CSF Answer Key

Q.1 Answer the following.

(a) Short questions (1 mark each)

1. **What is the purpose of encryption in cybersecurity?**
   - Encryption protects data by converting it into a secure format that can only be read by authorized users with a decryption key.
2. **Define a Trojan horse.**
   - A Trojan horse is a type of malware that disguises itself as legitimate software but, when executed, performs malicious actions such as stealing data or damaging systems.
3. **How does MAC filtering help prevent in wireless networks?**
   - MAC filtering restricts access to a network by allowing only devices with approved MAC addresses to connect, thereby preventing unauthorized access.

(b) Objective Type (MCQs/True-False/Fill in the Blanks) (1 mark each)

1. **What does WPA stand for in wireless security?**
   - WPA stands for **Wi-Fi Protected Access**.
2. **True or False:** WPA2 is more secure than WEP. (Justify your answer)
   - **True.** WPA2 uses stronger encryption (AES) and provides better security compared to WEP, which uses weaker encryption (RC4).
3. **Which of the following is a Denial-of-Service (DoS) attack?**
   - **Network flooding** (Answer: c)
4. **Fill in the blanks:** The process of verifying the identity of a user, device, or system is called **Authentication**.
5. **What is the primary function of a firewall in network security?**
   - A firewall **monitors and controls incoming and outgoing network traffic based on security rules** to prevent unauthorized access.
6. **Which command is used to display all active network connections in Windows?**
   - The command **netstat** is used.
7. **What is the main advantage of asymmetric encryption over symmetric encryption?**
   - Asymmetric encryption provides **better security** by using two separate keys (public and private), unlike symmetric encryption, which uses a single key for both encryption and decryption.

Q.2 Answer the following.

(a) Two Questions of 2 Marks

1. **Explain the concept of the CIA Triad in cybersecurity.**

    - The **CIA Triad** stands for **Confidentiality, Integrity, and Availability**:
        - **Confidentiality** ensures that information is accessible only to authorized users.
        - **Integrity** ensures that data is accurate and not altered by unauthorized users.
        - **Availability** ensures that information and systems are accessible when needed.

2. **What is a buffer overflow attack, and how does it work?**

    - A **buffer overflow attack** occurs when a program writes more data into a buffer (temporary storage) than it can hold, causing data to overwrite adjacent memory, which may lead to system crashes or allow attackers to execute malicious code.

(b) Two Questions of 3 Marks

1. **How does Address Space Layout Randomization (ASLR) help in OS security?**

    - ASLR enhances security by **randomizing the memory addresses** of key system components, making it difficult for attackers to predict memory locations for executing exploits like buffer overflow attacks.

2. **Describe how a Man-in-the-Middle (MITM) attack works and how it can be prevented.**

    - **MITM Attack:** An attacker intercepts communication between two parties to steal, alter, or inject malicious data.
    - **Prevention Methods:**
        - Use **HTTPS** instead of HTTP.
        - Employ **VPNs** for encrypted communication.
        - Enable **Two-Factor Authentication (2FA)** for additional security.

Q.3 Attempt any TWO.

1. **Compare and contrast WPA2 and WPA3 security protocols.**
    - **WPA2:** Uses AES encryption but is vulnerable to offline brute-force attacks.
    - **WPA3:** Provides stronger encryption with **Simultaneous Authentication of Equals (SAE)** and protection against dictionary attacks.
2. **Analyze how Zero-Day exploits pose a threat to operating system security.**
    - **Zero-Day Exploit:** A cyber attack targeting software vulnerabilities that developers are unaware of.
    - **Threats:**
        - Attackers can exploit flaws before a patch is released.
        - Can be used for espionage or large-scale cyberattacks.
3. **Assess the security risks associated with public Wi-Fi networks and propose countermeasures.**
    - **Risks:**
        - Data interception through **packet sniffing**.
        - Rogue hotspots set up by attackers.
        - Malware injection via unencrypted traffic.
    - **Countermeasures:**
        - Use **VPNs**.
        - Avoid accessing sensitive accounts over public Wi-Fi.
        - Enable **HTTPS Everywhere** extension.

Q.4 Answer the following.

(a) In what scenarios can applying the elements of the CIA triad together result in conflicts?

- **Scenario 1:** Implementing strong encryption (Confidentiality) might slow down data access (Availability).
- **Scenario 2:** Frequent software updates (Integrity) might require system reboots, affecting uptime (Availability).
- **Scenario 3:** Strict access controls (Confidentiality) may limit data modification permissions, affecting real-time updates (Integrity).

(b) How can social engineering attacks compromise cybersecurity? Discuss different types of social engineering techniques and ways to prevent them.

- **Social Engineering Attacks:** Psychological manipulation to trick users into revealing confidential information.
- **Types:**
  - **Phishing:** Fraudulent emails asking for sensitive data.
  - **Pretexting:** Impersonating authority figures to extract information.
  - **Baiting:** Offering free software with malware.
- **Prevention:**
  - Verify email authenticity.
  - Use **multi-factor authentication** (MFA).
  - Educate users about common scams.

OR

(b) What are password policies, and why are they important in securing user accounts? Provide examples of strong password practices.

- **Password policies** ensure users create secure passwords to prevent unauthorized access.
- **Importance:**
  - Reduces the risk of brute-force attacks.
  - Ensures compliance with security standards.
- **Strong Password Practices:**
  - Use at least **12 characters** with a mix of uppercase, lowercase, numbers, and symbols.
  - Avoid common words or personal information.
  - Use a **password manager** for secure storage.