C.I.A. Question Bank

❖ 2 Marks Questions

Q.1.) What is CIA triangle in cyber security ?

Ans :- The **CIA Triangle** (also called the **CIA Triad**) is a fundamental model in cybersecurity that represents three core principles necessary to protect information systems:

1. **Confidentiality** – Ensuring that sensitive information is accessible only to authorized individuals. Techniques like encryption, access control, and authentication help maintain confidentiality.
2. **Integrity** – Ensuring that data remains accurate, consistent, and unaltered by unauthorized users. Hashing, checksums, and digital signatures help protect data integrity.
3. **Availability** – Ensuring that systems, networks, and data are accessible when needed by authorized users. Measures such as redundancy, backups, and denial-of-service (DoS) protection help maintain availability.

Q.2.) Define the term cyber target in cryptography ?

Ans :- In **cryptography**, a **cyber target** refers to any **entity, system, or data** that an attacker aims to compromise, exploit, or manipulate for malicious purposes. Cyber targets can include:

1. **Sensitive Data** – Encrypted or plaintext information such as passwords, financial details, or personal records.
2. **Cryptographic Keys** – Secret keys used in encryption and decryption processes.
3. **Communication Channels** – Secure communication lines (e.g., VPNs, encrypted emails) that attackers may attempt to intercept.
4. **Hardware & Software** – Cryptographic systems, algorithms, or hardware like security tokens, TPM chips, or cryptographic libraries.

5. **Network Protocols** – Secure communication protocols (e.g., TLS, SSL, SSH) that attackers may try to break.

Q.3.) List out authentication principles in cryptography ?

Ans :- In **cryptography**, authentication ensures that the identity of users, devices, or systems is verified before granting access. The key **authentication principles** include:

1. Something You Know (Knowledge-Based Authentication)

- A **password**, **PIN**, or **security question** that only the user should know.
- Example: Entering a password to log in.

2. Something You Have (Possession-Based Authentication)

- A **physical or digital token**, such as a **smart card**, **OTP (One-Time Password) device**, or **security key**.
- Example: Using a hardware security key like a YubiKey or receiving an OTP via SMS.

3. Something You Are (Biometric Authentication)

- **Unique biological traits** such as **fingerprints, facial recognition, iris scans, or voice recognition**.
- Example: Unlocking a phone using Face ID or fingerprint scanning.

4. Mutual Authentication

- Both the **client and server authenticate each other** to ensure they are communicating with legitimate parties.
- Example: TLS (SSL) certificates in secure web communication.

5. Multi-Factor Authentication (MFA)

- **Combining two or more authentication factors** (e.g., password + OTP or fingerprint + smart card) to enhance security.
- Example: Logging into an account using a password and a 2FA (two-factor authentication) code.

6. Challenge-Response Authentication

- A dynamic process where a system presents a **challenge**, and the user must provide the correct **response**.
- Example: CAPTCHA verification or cryptographic challenge-response mechanisms like OTPs.

7. Session Authentication

- **Maintaining authentication** over an active session using tokens or session keys.
- Example: OAuth tokens in web applications to keep users logged in securely.

8. Non-Repudiation

- Ensuring that a user **cannot deny** their actions by using cryptographic signatures or logs.
- Example: Digital signatures on documents.

Q.4.) List out types of cryptography.

Ans :- The **types of cryptography** can be categorized into three main types:

1. **Symmetric Key Cryptography (Secret Key Cryptography)**
    - Uses a **single key** for both encryption and decryption.
    - Fast and efficient but requires secure key sharing.
    - Example: **AES, DES, Blowfish**
2. **Asymmetric Key Cryptography (Public Key Cryptography)**
    - Uses **two keys**: a **public key** for encryption and a **private key** for decryption.
    - More secure but slower than symmetric cryptography.
    - Example: **RSA, ECC, Diffie-Hellman**
3. **Hash Functions (Cryptographic Hashing)**

- Converts data into a **fixed-length hash** that is irreversible.
- Used for **data integrity, password hashing, and digital signatures**.
- Example: **SHA-256, MD5, SHA-3**

Q.5.) Give the various types of firewall.

