**Course- 4**

**Network Security & Database Vulnerabilities**

**Network Security:**

1. Firewalls:

- Definition: Firewalls act as a barrier between a trusted internal network and untrusted external networks.

- Purpose: Prevent unauthorized access and filter incoming/outgoing traffic.

2. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS):

- IDS monitors network/system activities for malicious actions.

- IPS actively blocks or prevents detected malicious activities.

3. Virtual Private Network (VPN):

- A secure way to connect remote users or offices to a private network over the internet.

- Encrypts the communication to ensure confidentiality.

4. Network Segmentation:

- Dividing a network into segments to contain and prevent the lateral movement of attackers.

- Enhances overall security by limiting the potential impact of a breach.

5. Secure Wi-Fi Protocols:

- Ensure the use of WPA3 for Wi-Fi security.

- Regularly update Wi-Fi passwords and use strong encryption.

6. Denial of Service (DoS) and Distributed Denial of Service (DDoS) Protection:

- Implement strategies to mitigate and prevent DoS and DDoS attacks.

- Use traffic filtering and rate limiting to reduce the impact.

7. Network Access Control (NAC):

- Controls devices' access to a network based on security policies.

- Ensures only authorized and compliant devices can connect.

8. Security Best Practices:

- Regularly update and patch network devices.

- Conduct security audits and vulnerability assessments.

- Monitor network traffic for anomalies.

Database Vulnerabilities:

1. SQL Injection:

- Attackers inject malicious SQL code into input fields to manipulate or gain unauthorized access to a database.

- Prevention involves using parameterized queries and input validation.

2. Cross-Site Scripting (XSS):

- Malicious scripts are injected into web applications viewed by other users.

- Implement input validation and output encoding to prevent XSS attacks.

3. Database Encryption:

- Protect sensitive data by encrypting it at rest and in transit.

- Use Transparent Data Encryption (TDE) for database files.

4. Access Control and Least Privilege:

- Limit database user permissions to the minimum required for their tasks.

- Regularly review and update access controls.

5. Database Auditing:

- Implement auditing to track database activities and detect potential security incidents.

- Monitor and review audit logs regularly.

6. Patch Management:

- Keep the database management system and associated software up-to-date.

- Apply patches promptly to address known vulnerabilities.

7. Backup and Recovery:

- Regularly backup databases to ensure data integrity and availability.

- Test and validate the backup and recovery process.

8. Data Masking and Redaction:

- Mask sensitive data to protect confidentiality during testing or non-production use.

- Redact or obscure sensitive information in reports or outputs.