Question 1: **Skipped**

What is the TCP port for HTTPS?

○ **80**

○ **56**

○ **22**

○ **443** **(Correct)**

Explanation

The TCP port for HTTPS is 443. HTTPS (Hypertext Transfer Protocol Secure) is a secure version of HTTP that uses encryption to protect data transmitted over the internet

Question 2: **Skipped**

Who will approve the incident response policy of an organization?

○ **CIO**

○ **IT team**

○ **CISO**

○ **Organization leadership** **(Correct)**

Explanation

The incident response policy of an organization is typically approved by the organization's leadership, which may include the executive team or the board of directors.

Question 3: **Skipped**

Which of these monitor the inputs of a user without him knowing that his inputs are being recorded?

○ **Logic Bomb**

○ **Trojan**

○ **Keylogger** **(Correct)**

○ **Backdoor**

Explanation

A keylogger is a type of malicious software that is designed to monitor and record the keystrokes made by a user on a computer keyboard. It can capture all the text entered by the user, including passwords, credit card numbers, and other sensitive information.

Question 4: **Skipped**

Which of the following document will include the terms regarding to the performance level of services by a cloud service provider for negotiation?

○ **MoU**

○ **service level agreement**

○ **MoI**

○ **service level requirements** **(Correct)**

Explanation

The document that includes the terms regarding the performance level of services by a cloud service provider for negotiation is Service Level Requirements. Service Level Requirements (SLRs) are a set of documents that define the minimum acceptable levels of service that a cloud service provider (CSP) must provide to their customers. SLRs typically include performance metrics, such as availability, response time, and throughput, that specify the level of service that the CSP is expected to deliver.

Question 5: **Skipped**

Supports the "least privilege" principle by mandating that only approved people, procedures, or systems should have need-to-know access to information.

○ **Confidentiality** **(Correct)**

○ **Integrity**

○ **Availability**

○ **Preventive controls**

Explanation

Confidentiality is a security principle that supports the "least privilege" principle by mandating that only approved people, procedures, or systems should have a need-to-know access to information. Confidentiality ensures that sensitive or confidential information is protected from unauthorized access or disclosure, and that access to such information is granted only to those who have a legitimate need for it.

Question 6: **Skipped**

Which is the MOST used access control model in most organizations in the real world?

○ **RBAC** **(Correct)**

○ **MAC**

○ **DAC**

○ **ABAC**

Explanation

The most widely used access control model in most organizations is the role-based access control (RBAC) model. In RBAC, access is granted based on the job function or role of the user. This model is widely used because it is easy to administer and manage. Access is granted based on a user's job duties and responsibilities, which makes it easier to keep track of who has access to what data and resources.

Question 7: **Skipped**

Which of the following ports denote to the SSH (secure shell) ?

○ **23**

○ **21**

○ **20**

○ **22** **(Correct)**

Explanation

Port 22 is used for SSH (Secure Shell) which is a network protocol used for secure communication between two networked devices.

Question 8: **Skipped**

What is the name of the group of machines that attackers usually use to launch a synchronized attack?

○ **ransomware**

○ **malware**

○ **MITM**

○ **Botnet** **(Correct)**

Explanation

A group of machines that are compromised by an attacker and controlled remotely to launch a synchronized attack is called a botnet.

Question 9: **Skipped**

What is the reason for assigning a ranking to assets in an organization?

○ **Critical assets identification** **(Correct)**

○ **Idenfity critical business operations**

○ **Expedite opertaions of the organization**

○ **It is part of guidelines**

Explanation

Assigning a ranking to assets in an organization is done to identify critical assets. By ranking assets based on their importance to the organization, it becomes easier to prioritize the allocation of resources for protecting those assets

Question 10: **Skipped**

Which type of access control is being tested when a penetration tester attempts to gain access to sensitive information from one of our servers?

○ **Operational**

○ **detective**

○ **technical** **(Correct)**

○ **physical**

Explanation

The type of access control being tested in this scenario is technical access control.

Question 11: **Skipped**

What are the five steps for an incident response plan?

○ **Preparation, analysis, eradication, containment, post incident review**

○ **Preparation, Detection & Analysis, Containment & Eradication, Recovery, Post Incident Review** **(Correct)**

○ **Detection, analysis, eradication, containment,**

post incident review

○ **Idenftifcation, preparation, retention, mitigation, review**

Explanation

According to the literature of isc2 chapter 2, the option 1 is the correct sequence of an incident response plan

Question 12: **Skipped**

In which model the subject has the permission to assign the permissions of the objects which he owns?

○ **DAC** **(Correct)**

○ **MAC**

○ **RBAC**

○ **ABAC**

Explanation

In the DAC model, the owner of an object (such as a file or a folder) has discretion over who is granted access to that object and what type of access they are granted. The owner can assign permissions to other users or groups of users, and can modify or revoke those permissions at any time.

Question 13: **Skipped**

What is the first step in risk management?

○ **Destruction**

○ **Identification** **(Correct)**

○ **Reduction**

○ **Mitigation**

Explanation

The first step in risk management is risk identification, where potential risks are identified and documented.

Question 14: **Skipped**

A security poster will be included in which of the following of an organization's training strategy?