Ans :- Firewalls are security systems that monitor and control incoming and outgoing network traffic. The various **types of firewalls** include:

1. Packet Filtering Firewall

- Filters network packets based on rules like **IP addresses, ports, and protocols**.
- Works at **Layer 3 (Network) and Layer 4 (Transport)** of the OSI model.
- Example: **Access Control Lists (ACLs) in routers**.

2. Stateful Inspection Firewall

- Tracks the **state of active connections** and allows only legitimate traffic.
- More secure than packet filtering firewalls.
- Example: **Checkpoint Firewalls**.

3. Proxy Firewall (Application Layer Firewall)

- Acts as an **intermediary** between users and the internet, filtering traffic at **Layer 7 (Application Layer)**.
- Provides **deep packet inspection** and hides internal network details.
- Example: **Squid Proxy, Fortinet Proxy Firewalls**.

4. Next-Generation Firewall (NGFW)

- Advanced firewall that includes **deep packet inspection, intrusion prevention, and application awareness**.
- Combines **traditional firewalls with AI-based threat detection**.
- Example: **Palo Alto Networks NGFW, Cisco Firepower**.

5. Circuit-Level Gateway Firewall

- Works at **Layer 5 (Session Layer)** to monitor TCP handshakes.
- Ensures that only **legitimate sessions** are established.
- Example: **SOCKS Proxy Firewall**.

6. Cloud-Based Firewall (Firewall as a Service - FWaaS)

- A **cloud-hosted firewall** that protects distributed networks and remote users.
- Scalable and suitable for organizations with cloud-based services.
- Example: **Zscaler, Cisco Umbrella**.

Q.6.) What are the common type of cyber attacks.

Ans :- **Common Types of Cyber Attacks**

1. **Phishing** – Fraudulent emails or messages trick users into revealing sensitive information like passwords or credit card details.
2. **Malware (Malicious Software)** – Includes viruses, worms, trojans, ransomware, and spyware designed to harm or steal data.
3. **Denial-of-Service (DoS) & Distributed Denial-of-Service (DDoS) Attacks** – Overloads a system, making it unavailable to legitimate users.
4. **Man-in-the-Middle (MitM) Attack** – An attacker intercepts and alters communication between two parties without their knowledge.
5. **SQL Injection (SQLi)** – Attackers insert malicious SQL queries to manipulate databases and extract sensitive data.
6. **Cross-Site Scripting (XSS)** – Injects malicious scripts into websites to steal user data or hijack sessions.
7. **Zero-Day Exploits** – Attacks that target vulnerabilities before developers release a fix.
8. **Brute Force Attack** – Repeatedly guessing passwords or encryption keys until the correct one is found.

9. **Credential Stuffing** – Using stolen usernames and passwords from data breaches to gain unauthorized access.
10. **Ransomware** – Encrypts files and demands payment for their release.
11. **Social Engineering** – Manipulating people into revealing confidential information (e.g., fake tech support scams).
12. **Insider Threats** – Employees or trusted individuals misusing access to harm an organization.

Protection Measures

- Use **strong passwords & MFA** (Multi-Factor Authentication).
- Keep software and systems **updated**.
- Implement **firewalls, antivirus, and endpoint security**.
- **Avoid clicking suspicious links or attachments**.
- **Regular data backups** to prevent data loss.

Q.7.) What is Ransomware ?

Ans :- Ransomware is a type of malware that encrypts files or locks a system, demanding payment (usually in cryptocurrency) to restore access. It is one of the most dangerous cyber threats, often targeting individuals, businesses, and government institutions.

How Ransomware Works

1. Infection – The malware is delivered through phishing emails, malicious downloads, or software vulnerabilities.

2. Execution – Once inside, it encrypts files or locks access to the system.

3. Ransom Demand – A ransom note appears, demanding payment for decryption.

4. Payment & Decryption (Not Guaranteed) – Even if the victim pays, there is no guarantee that the attacker will provide the decryption key.

