End Semester Security Answers - Detailed

17) Define Authentication and Authorization with Differences

Authentication is the process of verifying the identity of a user or system. It ensures that the person or system is who they claim to be.

Authorization, on the other hand, is the process of granting or denying access to resources based on the user's identity and permissions.

Key Differences:
- Authentication confirms identity, whereas authorization determines what resources a user can access.
- Authentication occurs before authorization.
- Authentication uses credentials like username and password; authorization uses access control policies.
- Example: Login is authentication; accessing an admin dashboard is authorization.

---

18) Explain CIA Triad with Suitable Example

The CIA Triad stands for Confidentiality, Integrity, and Availability, which are the core principles of information security.

- Confidentiality ensures information is accessed only by authorized users (e.g., encrypting sensitive data).
- Integrity ensures data is accurate and unaltered (e.g., using checksums or digital signatures).
- Availability ensures data and resources are accessible when needed (e.g., using backups and redundancy).

---

19) Explain Vulnerability Management Process

Vulnerability management involves identifying, evaluating, and mitigating security weaknesses in systems.

Steps include:

1. Identify vulnerabilities with scanning tools.

2. Evaluate risks and prioritize.

3. Remediate by patching or configuration changes.

4. Verify fixes.

5. Document and report.

---

20) Describe Risk Management Lifecycle

Risk management includes identifying, assessing, mitigating, monitoring, and communicating risks.

Phases:

- Identification of threats.

- Assessment of likelihood and impact.

- Mitigation through controls.

- Continuous monitoring.

- Communication with stakeholders.

---

21) Define Security Policies and its Types

Security policies are formal guidelines for protecting organizational assets.

Types include:

- Acceptable Use Policy (AUP)

- Access Control Policy
- Password Policy
- Email Policy
- Data Retention Policy

---

22) What is Access Control? Explain its Models

Access control restricts user access to resources.

Models:

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)

---

23) What is Malware? Explain its Types

Malware is software designed to damage or exploit.

Types:

- Virus, Worm, Trojan Horse, Ransomware, Spyware, Adware

---

24) What is DoS and DDoS?

Denial of Service (DoS) attacks overload systems; Distributed DoS (DDoS) uses many machines.

Impacts: Downtime, financial loss, reputational damage.

---

25) Explain Cybersecurity Tools

Examples include Wireshark, Nessus, Metasploit, Snort, Burp Suite.

---

26) What is IDS and IPS?

IDS detects threats and alerts; IPS detects and blocks threats.

---

27) Explain Encryption and Decryption with Types

Encryption converts data to unreadable format; decryption reverses it.

Types:

- Symmetric (same key)
- Asymmetric (public/private keys)

---

28) Explain Firewall and its Types

Firewalls monitor and control network traffic.

Types:

- Packet Filtering
- Stateful Inspection
- Proxy Firewalls
- Next-Gen Firewalls

---

29) What is VPN? Explain its Benefits

VPN creates a secure tunnel over public networks.

Benefits:

- Privacy, data protection, remote access, bypass geo-restrictions

---

30) Define Social Engineering and its Types

Social engineering manipulates people to gain confidential info.

Types:

- Phishing, Pretexting, Baiting, Tailgating

---

31) What is Data Encryption Standard (DES)?

DES is a symmetric-key algorithm for encrypting data, now largely replaced due to short key length.

---

32) Explain SSL/TLS Protocol

SSL/TLS protocols secure internet communication through encryption and authentication.

---

33) What are the Types of Cyber Attacks?

Includes Malware, Phishing, Man-in-the-middle, DoS/DDoS, SQL Injection, XSS, Password Attacks.

---

34) Define Ethical Hacking and its Phases

Ethical hacking involves authorized attempts to find vulnerabilities.

Phases:

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

---

35) Explain Cyber Forensics

Cyber forensics is the investigation of cyber crimes by collecting and analyzing digital evidence.

---

36) What is Two-Factor Authentication?

Two-factor authentication requires two forms of identification for access, increasing security.

---

37) Define Blockchain Technology

Blockchain is a decentralized ledger of transactions, ensuring transparency and immutability.

---

38) Explain Cloud Computing Models

Models include IaaS, PaaS, SaaS, each offering different levels of service.

---

39) What is Malware Analysis?

Malware analysis studies malicious software to understand behavior and develop defenses.

Types: Static, Dynamic, Behavioral.

---

40) Describe the Principle of Least Privilege

This principle states users should have only the minimum access necessary.

---

41) Explain the concept of Public Key Infrastructure (PKI)

PKI manages digital certificates and keys to enable secure communications.

Components:

- Certificate Authority (CA)
- Registration Authority (RA)
- Digital Certificates
- Public/Private Keys
- Certificate Repository

---

42) What are Honeypots? Explain their types

Honeypots are decoy systems to lure attackers.

Types:

- Low-Interaction
- High-Interaction
- Research
- Production

---

43) What is Phishing? How to Prevent it?

Phishing tricks users to disclose sensitive info.

Prevention includes awareness, filters, verification, MFA.

---

44) Define SQL Injection and its Prevention Techniques

SQL Injection is an attack inserting malicious code in inputs.

Prevention:

- Parameterized queries
- Input validation
- Least privileges

---

45) Explain Cross-Site Scripting (XSS) and its types

XSS injects malicious scripts into websites.

Types:

- Stored, Reflected, DOM-based

---

46) What is Malware Analysis? Types

Malware analysis examines malware.

Types:

- Static, Dynamic, Behavioral

---

47) Explain the concept of Data Leakage and Prevention Methods

Data leakage is unauthorized data transfer.

Prevention:

- DLP tools, encryption, access control, monitoring, training

---

48) What are Botnets? How do they operate?

Botnets are networks of infected computers controlled remotely.

Operation includes infection, C&C communication, attack execution.

---

49) Describe the Cybersecurity Incident Response Process

Incident response involves preparation, identification, containment, eradication, recovery, and lessons learned.