○ **Privacy policy**

○ **Security awareness** **(Correct)**

○ **password policy**

○ **zero trust**

Explanation

Yes, a security poster can be included in an organization's security awareness training strategy. Posters are a common way to display and reinforce security policies, procedures, and best practices to employees in a visual and easy-to-understand format.

Question 15: **Skipped**

Which of the following will provide the physical perimeter security for an organization?

○ **lock**

○ **Firewalls**

○ **Bollards**

○ **Fences** **(Correct)**

Explanation

Fences are a physical perimeter security measure that can be used to protect an organization's premises. Fences can help to deter unauthorized access and control the flow of people and vehicles in and out of the property. They can be constructed from a variety of materials, such as wood, metal, or concrete, and can be designed to meet different security needs

Question 16: **Skipped**

Which of the following document will assist in achieveing normal operations of an organization after a crisis?

○ **Zero trust**

○ **Business Impact Analysis**

○ **Business Continutiy Plan**

○ **Disaster Recovery Plan** **(Correct)**

Explanation

The document that will assist in achieving normal operations of an organization after a crisis is the Disaster Recovery Plan (DRP). A Disaster Recovery Plan is a document that outlines the steps an organization should take to restore normal operations after a disaster or other disruptive event

Question 17: **Skipped**

Which family of controls will monitor and controls the insight of the data in motion?

○ **Administrative controls**

○ **Operational controls**

○ **Technical controls** **(Correct)**

○ **Access controls**

Explanation

The family of controls that is responsible for monitoring and controlling the flow of data in motion is technical controls. Technical controls are security measures that are implemented through technology, such as firewalls, intrusion detection systems, and encryption. These controls help to ensure the confidentiality, integrity, and availability of data as it moves across a network.

Question 18: **Skipped**

Which of the following transport protocol uses SSH to add security to it?

○ **TLS**

○ **HTTPS**

○ **FTPS**

○ **SFTP** **(Correct)**

Explanation

SFTP (Secure File Transfer Protocol) uses SSH to add security to the file transfer process

Question 19: **Skipped**

What type of data is best secured with end-to-end encryption?

○ **Data in use**

○ **Data in archive**

○ **Data in motion** **(Correct)**

○ **Data at rest**

Explanation

End-to-end encryption is best used for securing data in motion.

Question 20: **Skipped**

Which of the following allows employees to do their job on the need to know and with only necessary privileges?

○ **DAC**

○ **zero trust**

○ **zero day**

○ **Least privlidge** **(Correct)**

Explanation

The principle of least privilege (POLP) is a concept in information security that requires that employees or users are only given the necessary privileges, access, and authority to do their job on a need-to-know basis. In other words, employees or users should be granted the minimum level of access to data and systems required to perform their job duties.

Question 21: **Skipped**

Which of the following has the characteristics of being Connection Oriented?

○ **TCP** **(Correct)**

○ **UDP**

○ **FTP**

○ **other**

Explanation

The protocol that has the characteristics of being Connection Oriented is TCP (Transmission Control Protocol). TCP is a transport layer protocol that provides reliable, ordered, and error-checked delivery of data between applications running on hosts on a network

Question 22: **Skipped**

Which term is commonly used to name the tool that is used to capture the network packets for monitoring?

○ **hub**

○ **Network analyzer**

○ **Firewall**

○ **Packet sniffer** **(Correct)**

Explanation

The term commonly used to name the tool that is used to capture network packets for monitoring is a Packet Sniffer. A packet sniffer is a software tool that captures and analyzes network traffic passing through a specific network interface. The tool captures packets and allows network administrators to analyze the contents of the packets, including the source and destination IP addresses, port numbers, protocols, and payload data

Question 23: **Skipped**

How many layers are there in OSI model?

○ **3**

○ **7** **(Correct)**

○ **9**

○ **2**

Explanation

The OSI model consists of seven layers, each with a specific function and set of protocols.

Question 24: **Skipped**

A malicious email intended to deceive a senior executive of a company is sent to him. Which attack is being used by the offender?

○ **XSS**

○ **Whaling** **(Correct)**

○ **SQL injection**

○ **Spear phishing**

Explanation

Whaling is a type of social engineering attack that targets senior executives or high-profile individuals within an organization. It is a form of phishing attack that uses deceptive emails, social media messages, or other forms of communication to trick the target into divulging sensitive information

Question 25: **Skipped**

Among the authentication methods we use, which type typically involves memorizing something as a means of authentication?

○ **Type 4**

○ **Type 2**

○ **Type 3**

○ **Type 1** **(Correct)**

Explanation

Type 1 authentication typically involves memorizing something as a means of authentication.

Question 26: **Skipped**

Which of the following is an example of multi-factor authentication?

○ **User name and password**

○ **OTP** **(Correct)**

○ **keys**

○ **badges**

Explanation

OTP (One-Time Password) is an example of multi-factor authentication. The OTP satisfies the type 2 Authentication (something you have).

Question 27: **Skipped**

During a pentesting activity, an email coming from the CEO was sent to several employees. The email contain a link. Most of the employees click the link. What should be done by the company management after this activity to reduce the risk for the organization?