Types of Ransomware

1. Locker Ransomware – Locks users out of their devices (e.g., screen lockers).
2. Crypto Ransomware – Encrypts files, making them inaccessible.
3. Double Extortion Ransomware

❖ 5 Marks Questions

Q.1.) Explain important of CIA triad.

Ans :- The **CIA Triad** is a core model in cybersecurity that represents the three foundational principles of **information security**: **Confidentiality, Integrity, and Availability**. These principles ensure that systems, networks, and data are protected from unauthorized access, manipulation, and destruction. Let's explore the importance of each element:

1. Confidentiality

- **Definition**: Ensuring that sensitive data is accessible only to those authorized to view it.
- **Importance**:
    - Protects **personal, financial**, and **business-sensitive** data from unauthorized access or disclosure.
    - Prevents **data breaches** where sensitive information, like passwords or financial records, is exposed to attackers.
    - Ensures **compliance** with regulations (e.g., GDPR, HIPAA) that mandate the protection of private data.
- **Example**: Using encryption and access controls to secure files so only authorized employees can view them.

2. Integrity

- **Definition**: Ensuring the accuracy, consistency, and trustworthiness of data, ensuring that it is not altered or tampered with by unauthorized users.
- **Importance**:
    - Ensures that the data remains **correct** and **unmodified**, especially in critical areas like financial transactions, medical records, and contractual agreements.
    - Prevents **cyberattacks** that manipulate data, such as altering financial data or tampering with personal information.
    - Helps maintain **trust** in systems, especially where high stakes are involved (e.g., banking, e-commerce).
- **Example**: Using hash functions, digital signatures, and checksums to verify the integrity of files or messages.

3. Availability

- **Definition**: Ensuring that information and resources are accessible when needed by authorized users.
- **Importance**:
    - Prevents **denial-of-service (DoS) attacks** and ensures that systems remain operational, allowing users to access services when required.
    - Ensures that critical applications, services, and data are always available to users, supporting business continuity.
    - Minimizes downtime and disruption, crucial in sectors like healthcare, finance, and emergency services.
- **Example**: Implementing redundant systems, backups, and failover mechanisms to ensure that critical services are available even in case of hardware failure or cyberattack.

Why is the CIA Triad Important?

1. **Comprehensive Protection**: By balancing **Confidentiality**, **Integrity**, and **Availability**, the CIA Triad provides a holistic approach to safeguarding sensitive information and maintaining trust in systems.

2. **Risk Mitigation**: It helps identify and mitigate risks related to data breaches, corruption, or loss, ensuring that organizations can operate securely and efficiently.
3. **Regulatory Compliance**: Many laws and regulations require organizations to implement practices that protect data, often aligning with the principles of the CIA Triad (e.g., GDPR, HIPAA).
4. **Trust and Credibility**: Organizations that follow the CIA Triad are better equipped to protect their users' data, which builds **trust** and **credibility** with customers, partners, and stakeholders.

Q.2.) Explain working of encryption and decryption tech in cryptography using example.

Ans :- **Encryption** and **decryption** are two core processes in cryptography that help protect sensitive data. They involve converting **plaintext** (readable data) into **ciphertext** (unreadable data) and vice versa. Let's break down how they work using an example.

1. Encryption (Converting Plaintext to Ciphertext)

- **Encryption** is the process of transforming **readable data** (plaintext) into an **unreadable format** (ciphertext) using an algorithm and a key.
- The purpose is to ensure that only authorized users (who possess the decryption key) can access the original data.

How it works:

- **Plaintext**: "HELLO"
- **Encryption Algorithm**: Caesar Cipher (a simple shift cipher).
- **Key**: A number that tells how much to shift the letters. Let's say the key is **3** (this means each letter in the plaintext will be shifted by 3 positions in the alphabet).

Steps:

1. For the letter "H", shift it by 3 positions:
   H → K

2. For "E", shift it by 3 positions:
   E → H
3. For "L", shift it by 3 positions:
   L → O
4. For the second "L", shift it by 3 positions:
   L → O
5. For "O", shift it by 3 positions:
   O → R

So, the ciphertext after applying the Caesar Cipher with a key of 3 is **"KHOOR"**.

