Question 5

1. Brief describe five possible causes of network security vulnerabilities.

Software:

Failure to apply software updates and security patches promptly can leave systems vulnerable to known exploits and attacks.

Hardware:

Outdated Hardware: Using outdated networking equipment or hardware components without firmware updates can expose the network to security vulnerabilities.

Organization Procedures:

Inadequate implementation of access control policies and procedures can result in unauthorized users gaining access to sensitive network resources.

Personnel:

Employees and personnel who are not adequately trained in cybersecurity best practices may fall victim to social engineering attacks such as phishing, leading to unauthorized access or data breaches.

Physical Environment:

Lack of physical security measures such as access controls, surveillance, and secure storage for networking equipment can result in unauthorized access or tampering with network infrastructure.

1. Discuss why modern business networks are susceptible to security vulnerabilities.

Modern business networks are susceptible to security vulnerabilities due to several factors. Firstly, the increasing complexity of network infrastructures, including interconnected devices and cloud services, creates more entry points for potential attacks. Secondly, the rapid pace of technological advancements often leads to outdated software and hardware, leaving networks vulnerable to known exploits. Additionally, the growing reliance on mobile devices and remote work has expanded the attack surface, making it challenging for organizations to monitor and secure every endpoint effectively. Lastly, the sophistication of cyber threats, such as malware, phishing, and ransomware, continues to evolve, requiring businesses to adopt robust security measures and stay vigilant against emerging threats.

Question (6)

1. Explain the Two steps in user authentication.

* Identification
* Verification

1. Briefly describe the four means of user authentication and give an example of each.

Password-based Authentication:

Users provide a secret password or passphrase known only to them.

Example: Logging into an email account with a combination of letters, numbers, and special characters.

Biometric Authentication:

Uses unique physical or behavioral characteristics of individuals for authentication.

Example: Unlocking a smartphone using fingerprint recognition or facial recognition.

Token-based Authentication:

Involves the use of physical or digital tokens to authenticate users.

Example: Using a hardware token (like RSA SecurID) that generates time-based one-time passwords (OTPs) for logging into a secure system.

Multi-factor Authentication (MFA):

Combines two or more different authentication factors for enhanced security.

Example: Logging into a bank account by entering a password (knowledge factor) and receiving a verification code on a mobile device (possession factor) via SMS.

1. Explain what multi-factor authentication is.

Combines two or more different authentication factors for enhanced security.

1. State Three disadvantage to multi-factor authentication systems.

Complexity for user

Dependency for external factors

Cost and implementation challenges