Question Number : 106 Question Id : 707756106 Question Type : MSQ Option Shuffling : No Display Question Number : Yes
Single Line Question Option : No Option Orientation : Vertical
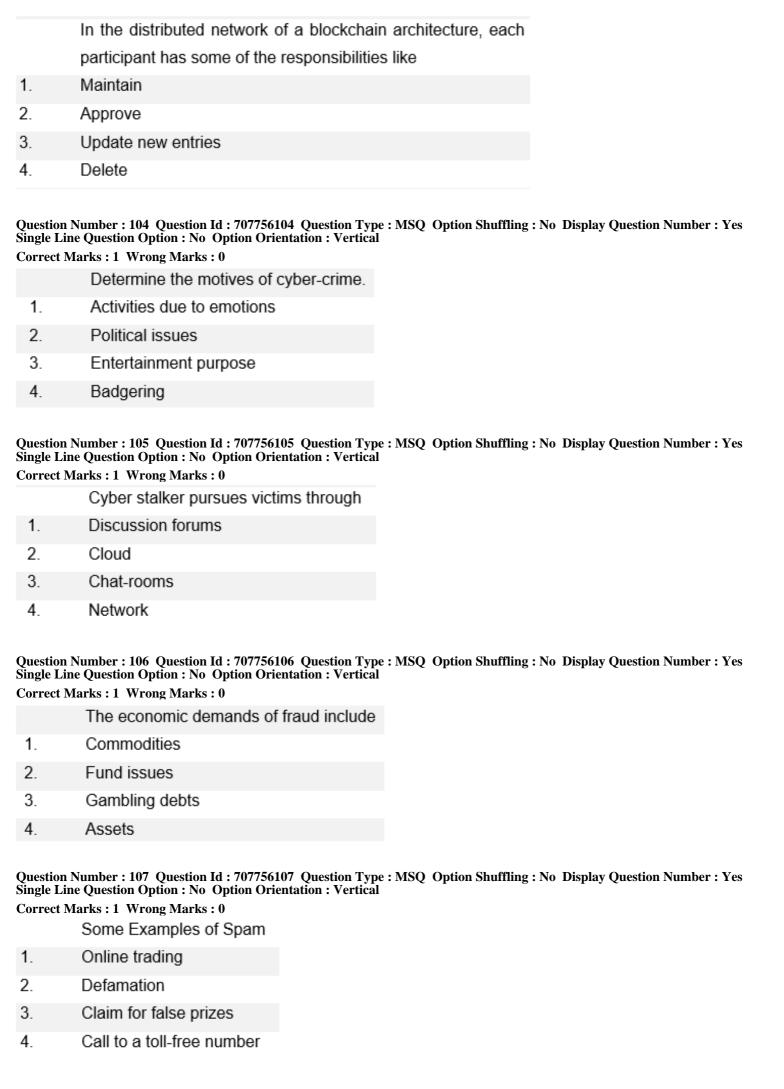Correct Marks : 1 Wrong Marks : 0

The economic demands of fraud include

1.	Commodities
2.	Fund issues
3.	Gambling debts
4.	Assets

Question Number : 107 Question Id : 707756107 Question Type : MSQ Option Shuffling : No Display Question Number : Yes
Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

Some Examples of Spam

1.	Online trading
2.	Defamation
3.	Claim for false prizes
4.	Call to a toll-free number

Question Number : 108 Question Id : 707756108 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Entity extraction is otherwise called as

1. Entity name recognition
2. Entity name extraction
3. Named entity extraction
4. Named entity recognition

Question Number : 109 Question Id : 707756109 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Human behavior analysis with smart machines help for

1. Automatic recognition of human actions
2. Extract features
3. Combine with algorithms
4. Detect potential hazards

Question Number : 110 Question Id : 707756110 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Factors proposed for extracting features are

1. Character n-Grams
2. Character count
3. Function words
4. Word count

Question Number : 111 Question Id : 707756111 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Text documents and spreadsheets provide advantages for data sharing due to their

1. Effectiveness
2. Flexibility
3. Rigidity
4. Reliability

Question Number : 112 Question Id : 707756112 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Examples of Civil Investigations are