Ciphertext: "KHOOR"

2. Decryption (Converting Ciphertext to Plaintext)

- **Decryption** is the process of converting **ciphertext** back to **plaintext** using a decryption key. The decryption key is often the **inverse** of the encryption key.

How it works:

- **Ciphertext**: "KHOOR"
- **Decryption Algorithm**: Caesar Cipher (reverse shift).
- **Key**: **3** (reverse the shift by 3 positions).

Steps:

1. For the letter "K", shift it **back** by 3 positions:
   K → H
2. For "H", shift it **back** by 3 positions:
   H → E
3. For "O", shift it **back** by 3 positions:
   O → L
4. For the second "O", shift it **back** by 3 positions:
   O → L
5. For "R", shift it **back** by 3 positions:
   R → O

After decrypting, you get the **original plaintext**: **"HELLO"**.

Plaintext: "HELLO"

Types of Cryptographic Encryption

1. **Symmetric Key Encryption**:
    - The same key is used for both encryption and decryption.
    - Faster but requires secure key distribution.
    - Example: **AES**, **DES**, **Blowfish**.
2. **Asymmetric Key Encryption**:
    - Uses a **pair of keys**: a **public key** (used for encryption) and a **private key** (used for decryption).
    - The public key can be shared openly, while the private key is kept secret.
    - Example: **RSA**, **ECC**.

Example of Asymmetric Encryption (RSA)

1. **Public Key** (used to encrypt data):
   Imagine Alice wants to send a secure message to Bob. She encrypts the message with Bob's **public key**.
    - **Plaintext**: "HELLO"
    - **Bob's Public Key**: Used by Alice to encrypt the message.

After encryption, the message turns into **ciphertext**.

2. **Private Key** (used to decrypt data):
   Bob receives the encrypted message. He uses his **private key** to decrypt it.
    - **Ciphertext**: Encrypted message.
    - **Bob's Private Key**: Used by Bob to decrypt the message and retrieve the original **plaintext** ("HELLO").

Q.3.) Explain application of cryptography.

Ans :- Cryptography plays a crucial role in securing communications and protecting sensitive information. Here are the **key applications** of cryptography in various fields:

1. Secure Communication

- **Application**: Protecting the privacy of communication over the internet (e.g., emails, instant messaging, and voice calls).
- **How Cryptography Works**:
    - **Encryption** is used to protect the contents of messages so that only the intended recipient can read them.
    - **Public Key Infrastructure (PKI)** and **SSL/TLS** protocols are commonly used to secure web traffic.
- **Example**: **End-to-end encrypted messaging services** (like WhatsApp, Signal) use encryption to ensure that only the sender and receiver can read the messages.

2. Data Protection and Privacy

- **Application**: Ensuring the confidentiality and integrity of sensitive data, whether it's stored on a device or transmitted over a network.
- **How Cryptography Works**:
    - **Data Encryption** ensures that sensitive data such as financial records, personal information, or passwords are protected.
    - **Hash functions** are used to verify the integrity of data, ensuring it hasn't been tampered with.
- **Example**: **Disk encryption tools** like BitLocker or FileVault encrypt the data on a device to protect it from unauthorized access.

3. Digital Signatures

- **Application**: Ensuring the authenticity, integrity, and non-repudiation of digital documents or transactions.
- **How Cryptography Works**:

    - A **digital signature** uses **asymmetric encryption** to sign a document. The signature verifies the identity of the sender and ensures that the document has not been altered.
- **Example**: **E-signatures** for legal agreements, contracts, and electronic forms rely on digital signatures for authentication and security.

4. Authentication

- **Application**: Verifying the identity of users and systems to grant access to resources.
- **How Cryptography Works**:
    - **Passwords** can be securely stored using cryptographic **hashing algorithms** (e.g., SHA-256), making it difficult for attackers to retrieve the original password.
    - **Multi-factor authentication (MFA)** adds an extra layer of security by using a combination of something you know (password) and something you have (a mobile device or a hardware token).
- **Example**: **Two-factor authentication (2FA)** in online services like Google and Facebook, where users authenticate themselves by entering a password and then providing a code sent to their mobile phone.