○ **Add more awareness regarding phising attacks in the employee awareness training program** **(Correct)**

○ **Refer those employees to meet IT**

○ **Fire the employees who clicked the link**

○ **Paste security posters in office**

Explanation

One of the most effective steps they can take is to add more awareness regarding phishing attacks in the employee awareness training program. This training program should cover the different types of phishing attacks, how to recognize them, and the appropriate response. Employees should be taught to be cautious when opening emails from unknown or suspicious sources, to carefully scrutinize URLs and hyperlinks before clicking on them, and to report any suspicious emails to the IT or security team

Question 28: **Skipped**

What authentication method involves possessing something that you are expected to have in your possession?

○ **Type 4**

○ **Type 2** **(Correct)**

○ **Type 1**

○ **Type 3**

Explanation

This is an example of possession-based (Type 2) authentication, where the user is expected to have a physical object such as a smart card, security token, or mobile device in their possession to prove their identity.

Question 29: **Skipped**

What will be the top MOST priority of the team after an incident has occurred?

○ **Inform the management**

○ **Restore the operations to the last stable condition** **(Correct)**

○ **Save the organziation from more damage**

○ **Find the attacker**

Explanation

Restoring operations to the last stable condition is generally the topmost priority of a team after an incident has occurred.

Question 30: **Skipped**

Which of the following is a basic concept in the context of informationsecurity?

○ **Zero day**

○ **IAM**

○ **CIA** **(Correct)**

○ **MDM**

Explanation

The basic concept in the context of information security is Confidentiality, Integrity, and Availability (CIA) triad. The CIA triad is a fundamental concept in information security and is used to guide the development of security policies and procedures to protect information and systems from a wide range of threats and risks.

Question 31: **Skipped**

Which of the following controls will lie in the category of Administrative Security Control?

○ **Access Control List**

○ **Acceptable Use Policy** **(Correct)**

○ **Firewall**

○ **Security Cameras**

Explanation

Administrative Security Controls are security measures that are implemented through administrative procedures and policies. They help to manage and mitigate security risks by providing guidance and direction for personnel, processes, and systems. Acceptable Use Policy is an example of an administrative security control that defines the acceptable use of organizational resources and systems by employees, contractors, and other users.

Question 32: **Skipped**

What will be the most effective way to reduce the chances of fraud in an organization?

○ **Least Priviledge**

○ **Network segmentation**

○ **Zero trust**

○ **Segregation of duties** **(Correct)**

Explanation

One of the most effective ways to reduce the chances of fraud in an organization is to implement a segregation of duties (SoD) policy. This policy involves separating key functions and responsibilities between different individuals or teams, to prevent any one person from having complete control over a critical process

Question 33: **Skipped**

Which of the following is a principle of isc2 code of ethics?

○ **Provide diligent and competent service to clients**

○ **Act honorably, honestly, justly, responsibly, and rationally**

○ **Advance and protect the organization**

○ **Protect society, the common good, necessary public trust and confidence, and the infrastructure.** **(Correct)**

Explanation

According to isc2 Code of Ethics, the option 1 is the only correct answer. "Protect society, the common good, necessary public trust and confidence, and the infrastructure".

Question 34: **Skipped**

What kind of malware is hidden in a benign program to deceive the user?

○ **Virus**

○ **Logic bomb**

○ **Trojan** **(Correct)**

○ **Worms**

Explanation

A malware that is hidden in a benign program to deceive the user is called a Trojan

Question 35: **Skipped**

What will be the most effective term when engaging employees about data privacy in the organization?

○ **MDM**

○ **Privacy Policy** **(Correct)**

○ **Acceptable Use Policy**

○ **Zeo trust**

Explanation

A Privacy Policy is a legal document that outlines how an organization collects, uses, and manages personal information therefore "Privacy Policy" would be the most effective term when engaging employees about data privacy in the organization.

Question 36: **Skipped**

Which of the following will rely on the job function of the person and not the identitiy of the person?

○ **MAC**

○ **RBAC** **(Correct)**

○ **DAC**

○ **ABAC**

Explanation

The access control model that relies on the job function of the person and not the identity of the person is Role-Based Access Control (RBAC). RBAC is an access control model that assigns permissions to users based on their assigned roles within an organization.

Question 37: **Skipped**

Which of the following protocols uses a three way handshake for connection?

○ **IMAP**

○ **TCP** **(Correct)**

○ **UDP**

○ **FTP**

Explanation

TCP (Transmission Control Protocol) uses a three-way handshake for connection establishment between two devices on a network

Question 38: **Skipped**

Which of the following is a detective control?

○ CCTV Camera

○ Alarms

○ Smoke sensors (Correct)

○ Firewall

Explanation

By definition, smoke detectors are fire protection devices employed for the early detection of fire.

Question 39: **Skipped**

What is the purpose of data classification?

○ **Data criteria identity** **(Correct)**

○ **Ease of access**

○ **Store data efficientlty**

○ **Data verification**

Explanation

The purpose of data classification is to identify the sensitivity of data and assign appropriate levels of protection based on the potential impact of a data breach or unauthorized disclosure.

Question 40: **Skipped**

We are using Rule Based Access Control in our organization. What is that based on?

○ **The content described for the rule** **(Correct)**

○ **The clearence assigned to the subject**

○ **The job role of the user**

○ **The discretion of the object owner**

Explanation

Rule Based Access Control (RBAC) is based on a set of rules that determine whether access should be granted or denied based on various criteria such as the user's job function, clearance level, and other factors. These rules are defined in advance and enforced by the system.

Question 41: **Skipped**

A company needs to monitor the tablet devices issued to emloyees for official work by the company. Which of the following will assist in this task?

