## Question:

**Explain why it is impossible to design a perfectly secure Network & Information System.**

## Answer:

It is impossible to design a perfectly secure Network & Information System due to the following reasons:

1. **Evolving Threats**: Cybersecurity threats are constantly changing. Attackers develop new techniques and exploit previously unknown vulnerabilities, making it impossible to anticipate and counter all potential attacks.
2. **Human Error**: Many security breaches result from mistakes made by users or administrators, such as weak passwords, improper configurations, or falling victim to social engineering attacks. Human behavior is inherently unpredictable and cannot be fully secured.
3. **Complexity of Systems**: Modern systems are highly complex, with multiple interconnected components. This complexity increases the likelihood of vulnerabilities that attackers can exploit. Ensuring every component is secure is practically unachievable.
4. **Resource Limitations**: Implementing security measures involves costs and trade-offs, such as reduced system performance or higher maintenance requirements. Organizations often cannot afford the resources needed for comprehensive security.
5. **Conflict Between Usability and Security**: Strong security measures often make systems harder to use, leading to resistance from users. Balancing usability with security inevitably creates gaps that attackers can exploit.

These challenges ensure that absolute security remains unattainable; instead, the goal is to mitigate risks to an acceptable level through continuous monitoring and updating of security measures.

## Question:

**(b) DETERMINE the following Denial of Service Attacks with the help of example [CLO-2] [6 Marks]**

- **TCP SYN Flooding Attacks**
- **ICMP Flooding**
- **Reflection Attacks**

## Answer:

### *1. TCP SYN Flooding Attacks:*

This attack exploits the TCP three-way handshake mechanism. The attacker sends a large number of SYN (synchronize) packets with spoofed source addresses to the server. The server responds with SYN-ACK (synchronize-acknowledge) packets and waits for the final ACK from the client to complete the handshake. However, since the source addresses are spoofed, no final ACK is received, leaving the connection half-open and consuming server resources.

**Example:**

A web server targeted with SYN packets is forced to hold multiple incomplete connections, filling its connection table. As a result, legitimate users cannot connect because the server cannot handle additional requests.

### *2. ICMP Flooding Attacks:*

This attack overwhelms a server by flooding it with ICMP (Internet Control Message Protocol) packets, such as echo requests (ping). It consumes the target's bandwidth and processing power, leading to denial of service for legitimate traffic.

**Example:**

An attacker sends a continuous stream of ping requests to a victim's server using spoofed IP addresses, causing the server to waste resources on responding to invalid requests instead of serving legitimate users.

### *3. Reflection Attacks:*

In reflection attacks, the attacker sends requests to legitimate servers (reflectors) with the spoofed IP address of the target. These servers respond to the spoofed address (the victim), overwhelming it with traffic.

**Example:**

A DNS reflection attack involves sending small DNS queries to DNS servers with the victim's IP address as the source. The servers respond with large DNS responses, flooding the victim's network.

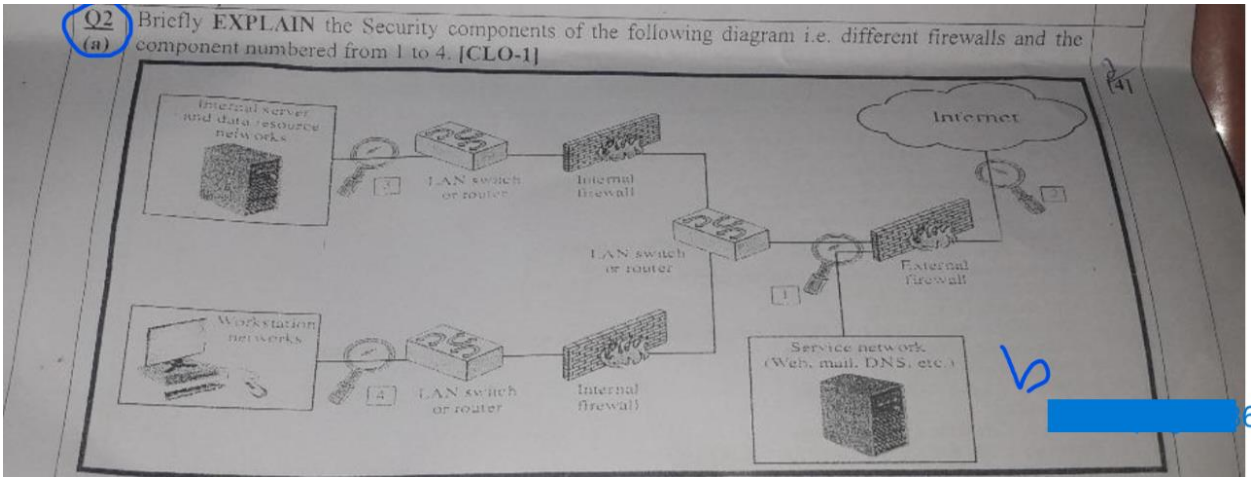
## Key Points:

- **TCP SYN Flood** targets server connection tables.
- **ICMP Flood** exhausts bandwidth and processing capacity.
- **Reflection Attack** uses intermediary servers to amplify the attack on the victim.