5. Virtual Private Networks (VPNs)

- **Application**: Providing secure and private communication over public networks.
- **How Cryptography Works**:
    - VPNs use **encryption protocols** such as **IPsec** or **SSL/TLS** to create secure tunnels between the user's device and the remote server, ensuring that no one can intercept or tamper with the data.
- **Example**: **Remote access VPNs** allow employees to securely access company resources from anywhere, even when using public networks like Wi-Fi in coffee shops or airports.

6. Blockchain and Cryptocurrencies

- **Application**: Securing digital currencies and creating decentralized, tamper-proof systems.

- **How Cryptography Works**:
    - **Cryptographic hashing** ensures the integrity of the blocks in a blockchain. Each block is linked to the previous one through a hash, making it nearly impossible to alter the blockchain without detection.
    - **Public-key cryptography** is used to secure cryptocurrency wallets and transactions.
- **Example**: **Bitcoin** and other cryptocurrencies rely on cryptography to secure transactions and control the creation of new units.

7. Secure File Transfer

- **Application**: Sending files securely over a network, ensuring confidentiality and integrity.
- **How Cryptography Works**:
    - Files are **encrypted** before transmission, and **digital signatures** may be used to authenticate the sender.
- **Example**: **SFTP (Secure File Transfer Protocol)** and **HTTPS** are commonly used to securely transfer files over the internet, such as uploading sensitive documents to cloud storage services.

8. Electronic Voting Systems

- **Application**: Ensuring the integrity, anonymity, and authenticity of votes in electronic voting systems.
- **How Cryptography Works**:
    - **Encryption** is used to ensure that votes are **confidential**, and **digital signatures** help authenticate the voter.
    - **Homomorphic encryption** can be used to ensure that votes can be counted without decrypting them, preserving both privacy and integrity.
- **Example**: **E-voting systems** in some countries use cryptography to allow secure online voting while maintaining voter privacy and preventing vote tampering.

9. Secure Payment Systems

- **Application**: Protecting online financial transactions and preventing fraud.
- **How Cryptography Works**:
    - **SSL/TLS** is used to encrypt payment information, ensuring secure communication between the client and server during transactions.
    - **Tokenization** and **public-key cryptography** are used to protect sensitive payment data, such as credit card numbers.
- **Example**: **Online banking, credit card payments, and digital wallets** (e.g., PayPal, Apple Pay) use cryptographic protocols to ensure the security of financial transactions.

10. Secure Software and Firmware Updates

- **Application**: Ensuring that updates to software or firmware are legitimate and not tampered with.
- **How Cryptography Works**:
    - **Digital signatures** are used to verify the authenticity of software updates, ensuring that they come from a trusted source.
    - **Hashing** ensures that the software hasn't been altered during the update process.
- **Example**: **Operating system updates** or **firmware updates** for devices like routers often use cryptography to ensure the integrity and authenticity of the downloaded files.

Q.4.) How do the different types of firewall work.

Ans :- Firewalls are essential components of network security that control incoming and outgoing traffic based on predetermined security rules. They act as barriers between trusted internal networks and untrusted external networks (such as the internet). The way they work depends on their type, and different firewalls use different methods to filter traffic. Here are the different types of firewalls and how they work:

1. Packet-Filtering Firewalls

- **How They Work**:
  Packet-filtering firewalls are the most basic type. They examine each data packet passing through the firewall and compare it against a set of rules (such as allowed IP addresses, ports, and protocols). If a packet matches an allowed rule, it is forwarded; if it does not, the packet is dropped or rejected.
- **Key Characteristics**:
  - Operate at the **network layer** (Layer 3) of the OSI model.
  - Can filter traffic based on IP addresses, port numbers, and protocols.
  - **Stateless**, meaning they do not track the state of the connections (they treat each packet independently).
- **Pros**:
  - Fast and efficient.
  - Simple to configure.
- **Cons**:
  - Limited filtering capabilities.
  - Does not inspect the payload (content) of packets.
  - Vulnerable to IP spoofing and more sophisticated attacks.
- **Example**: A packet-filtering firewall might block all incoming traffic on port 80 (HTTP) unless the packet originates from an allowed IP address.