○ **MITM**

○ **Least Priviledge**

○ **MDM** **(Correct)**

○ **BYOD**

Explanation

The primary purpose of implementing Mobile Device Management (MDM) is to deploy, maintain, and monitor mobile devices. Devices may include laptops, smartphones, tablets, notebooks, or any other electronic device that can be moved outside the corporate office to home or some public place and then gets connected to the corporate office by some means.

Question 42: **Skipped**

Which document will best describe the procedure to maintain critical operations during and after a major incident?

○ **Acceptable Use Policy**

○ **Disaster Recovery Plan**

○ **Business Impact Analysis**

○ **Business Continuity Plan** **(Correct)**

Explanation

The document that best describes the procedure to maintain critical operations during and after a major incident is the Business Continuity Plan (BCP). A BCP is a comprehensive document that outlines the steps an organization will take to ensure that critical business functions can continue during and after a disruptive event.

Question 43: **Skipped**

In the event of a disaster or crisis, saving which of these would be the PRIMARY objective

○ **Organization**

○ **Database**

○ **People** **(Correct)**

○ **Critical system**

Explanation

In the event of a disaster or crisis, saving people is always the primary objective. The safety and well-being of people should always be the first priority, and all other considerations should be secondary. This includes not only employees but also customers, visitors, and members of the public who may be affected by the disaster.

Question 44: **Skipped**

Which of these has the Primary task of identifying and prioritizing critical business processes?

○ **Disaster Recovery Plan**

○ **Business Continutiy Plan**

○ **Asset identification**

○ **Business Impact Analysis** **(Correct)**

Explanation

Business Impact Analysis (BIA) is a risk management process that involves identifying and assessing the potential impacts of a disruption to critical business operations. The primary task of BIA is to identify and prioritize critical business processes based on their impact on the organization's operations, reputation, and financial stability.

Question 45: **Skipped**

Which is same as technical control?

○ **Physical controls**

○ **Access control**

○ **Safeguard** (Correct)

○ **Alarms**

Explanation

Technical control is the same as safeguard. Technical controls are safeguards implemented through technology, such as firewalls, intrusion detection systems, encryption, and access controls implemented in software or hardware. These controls are designed to prevent, detect, or mitigate threats and vulnerabilities to computer systems, networks, and data.

Question 46: **Skipped**

Which type of IPS will detect the threat on the basis of attack pattern and behavior?

○ **Protocol based**

○ **Heuristic** **(Correct)**

○ **Signautre based**

○ **Host based**

Explanation

The type of Intrusion Prevention System (IPS) that detects threats on the basis of attack pattern and behavior is called a Heuristic IPS. Heuristic IPS uses a set of rules and algorithms to detect threats that match known attack patterns or exhibit abnormal behavior. This allows it to identify and prevent previously unknown threats, zero-day attacks, and other sophisticated attacks

Question 47: **Skipped**

What should be considered by a user when establishing or resetting a password?

○ **Password & privacy policy**

○ **Password length and complexity** **(Correct)**

○ **None of the above**

○ **Password salt & hash**

Explanation

When establishing or resetting a password, the user should consider various factors, including password length and complexity. Passwords that are long and complex are generally more secure than short and simple passwords.

Question 48: **Skipped**

Which of the following area is directly connected to PHI and PII?

○ **Integrity**

○ **Availability**

○ **Authorization**

○ **Confidentiality** **(Correct)**

Explanation

PHI (Protected Health Information) and PII (Personally Identifiable Information) are both types of sensitive information that require strict confidentiality protections. PHI includes any information about an individual's health status, treatment, or payment for healthcare services, while PII includes any information that can be used to identify an individual, such as their name, address, Social Security number, or date of birth.

Question 49: **Skipped**

What would be the most suitable type of authorization mechanism for an organization that needs to simplify the assignment of various system access permissions for many users with similar job responsibilities?

○ **RBAC** **(Correct)**

○ **TBAC**

○ **DAC**

○ **MAC**

Explanation

Role-Based Access Control (RBAC) would be the most suitable type of authorization mechanism for an organization that needs to simplify the assignment of various system access permissions for many users with similar job responsibilities. In RBAC, access permissions are assigned to roles, and users are assigned to roles based on their job responsibilities. This allows for simplified administration of access control, reducing the workload on administrators and minimizing the risk of errors or unauthorized access.

Question 50: **Skipped**

What will be the best possible way to recover the system after a ransomware attack?

○ **Run the Vulnerability Scanner**

○ **Reboot the system**

○ **Backup the latest copy of**

the data stored separately on an alternative machine (Correct)

○ **Upgrade the OS**

Explanation

One of the best possible ways to recover the system after a ransomware attack is to restore the latest clean backup of the data that was stored separately on an alternative machine or in the cloud. This will help ensure that the data is not corrupted by the ransomware, and it will allow the organization to recover from the attack quickly without having to pay the ransom

Question 51: **Skipped**

We are considering another location for our catastrophe planning. If our primary facility went down, we would

prefer there to be no meaningful downtime. What are we thinking about?

○ **Warm site**

○ **Redundant site** **(Correct)**

○ **Cold site**

○ **Hot site**

Explanation

You are thinking about a redundant site. This is a backup facility that is ready to take over the functions of your primary facility in the event of a disaster or outage, with little or no downtime

Question 52: **Skipped**

What is the first step in information security management of an organization?