This categorization helps in understanding how attackers exploit network protocols to perform DoS attacks.

**Question:**

**Q2(a)** Briefly EXPLAIN the Security components of the following diagram i.e., different firewalls and the components numbered from 1 to 4. [CLO-1]



**Answer:**

1. **External Firewall (Component 1):**
    a. Acts as the first layer of defense between the Internet and the internal network.
    b. Filters incoming and outgoing traffic based on the organization's security policies.
    c. Protects the DMZ (Demilitarized Zone) network from direct external attacks.
2. **Service Network or DMZ (Component 2):**
    a. Includes public-facing services like web servers, mail servers, and DNS servers.
    b. Placed between the external and internal firewalls to provide limited access to external users.
    c. Ensures that attackers cannot directly access the internal network, even if the DMZ is compromised.
3. **Internal Firewall (Component 3):**
    a. Provides an additional layer of security by protecting the internal networks from the DMZ.
    b. Ensures that traffic between the DMZ and internal network adheres to strict security policies.
    c. Prevents malware or compromised systems in the DMZ from infiltrating critical internal resources.
4. **Internal Network (Component 4):**
    a. Consists of workstations, internal servers, and critical data resources.
    b. Protected by the internal firewall to ensure only authorized traffic reaches these sensitive components.
    c. Hosts internal users and applications that need high-level security.

This multi-layered architecture (external firewall, DMZ, internal firewall) ensures a robust security posture by isolating external threats, protecting public services, and safeguarding critical internal systems.

**Question:**

Determine how you will secure a website www.ecommerce.com using PKI and HTTPS by taking into consideration the security requirements of e-commerce websites. (CLO-2)

**Answer:**

To secure www.ecommerce.com using PKI and HTTPS, the following steps will be implemented:

1. **Public Key Infrastructure (PKI):**
    a. **Digital Certificates:** Obtain an X.509 digital certificate from a trusted Certificate Authority (CA). This certificate will validate the identity of the website and provide a public key for secure communication.
    b. **Key Pair Generation:** Generate a private and public key pair. The private key will remain secure with the website server, while the public key will be included in the certificate issued by the CA.
    c. **Certificate Deployment:** Install the digital certificate on the web server hosting the e-commerce site.
2. **Implementing HTTPS:**
    a. **SSL/TLS Protocol:** Configure the web server to support HTTPS by enabling SSL/TLS protocols, which encrypt communication between the client (browser) and server.
    b. **Data Encryption:** Encrypt sensitive information such as login credentials, payment details, and personal data during transmission. This ensures confidentiality and prevents eavesdropping.
    c. **Handshake Process:** Use the TLS Handshake Protocol to securely exchange cryptographic keys between the client and server before starting communication. This will establish a secure session.
3. **Security Measures for E-commerce:**
    a. **Authentication:** PKI ensures the website's authenticity, allowing users to trust the source of the website.
    b. **Integrity:** Use Message Authentication Codes (MAC) provided by TLS to ensure data integrity, preventing tampering during transmission.
    c. **HTTPS Indicators:** Users will see "https://" in the URL and a padlock icon in the browser, enhancing trust and reducing phishing risks.
    d. **Certificate Revocation Checks:** Regularly verify certificate status using CRLs (Certificate Revocation Lists) or OCSP (Online Certificate Status Protocol) to ensure expired or compromised certificates are not used.

By combining PKI and HTTPS, the e-commerce website ensures confidentiality, integrity, and authenticity, meeting the high security requirements essential for online transactions.

**Question:**

Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Explain the examples of confidentiality, integrity, and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement. [CLO-1]

**Answer:**

In an automated cash deposit machine, the following security requirements apply:

1. **Confidentiality** (High Importance):
    a. **Requirement:** The machine must ensure that sensitive user data, such as account numbers, PINs, and transaction details, are encrypted during transmission and storage to prevent unauthorized access.
    b. **Example:** If a user enters their PIN or account number, this data must be encrypted to protect it from interception or disclosure to unauthorized entities.
    c. **Importance:** High, as a breach of confidentiality could lead to financial loss, identity theft, or reputational damage to the bank.
2. **Integrity** (High Importance):
    a. **Requirement:** The machine must ensure that the data entered (e.g., cash deposit amount, account number) is not altered during processing or transmission.
    b. **Example:** A user deposits $500, and the machine records this amount accurately without any tampering. Additionally, the receipt must reflect the exact transaction details.
    c. **Importance:** High, as compromised integrity could result in incorrect account balances or fraudulent transactions, directly affecting users' trust and financial security.
3. **Availability** (Moderate to High Importance):
    a. **Requirement:** The machine must be operational and accessible to users during specified hours, with minimal downtime.
    b. **Example:** If users attempt to deposit cash, the system should be available and functioning to process the transaction promptly without unnecessary delays or system crashes.
    c. **Importance:** Moderate to high, as unavailability during critical times could lead to user dissatisfaction and operational inefficiencies, especially for time-sensitive transactions.

By addressing these three pillars—confidentiality, integrity, and availability—the automated cash deposit machine ensures secure, reliable, and user-friendly financial services.