1. Money laundering
2. Breach of contract
3. Homicide
4. Loss of inventory

Question Number : 113 Question Id : 707756113 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The description of the warrant during an investigation process must contain details to be searched on

1. Files
2. Internet
3. Data
4. Electronic devices

Question Number : 114 Question Id : 707756114 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The psychological view of criminal behavioral structure includes

1. Responsibility
2. Antisocial personality
3. Impulsivity
4. Confirmation to social norms

Question Number : 115 Question Id : 707756115 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The metadata from suspected cybercriminals can be collected from

1. Offender behavior
2. Timestamps
3. Blog entries
4. Wired connection

Question Number : 116 Question Id : 707756116 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Digital forensic techniques reconstruct the events from the past with these processes.

1. Collection
2. Modification
3. Identification
4. Validation

Question Number : 117 Question Id : 707756117 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The administrative issues recognized by forensic examiners are

1. Increasing storage space
2. Accepted standards
3. Development of innovative technologies
4. Fit to practice

Question Number : 118 Question Id : 707756118 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The electronic evidences present on different devices can be

1. Seized
2. Modified
3. scrutinized
4. Viewed

Question Number : 119 Question Id : 707756119 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

In Device IoT forensics, the evidences can be collected from

1. Intrusion Detection System
2. Firewall
3. CCTV camera
4. Amazon Echo

Question Number : 120 Question Id : 707756120 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Select the suitable factors that require warrant from officials to carry out further investigation in digital forensic investigation.

1. Information theft
2. Security policy violation
3. Unofficial use of Internet
4. Tampering of electronic documents

Question Number : 121 Question Id : 707756121 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The details of the digital forensic investigation report must include

1. Data and time of examination
2. Analysis of raw data
3. Physical condition of device
4. Outcome of statement of opinion

Question Number : 122 Question Id : 707756122 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

EnCase tool finds its application in

1. E-discovery
2. Criminal profile
3. Stylometry
4. Cyber Security

Question Number : 123 Question Id : 707756123 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The places where evidences can be searched for in Windows and Linux operating platforms

1. Hidden files
2. Patches
3. Password-protected files
4. Command line arguments

Question Number : 124 Question Id : 707756124 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The cybercrimes that come under section 66F are

1. Integrity
2. Denial of Service attacks
3. Illegal access to information
4. Illegal access to computer resources

Question Number : 125 Question Id : 707756125 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

These functions integrate the cyber security strategies across

organizations to strengthen cyber security.

1. Outsider threats
2. Process control security
3. Organization features
4. Physical security

Question Number : 126 Question Id : 707756126 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

The electromagnetic storage devices considered in Banker's

Book Evidence Act include

1. Floppy
2. Mobile
3. Tape
4. Palmtops

Question Number : 127 Question Id : 707756127 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

Usage of personal e-mail account in workplace may face these

issues

1. Internet Service Provider releases e-mail contents
2. Monitored by admin
3. Agents are capable of accessing individual's account
4. Less employee privacy

Question Number : 128 Question Id : 707756128 Question Type : MSQ Option Shuffling : No Display Question Number : Yes Single Line Question Option : No Option Orientation : Vertical

Correct Marks : 1 Wrong Marks : 0

	Provide the necessary requirements of evidentiary values during data modification.
1.	Affiliation of modifier
2.	Source of record
3.	List of originals
4.	Name of original creator

Question Number : 129 Question Id : 707756129 Question Type : MSQ Option Shuffling : No Display Question Number : Yes
Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

	The salient features of Reserve Bank of India Act are
1.	Restricted the stability of monetary
2.	Regularized the issues of bank notes
3.	Acts as an adviser to the government
4.	Reserve bank is the banker's bank

Question Number : 130 Question Id : 707756130 Question Type : MSQ Option Shuffling : No Display Question Number : Yes
Single Line Question Option : No Option Orientation : Vertical
Correct Marks : 1 Wrong Marks : 0

	The objectives of Prevention of Money Laundering Act are
1.	Expand physical property assets
2.	Help business organizations
3.	Control money laundering
4.	Seize the property obtained from laundered money