○ **Validation**

○ **Planning** **(Correct)**

○ **Testing**

○ **Designing**

Explanation

Yes, the first step in the information security management of an organization is planning. This includes developing policies, procedures, and guidelines for the security program, determining the scope and objectives of the program, and identifying the risks and threats that the organization faces.

Question 53: **Skipped**

In which attack, the attacker will utilize the electromagnetic data of device as an input to assess the risk of the device?

○ **Packet Attack**

○ **Side channel attack** **(Correct)**

○ **Man in the middle attack**

○ **XSS attack**

Explanation

The attack that utilizes the electromagnetic data of a device as an input to assess the risk of the device is known as a Side-Channel attack. In this type of attack, the attacker uses information that is unintentionally leaked by a device during its normal operation to gain unauthorized access to the device or extract sensitive information.

Question 54: **Skipped**

We are blocking unused ports as part of maintaining the baseline security of our servers. We have blocked port 22. What are we blocking?

○ **FTP control**

○ **SSH** **(Correct)**

○ **HTTP**

○ **SMTP**

Explanation

Port 22 is commonly used for SSH (Secure Shell) and you are blocking this port, thus preventing any SSH traffic to your servers

Question 55: **Skipped**

The address 00-B0-D0-63-C2-26 is a:

○ **MAC address** **(Correct)**

○ **IPV6**

○ **IPV4**

○ **Web address**

Explanation

The address 00-B0-D0-63-C2-26 is a Media Access Control (MAC) address, which is a unique identifier assigned to a network interface controller (NIC) for use as a network address in communications within a network segment.

Question 56: **Skipped**

In which type of attack, the attacker injects the code into the website response of a benign website?

○ **CSRF**

○ **XSS** **(Correct)**

○ **MITM**

○ **SQL injection**

Explanation

The type of attack in which the attacker injects code into a benign website's response is called Cross-Site Scripting (XSS) attack. In this attack, the attacker injects malicious code, typically in the form of a script, into a web page viewed by other users. When a user visits the infected web page, the malicious code is executed, allowing the attacker to steal sensitive information or take control of the user's session.

Question 57: **Skipped**

Which of these enables point to point online communication over an untrusted network?

○ **HIDS**

○ **NIDS**

○ **VLAN**

○ **VPN** **(Correct)**

Explanation

A VPN (Virtual Private Network) enables point-to-point online communication over an untrusted network, such as the internet. It allows two or more devices to communicate securely by creating a private network over a public network.

Question 58: **Skipped**

A type of error that occurs in biometric authentication systems where the system incorrectly matches an unauthorized person's biometric data with an authorized user's data and grants access

○ **False Rejection**

○ **False Positive** **(Correct)**

○ **False Rejection Rate**

○ **False Acceptance Rate**

Explanation

False Acceptance is a type of error that occurs in biometric authentication systems where the system incorrectly matches an unauthorized person's biometric data with an authorized user's data and grants access. It is also known as a Type II error or a "false positive."

Question 59: **Skipped**

What is the type of attack that conceals the activity of the system by modifying data at data structures and at

OS Level

○ **rootkit** **(Correct)**

○ **Identity theft**

○ **Ransomware**

○ **backdoor**

Explanation

a rootkit is a type of attack that conceals the activity of the system by modifying data at data structures and at the operating system level.

Question 60: **Skipped**

Which attack would be the best to compromise the Availability part of the CIA triad?

○ **DDOS** **(Correct)**

○ **SQL injection**

○ **XSS**

○ **Man in the middle**

Explanation

A DDoS (Distributed Denial-of-Service) attack is designed to overwhelm a targeted system or network with a flood of traffic, requests, or data, causing it to become unavailable to users or customers. DDoS attacks can be carried out using botnets, which are networks of compromised devices that are controlled by an attacker. By flooding a system or network with traffic, a DDoS attack can make it unavailable to users or customers, thereby compromising its availability.

Question 61: **Skipped**

Labels are used for objects. This is an example of which type of access management?

○ **TBAC**

○ **RBAC**

○ **DAC**

○ **MAC** (Correct)

Explanation

Labels are used for objects in Mandatory Access Control (MAC) access management. MAC is a type of access control where access to resources is based on labels assigned to objects.

Question 62: **Skipped**

Which physical control will prevent tailgaiting in your ogranzation?

○ **lock**

○ **Turnstile** (Correct)

○ **Cameras**

○ **Bollards**

Explanation

The physical control that is most effective in preventing tailgating in an organization is the use of turnstiles. A turnstile is a physical barrier that allows only one person at a time to pass through. It uses a rotating mechanism to control access and prevent unauthorized entry

Question 63: **Skipped**

Which TCP port usually corresponds to the SMTP?

○ **24**

○ **21**

○ **25** **(Correct)**

○ **22**

Explanation

SMTP (Simple Mail Transfer Protocol) is a protocol used for sending and receiving email messages. The default TCP port for SMTP is port 25. This is the port used by mail servers to send outgoing email messages to other mail servers on the internet.

Question 64: **Skipped**

Something you know, something you have, something you are, these properties assist in achieving which

property of security?