2. Stateful Inspection Firewalls

- **How They Work**:
  Stateful inspection (also known as dynamic packet filtering) firewalls keep track of the state of active connections. They examine both the header and the state of each packet, ensuring that it is part of a valid ongoing connection. These firewalls maintain a **state table** to monitor the traffic flow.
- **Key Characteristics**:

    - Operate at the **transport layer** (Layer 4).
    - Track the state of connections and monitor each session's integrity.
    - Can filter based on more dynamic and session-specific data.
- **Pros**:
    - More intelligent and secure than packet-filtering firewalls.
    - Can handle complex protocols (e.g., FTP, which opens multiple ports).
- **Cons**:
    - Slower than packet-filtering firewalls due to state-tracking.
    - May still be vulnerable to certain types of attacks like SYN floods.
- **Example**: A stateful inspection firewall may allow an incoming response packet if it corresponds to an outgoing request, thus ensuring it is part of an established connection.

3. Proxy Firewalls (Application-Level Gateways)

- **How They Work**:
  Proxy firewalls act as intermediaries between the internal network and the external network. When a request is made, the proxy server fetches the content on behalf of the user and sends it back, essentially hiding the true identity and network of the user. This process is known as **network address translation (NAT)**. Proxy firewalls can inspect traffic at the **application layer** (Layer 7) of the OSI model, which allows them to understand the specific application being accessed.
- **Key Characteristics**:
    - Act at the **application layer**.
    - Can fully inspect the content of traffic (e.g., HTTP, FTP).
    - Can cache frequently requested content to improve performance.
- **Pros**:
    - Highly effective at blocking application-level attacks (e.g., SQL injection, cross-site scripting).

    - Provides strong protection by isolating the internal network from the internet.
- **Cons**:
    - Can be slow due to the deep inspection of traffic.
    - More complex to configure and maintain.
- **Example**: A proxy firewall can inspect and filter HTTP traffic, ensuring that no malicious content is sent from an external web server to an internal user.

4. Next-Generation Firewalls (NGFW)

- **How They Work**:
  Next-Generation Firewalls combine traditional firewall features with advanced filtering capabilities, such as application awareness, integrated intrusion prevention systems (IPS), and deep packet inspection (DPI). They can analyze the payload and the context of network traffic to detect and block more sophisticated attacks.
- **Key Characteristics**:
    - Include features like **deep packet inspection (DPI)**, **intrusion prevention systems (IPS)**, **VPN support**, and **application-layer filtering**.
    - Can detect and block attacks like malware, ransomware, and advanced persistent threats (APTs).
    - Provides **granular control** over application-specific traffic.
- **Pros**:
    - Provides comprehensive security by combining multiple technologies.
    - Effective at blocking advanced threats like malware and APTs.
    - Offers visibility and control over applications and network traffic.
- **Cons**:
    - More expensive and complex to deploy and manage.

    - May introduce latency due to deep inspection and advanced features.
- **Example**: An NGFW might inspect HTTPS traffic for threats, block malicious web applications, and allow legitimate traffic based on predefined rules.

5. Hybrid Firewalls

- **How They Work**:
  Hybrid firewalls combine the features of stateful inspection firewalls and application-level proxy firewalls. They provide a more integrated approach to filtering, allowing for both deep packet inspection and efficient handling of dynamic connections.
- **Key Characteristics**:
    - A blend of stateful inspection and proxy filtering.
    - Can handle both session-level filtering and application-level filtering.
    - Provides a balanced approach between performance and security.
- **Pros**:
    - Comprehensive security with a balance between performance and deep inspection.
    - Often used in high-security environments.
- **Cons**:
    - Can be resource-intensive, depending on the configuration.
    - Requires careful tuning to ensure both efficiency and security.
- **Example**: A hybrid firewall might inspect application traffic while also maintaining the connection state, allowing it to block advanced threats while still handling complex protocols efficiently.

