

# ASS22&23.

1. What does the "CIA Triad" stand for in cybersecurity?

**A) Confidentiality, Integrity, Availability** - The "CIA Triad" stands for these three principles in cybersecurity

2. Which of the following is NOT a type of threat actor?

**C) Packet analyzers** : cause Packet analyzers are tools, not threat actors

3. In which layer of the OSI model does a firewall primarily operate?

**B) Layer 3 (Network)**

Firewalls primarily operate at Layer 3 of the OSI model, filtering traffic based on IP addresses.

4. What is a benefit of using a Security Information and Event Management (SIEM) system?

**B) It provides real-time analysis of security alerts** - SIEM systems are designed for real-time security monitoring and analysis.

5. Which protocol is responsible for encrypting web traffic?

**C) HTTPS**

6. What is the purpose of a VPN in network security?

**B) To provide secure communication over an untrusted network**

7. Which security tool is used for network packet capture and analysis?

B) Wireshark

## 8. What is the primary function of an Intrusion Detection System (IDS)?

**B) To detect suspicious activities in real-time**

IDS is designed to monitor for and detect potential security breaches.

## 9. Which device is used to segment a network into different broadcast domains?

**C) Router**

Routers are used to segment networks into different broadcast domains.

## 10. What kind of attack involves overwhelming a system with traffic to make it unavailable to users?

B) Denial of Service (DoS) attack

## 11. Which type of malware encrypts files on the victim's computer and demands payment to unlock them?

**B) Ransomware**

Ransomware encrypts files and demands payment to unlock them.

## 12. What is the main purpose of cryptographic hashing in cybersecurity?

**C) To verify data integrity**

Cryptographic hashing is used to ensure the integrity of data by verifying that it has not been altered.

## 13. Which of the following is a security best practice for managing user accounts?

**B) Enabling multi-factor authentication (MFA)**

MFA is a best practice for securing user accounts.

14. Which protocol is responsible for network device communication on local networks and translates IP addresses into MAC addresses?

**C) ARP**

The ARP protocol resolves IP addresses to MAC addresses on local networks.

15. What does a vulnerability assessment primarily identify?

**B) Security weaknesses that may be exploited**

A vulnerability assessment identifies weaknesses that could potentially be exploited.