○ **Authentication** **(Correct)**

○ **Availability**

○ **Authorization**

○ **Confidentiality**

Explanation

The properties of "something you know, something you have, something you are" are commonly used in multi-factor authentication, which assists in achieving the property of authentication in security

Question 65: **Skipped**

What is the Primary Objective of degaussing?

○ **Prevent side channel attack**

○ **Retain the data on a disk**

○ **Encrypt data on a disk**

○ **Erase the data from a disk** **(Correct)**

Explanation

Degaussing is a process that uses a strong magnetic field to erase or neutralize the magnetic fields of storage media such as hard drives, floppy disks, and magnetic tapes. This process makes the data on the media unreadable and irretrievable, ensuring that sensitive or confidential information cannot be accessed by unauthorized parties.

Question 66: **Skipped**

What is the last step in data life cycle?

○ **Share**

○ **Store**

○ **Archive**

○ **Destruction** **(Correct)**

Explanation

The last step in the data life cycle is typically the destruction or disposal of the data. This may include the secure deletion of electronic data or the physical destruction of data storage devices, such as hard drives or tapes.

Question 67: **Skipped**

Which cloud model entails LESS responsibility for the infrastructure on the part of the cloud customer?

○ **XaaS**

○ **IaaS**

○ **SaaS** **(Correct)**

○ **PaaS**

Explanation

In SaaS model, the cloud customer is responsible for using the software application, while the cloud service provider is responsible for managing the underlying infrastructure, including servers, storage, and networking. The cloud customer does not need to worry about maintaining the hardware and software infrastructure, as it is the responsibility of the cloud service provider.

Question 68: **Skipped**

Which of the following will be used to authenticate the actions of an individual?

○ **Accessibility**

○ **Confidentiality**

○ **Non-repudiation** **(Correct)**

○ **Action Validation**

Explanation

Yes, non-repudiation is used to authenticate the actions of an individual, ensuring that they cannot deny having performed a particular action or transaction. This is typically achieved through the use of digital signatures, timestamps, and other cryptographic techniques.

Question 69: **Skipped**

If an attack interrupts a service or make it unavailable, then which type of attack is this?

○ **DDOS** **(Correct)**

○ **CSRF**

○ **MITM**

○ **XSS**

Explanation

If an attack interrupts a service or makes it unavailable, then it is a Denial of Service (DoS) attack. A DoS attack is an attack in which an attacker attempts to prevent legitimate users from accessing a resource, such as a website, network, or application, by overwhelming it with traffic or other means.

Question 70: **Skipped**

Which of these rights is provided by GDPR to the individuals over their data?

○ **right to rectification** **(Correct)**

○ **right to complain**

○ **right to store**

○ **right to subject**

Explanation

The General Data Protection Regulation (GDPR) provides several rights to individuals over their data, and one of them is the right to rectification. The right to rectification gives individuals the right to have inaccurate or incomplete personal data corrected or completed. This means that individuals have the right to request that their personal data be updated or corrected if it is inaccurate or incomplete

Question 71: **Skipped**

What is the BEST way to secure a door from unauthorized access?

○ **Access controls**

○ **Lock** **(Correct)**

○ **Biometric**

○ **Security cameras**

Explanation

The best way to secure a door from unauthorized access is to use a lock. Locks are a basic but effective physical security measure that can be used to prevent unauthorized access to a room, building, or facility.

Question 72: **Skipped**

Which device is used to connect a local LAN containing multiple hosts to the internet?

○ **Router** **(Correct)**

○ **Hub**

○ **Switch**

○ **Network analyzer**

Explanation

A router is used to connect a local LAN containing multiple hosts to the internet. A router is a network device that connects two or more networks together and routes traffic between them. In the case of a LAN, a router can be used to connect the LAN to the internet, allowing multiple hosts on the LAN to access the internet. The router serves as a gateway between the LAN and the internet

Question 73: **Skipped**

What will be the most appropriate tool to detect intrusion into the network of an organization by analyzing network packets?

○ **NIDS** **(Correct)**

○ **firewall**

○ **Network analyzer**

○ **HIDS**

Explanation

The most appropriate tool to detect intrusion into the network of an organization by analyzing network packets is NIDS (Network Intrusion Detection System)

Question 74: **Skipped**

Which of these malware varieties can replicate itself without human intervention?

○ **Virus**

○ **Adware**

○ **Worm** **(Correct)**

○ **Trojan**

Explanation

A worm is a type of malware that can self-replicate and spread to other computers or devices without requiring any human intervention. Worms can exploit vulnerabilities in operating systems or software to spread quickly and infect large numbers of computers or devices.

Question 75: **Skipped**

Which kind of intrusion detection system only warns us when it finds malicious traffic?

○ **IDS** **(Correct)**

○ **Firewalls**

○ **IPS**

○ **DMZ**

Explanation

An Intrusion Detection System (IDS) only generates alerts when it detects malicious traffic. It compares network traffic against a database of known attack signatures and generates an alert when it matches a signature.

Question 76: **Skipped**

Which of these devices would we find on OSI layer 1?

○ **Hubs** **(Correct)**

○ **Routers**

○ **Switches**

○ **Firewalls**

Explanation

Layer 1 of the OSI model is the Physical Layer. It deals with the physical aspects of network communication, such as voltage levels, cabling, connectors, and signaling. At this layer, devices such as hubs, repeaters, and network adapters operate.