6. Cloud Firewalls (Firewall-as-a-Service)

- **How They Work**:
  Cloud firewalls, or **Firewall-as-a-Service (FWaaS)**, are hosted in the cloud and protect users and networks by filtering traffic before it reaches

the cloud infrastructure or end-user devices. They offer scalable, centralized management and real-time protection for cloud-based applications and services.

- **Key Characteristics**:
  - Scalable and flexible, typically deployed in cloud environments.
  - Can protect users and devices regardless of their physical location.
  - Often integrated with other cloud security services.
- **Pros**:
  - Easy to scale and manage, especially for distributed environments.
  - Provides comprehensive protection for cloud applications and networks.
- **Cons**:
  - Dependent on cloud infrastructure availability.
  - Can be slower due to traffic being routed through the cloud.
- **Example**: Cloud firewalls protect SaaS applications, remote users, and virtual machines in cloud environments like AWS or Microsoft Azure.

Q.5.) What are the SCS of cyber security.

Ans :- The **SCS** in cybersecurity typically refers to the **"Security Control Standards"** or **"Security Control Systems"** that define the policies, guidelines, and mechanisms for securing IT environments. These controls are often designed to ensure the confidentiality, integrity, and availability of data and systems.

Here are the **types of security control systems** commonly referred to in cybersecurity:

1. Preventive Controls

- **Purpose**: Designed to prevent security incidents or breaches from occurring in the first place.

- **Examples**:
    - **Firewalls**: Control incoming and outgoing traffic based on predefined security rules.
    - **Encryption**: Protects sensitive data by transforming it into unreadable formats.
    - **Access Control**: Restricts unauthorized users from accessing systems and data.
    - **Anti-malware**: Prevents malicious software from infecting systems.

2. Detective Controls

- **Purpose**: Designed to detect and identify any security incidents or unauthorized activity that occurs.
- **Examples**:
    - **Intrusion Detection Systems (IDS)**: Monitors network traffic and system activities for malicious behavior.
    - **Log Analysis**: Analyzing logs to detect unauthorized access or abnormal activities.
    - **Security Monitoring**: Real-time monitoring for security threats or breaches.
    - **Security Cameras**: Physical security measures that detect unauthorized physical access to systems or premises.

3. Corrective Controls

- **Purpose**: Implemented to correct any security issues and mitigate damage after an attack or breach has been detected.
- **Examples**:
    - **Incident Response Plans**: A predefined approach to respond to security incidents, limit damage, and recover quickly.
    - **Patching**: Applying software updates and security patches to fix vulnerabilities.

- **Backup Systems**: Restoring lost or corrupted data after a breach or disaster.
- **Reconfiguration**: Modifying systems or processes to prevent further damage or attacks.

4. Recovery Controls

- **Purpose**: Focus on recovering systems, data, and operations after an incident has occurred, minimizing downtime, and restoring services.
- **Examples**:
  - **Disaster Recovery Plans (DRP)**: A structured approach for recovering IT systems and data after a disaster.
  - **Business Continuity Plans (BCP)**: Ensures that critical business functions continue during and after a cybersecurity incident.
  - **Data Restoration**: Recovering data from backups after data loss or corruption.

5. Compensating Controls

- **Purpose**: Additional controls used when primary security measures are not feasible or effective in mitigating risk.
- **Examples**:
  - **Multi-factor Authentication (MFA)**: Adds an extra layer of security beyond passwords, compensating for weak password security.
  - **Security Audits**: Perform regular security audits and vulnerability assessments to compensate for other controls that may be lacking.
  - **Physical Security Controls**: Physical barriers, such as locked doors or biometric systems, that support the security of IT systems.

Q.6.) How does a computer get infected with Ransomware.

Ans :- A computer can get infected with ransomware through several different methods. Ransomware is a type of malicious software (malware) that encrypts the victim's files and demands a ransom, usually in cryptocurrency, for the

decryption key. The infection process typically involves one or more of the following methods:

1. Phishing Emails

- **How It Works**:
    - Phishing is one of the most common ways ransomware is delivered. Attackers send emails that appear legitimate, often impersonating trusted organizations like banks, service providers, or even coworkers.
    - The email typically contains a malicious attachment (e.g., a Word document, PDF, or ZIP file) or a link to a malicious website.
    - Once the victim opens the attachment or clicks on the link, the ransomware is downloaded and executed on their computer.
- **Example**:
  An email may look like a bank statement, but once the attachment is opened, ransomware is triggered and begins encrypting files.