Question 77: **Skipped**

A biometric reader that grants access to a computer system in a data center is an example of:

○ **Authorization control**

○ **Technical control** **(Correct)**

○ **Physical control**

○ **Administrative control**

Explanation

A biometric reader that grants access to a computer system in a data center is an example of a technical control because it uses biometric technology to verify the identity of the user before granting access to the computer system.

Question 78: **Skipped**

What control will prevent the theft of data from shoulder surfing in an organization when employees are working on the data actively on their systems?

○ **Window**

○ **Lock**

○ **Turnstile**

○ **Screen lock & Angled Screen View** **(Correct)**

Explanation

The control that will prevent the theft of data from shoulder surfing in an organization when employees are working on the data actively on their systems is a combination of screen lock and angled screen view.

Question 79: **Skipped**

Which risk management technique is being implemented when a company engages an insurance company to reduce risk?

○ **Risk mitigation**

○ **Risk avoidance**

○ **Risk transfer** **(Correct)**

○ **Risk acceptance**

Explanation

Risk transfer is a risk management technique where a company transfers the risk to another party, typically an insurance company, by paying premiums. In case of a loss, the insurance company will bear the financial burden of the loss, reducing the risk to the company.

Question 80: **Skipped**

Which of the following exists on the application layer of OSI model?

○ **FTP** **(Correct)**

○ **ICMAP**

○ **UDP**

○ **TCP**

Explanation

FTP (File Transfer Protocol) is an application layer protocol that is used to transfer files over the internet. The application layer is the seventh layer of the OSI (Open Systems Interconnection) model, which is responsible for providing services and interfaces to the application programs that operate on the user's computer.

Question 81: **Skipped**

Which of the following segment will you use to place the network segementation for identifying the location of the hosting web servers

○ **DMZ** **(Correct)**

○ **VPN**

○ **DMZ**

○ **Network VLAN**

Explanation

To identify the location of hosting web servers in a network, the network segment that is commonly used is the Demilitarized Zone (DMZ). The DMZ is a secure network segment that sits between an organization's internal network and the public internet. It is designed to provide a secure area for hosting publicly accessible services, such as web servers, while isolating them from the rest of the internal network.

Question 82: **Skipped**

Which of the following protocols assists in VoIP calls?

○ **TCP**

○ **FTP**

○ **UDP** **(Correct)**

○ **DHCP**

Explanation

UDP is commonly used for VoIP calls due to its low latency and ability to handle real-time data. TCP can introduce too much delay due to its error-checking mechanisms.

Question 83: **Skipped**

Which of these methods for testing a business continuity plan is the most effective and efficient?

○ **Post indicent activity**

○ **Table top exercise**

○ **Simulations** **(Correct)**

○ **Reviews**

Explanation

Simulations are considered the most effective and efficient method for testing a business continuity plan. A simulation involves creating a realistic scenario in which a disaster or other disruptive event occurs, and then testing the plan by implementing the procedures and strategies outlined in the plan. This allows organizations to identify weaknesses and areas for improvement in their business continuity plan, as well as to train staff on their roles and responsibilities in the event of a real crisis.

Question 84: **Skipped**

What will an organization do to check the effectiveness of the vulnerability remediation after performing risk mitigation activity?

○ **Perform an attack**

○ **Upgrade the systems**

○ **Validate the patches** **(Correct)**

○ **Run vendor provided patch test**

Explanation

Organizations can validate the patches to ensure that the vulnerability has been properly remediated. This can be done by performing vulnerability scans or penetration testing. The organization should also review its patch management process to ensure that vulnerabilities are being remediated in a timely manner. Running a vendor-provided patch test can be helpful in identifying whether the patch has been installed correctly, but it is not the primary method for validating the effectiveness of vulnerability remediation. Upgrading the systems is also not necessarily the solution for vulnerability remediation, and performing an attack is not recommended.

Question 85: **Skipped**

Which of these methods will guarantee the 'non-repudiation' property?

○ **Passwords**

○ **Hashing**

○ **Digital Signatures** **(Correct)**

○ **Firewall**

Explanation

Non-repudiation is a security property that ensures that the sender of a message cannot deny having sent it. In other words, it provides proof of the authenticity of the message and the identity of the sender.Digital signatures are a cryptographic technique that provides non-repudiation by using a combination of hashing and encryption.

Question 86: **Skipped**

Your colleague has asked about the size of IPv6 addresses. How would you respond?

○ **64 bits**

○ **256 bits**

○ **128 bits** **(Correct)**

○ **32 bits**

Explanation

Yes, the size of IPv6 addresses is 128 bits, which is four times larger than IPv4 addresses that are only 32 bits. The increased size of IPv6 addresses provides a virtually unlimited number of unique IP addresses, enabling the expansion of the internet and the proliferation of connected devices.

Question 87: **Skipped**

A security event that jeopardizes the availability, confidentiality, or integrity of a data asset.

○ **Trademark**

○ **Breach**

○ **Due care**

○ **Incident** **(Correct)**

Explanation

An incident is a security event that jeopardizes the availability, confidentiality, or integrity of a data asset. Security incidents can include unauthorized access to data, data breaches, malware infections, phishing attacks, physical theft or damage to hardware, and other events that can compromise the security of an organization's data

Question 88: **Skipped**

If a person is provided access to the resource that he/she is supposed to use for performing his duties, what is this concept called in the context of information security?

○ **Availability**

○ **Authorization** **(Correct)**

○ **Confidentiality**

○ **Authentication**

Explanation

According to IAAA concepts, authorization is the correct answers for the given scenario.

Question 89: **Skipped**

Which OSI layer do TCP and UDP operate at?

○ **Data link**

○ **Physical**

○ **Session**

○ **Transport** **(Correct)**

Explanation

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are both transport layer protocols in the OSI (Open Systems Interconnection) model. The transport layer is responsible for providing reliable and efficient data transport services between applications running on different devices.

Question 90: **Skipped**

Which protocol will you choose if reliability is necessary and time is not a constraint?

○ **TCP** **(Correct)**

○ **UDP**

○ **DHCP**

○ **FTP**

Explanation

If reliability is necessary and time is not a constraint, then the Transmission Control Protocol (TCP) would be the best protocol to choose. TCP provides reliable, connection-oriented communication between applications, ensuring that all data is delivered correctly and in order

Question 91: **Skipped**

Which of the following is the MOST restrictive network design concept?

○ **VPN**

○ **Zero Trust**

○ **VLAN** **(Correct)**

○ **NAT**

Explanation

Out of the given options, VLAN (Virtual Local Area Network) is the most restrictive network design concept. It limits the communication between devices within the same VLAN and restricts communication between devices in different VLANs. VLANs are often used to enhance security by isolating sensitive data or applications from the rest of the network

Question 92: **Skipped**

What will be the BEST term to describe if an organization changes the way of doing business for reducing the risk for the organization

○ **Risk mitigation**

○ **Risk avoidance** **(Correct)**

○ **Risk acceptance**

○ **Risk reduction**

Explanation

Risk avoidance is the best term to describe if an organization changes the way of doing business for reducing the risk for the organization. Risk avoidance involves identifying a risk and taking action to eliminate the risk altogether.

Question 93: **Skipped**

In which cloud model, the fundamental computer resources are allocated to the client?

○ **XaaS**

○ **IaaS** **(Correct)**

○ **SaaS**

○ **PaaS**

Explanation

The cloud model in which the fundamental computer resources are allocated to the client is Infrastructure as a Service (IaaS). IaaS is a cloud computing model that provides clients with access to fundamental computing resources, such as virtual machines, storage, and networking, over the internet.

Question 94: **Skipped**

Which of the following is an example of physical control in information security?

○ **Antivirus**

○ **All of the above**

○ **Access card system** **(Correct)**

○ **Firewall**

Explanation

An access card system is an example of physical control in information security.

Question 95: **Skipped**

If an attacker steals the social security number, bank account numbers, passport info, etc. then which of the following is the correct term for this act?

○ **Data breach** **(Correct)**

○ **Identity theft**

○ **Ransomware**

○ **DDOS**

Explanation

The act of stealing sensitive and confidential information such as social security number, bank account numbers, passport info, etc. is called data theft, while a data breach refers to a security incident in which sensitive and confidential data is accessed, stolen, or exposed by an unauthorized individual or entity

Question 96: **Skipped**

Which of these is a common layer 4 attack if we are considering the OSI model?

○ **SYN Flood** **(Correct)**

○ **Slowloris attacks**

○ **Eavesdropping**

○ **Ping of death**

Explanation

SYN flood is a common layer 4 attack if we are considering the OSI model. It is a type of Denial of Service (DoS) attack that exploits the three-way handshake process of the Transmission Control Protocol (TCP) to overwhelm a server with a flood of connection requests, making it unavailable to legitimate users.

Question 97: **Skipped**

What will be the most effective in terms of backup power for preventing losses due to power fluctuation by normal power supply?

○ **Backup Generator** **(Correct)**

○ **Solar**

○ **Battery**

○ **Wind power**

Explanation

A backup generator is the most effective solution for preventing losses due to power fluctuations by normal power supply. Backup generators provide a reliable source of power in the event of a power outage or other interruption to the normal power supply. They are designed to automatically start up and take over when the primary power source fails, providing uninterrupted power to critical systems and equipment.

Question 98: **Skipped**

Which cloud service model provides the most suitable environment for customers who want to install their custom operating system

○ **IaaS** **(Correct)**

○ **PaaS**

○ **XaaS**

○ **SaaS**

Explanation

IaaS stands for Infrastructure as a Service, which is a cloud computing service model that provides customers with virtualized computing resources, such as servers, storage, and networking infrastructure, over the internet. With IaaS, customers have complete control over the operating system and applications running on the virtualized infrastructure. They can install and configure their custom operating system and applications, just as they would on physical servers.

Question 99: **Skipped**

The Bell and Lapadula access control model lies in which category?

○ **DAC**

○ **RBAC**

○ **ABAC**

○ **MAC** **(Correct)**

Explanation

The Bell and Lapadula access control model lies in the Mandatory Access Control (MAC) category.

Question 100: **Skipped**

Which of these is the greatest choice for a network administrator who has to manage network access?

○ **DMZ**

○ **Firewall** **(Correct)**

○ **SIEM**

○ **NAC**

Explanation

NAC (Network Access Control) is a security solution that enables network administrators to manage network access by controlling the devices and users that are allowed to access the network. NAC provides a centralized platform for managing access policies, authentication, and authorization, and it can be used to enforce security policies across multiple network devices, such as switches, routers, and firewalls.