2. Malicious Websites and Malvertising

- **How It Works**:
    - Malicious websites or **malvertising** (malicious advertising) can infect a computer through drive-by downloads.
    - Simply visiting an infected website or clicking on an advertisement on a legitimate website can lead to the automatic download of ransomware.
    - These websites exploit vulnerabilities in the browser or outdated software (like Flash or Java) to inject ransomware onto the victim's computer.
- **Example**:
  A legitimate website might show an ad infected with malware, which downloads ransomware onto the computer when the user clicks on the ad or simply visits the page.

3. Exploit Kits

- **How It Works**:
  Exploit kits are tools used by cybercriminals to exploit vulnerabilities in software, such as web browsers, plugins, or operating systems.
    - When the user visits an infected website, the exploit kit looks for security holes in their browser or other software.
    - If a vulnerability is found, the exploit kit automatically installs ransomware on the computer.
- **Example**:
  An outdated version of a browser or plugin (e.g., Adobe Flash) may be targeted by an exploit kit, allowing ransomware to be silently installed.

4. Remote Desktop Protocol (RDP) Attacks

- **How It Works**:
  RDP is a feature used to access a computer remotely, and cybercriminals often target weak or exposed RDP credentials.
    - Once attackers gain access through weak passwords or exposed RDP connections, they can manually install ransomware on the compromised system.
    - Brute-force attacks are used to crack weak passwords, or attackers may exploit unpatched vulnerabilities in the RDP service.
- **Example**:
  An attacker guesses the password to an RDP connection and installs ransomware to encrypt files on the victim's computer.

5. Software Vulnerabilities

- **How It Works**:
  Cybercriminals often exploit known vulnerabilities in operating systems or software that have not been patched or updated by the user.
    - Once the vulnerability is exploited, ransomware is delivered and installed on the system.
    - This is often part of a broader attack where ransomware is installed as the final payload after other types of malware have been delivered.

- **Example**:
  An unpatched operating system or software (like Windows) may be exploited to drop ransomware onto the system.

6. Malicious Attachments in Cloud Storage or File Sharing

- **How It Works**:
  Ransomware can also spread through malicious attachments shared via cloud storage services (e.g., Google Drive, Dropbox) or file-sharing platforms.
    - A cybercriminal sends a link to a malicious file or a shared folder containing ransomware, and when the recipient downloads or opens the file, it triggers the infection.
- **Example**:
  A person may receive a link to a shared folder or file, and once they download or open it, ransomware is executed on their machine.

7. Infected Software or Cracked Software

- **How It Works**:
  Ransomware can also be bundled with pirated or cracked software. Cybercriminals often offer free or illegally downloaded software, which may contain ransomware or other types of malware.
    - When the user installs this software, ransomware is silently installed in the background.
- **Example**:
  Someone downloading a cracked version of a popular software tool may unknowingly install ransomware as part of the download.

8. USB Drives and External Devices

- **How It Works**:
  Ransomware can spread through infected USB drives, external hard drives, or other removable media. When these devices are connected to a computer, the ransomware can automatically install itself onto the system.
    - The ransomware can either be run manually (by the user) or exploit vulnerabilities to spread automatically when the device is connected.

- **Example**:
  An infected USB stick is plugged into a computer, and the ransomware is triggered by autorun features or vulnerabilities.

9. Network Propagation

- **How It Works**:
  In some cases, ransomware can spread laterally within a network once it infects one system. It uses network shares, weak credentials, or exploits to move between computers in the network, encrypting files on all connected systems.
    - This type of propagation allows ransomware to affect multiple systems in a corporate environment, making recovery difficult.
- **Example**:
  The ransomware infiltrates a single computer, then uses network shares to spread and encrypt files on other systems within the company's network.