Week 9 Revision notes

Week 9 - Service Level Agreements (SLAs) and Network Security (Part 2)

1. Service Level Agreement (SLA)

- **Definition of SLA**:
  - A **Service Level Agreement (SLA)** is a contract between a service provider and a client.
  - It defines the quality, availability, and responsibilities of the services provided.
- **Purpose of SLAs**:
  - Clearly defines expectations for both the client and provider, preventing misunderstandings.
  - Establishes measurable service metrics and remedies for contract breaches.
  - Ensures accountability and improves trust in service relationships.

2. Key Elements of an SLA

- **Objectives**: Outlines the main goals of the service.
- **Service Descriptions**: Details of the specific services covered by the SLA.
- **Provider's and Client's Duties**: Each party's responsibilities to maintain service quality.
- **Performance Metrics**: Quantifiable standards to measure service performance.
- **Response Time**: Specifies the time frame for the provider's response.
- **Penalties/Remedies**: Specifies consequences for failing to meet SLA terms, such as service credits.

3. Important SLA Metrics

- **Network Availability**:
  - Measured as the percentage of time a network is operational.
  - Industry standard is **99.999% uptime**, translating to about 5 minutes of downtime per year.
  - Formula: ((\text{Operational Hours} ÷ 8760) × 100).
- **Network Performance**:
  - **Bandwidth**: The maximum data capacity of the network, measured in bits per second (bps).
  - **Throughput**: The actual data successfully delivered, reflecting network efficiency.
- **Latency**: Time taken for data to travel from source to destination (measured in milliseconds).

- **Jitter**: The variation in delay between data packet deliveries.
- **Packet Loss**: The percentage of data packets that fail to reach their destination.

4. Network Security Overview

- **Network Security Policy**:
  - A document outlining rules for accessing a company's information resources.
  - Protects data and assets against internal and external threats, enhancing trust and credibility.
- **The CIA Triad**:
  - **Confidentiality**: Ensures data access is restricted to authorized users.
  - **Integrity**: Protects data accuracy and prevents unauthorized modification.
  - **Availability**: Ensures that authorized users have consistent access to data.

5. Types of Security Controls

- **Administrative Controls**: Policies and guidelines that direct secure practices (e.g., employee training).
- **Physical Controls**: Physical barriers to secure network resources (e.g., locks, biometric scanners).
- **Technical Controls**: Technology-based defenses like firewalls, encryption, and authentication.

6. Authentication, Authorization, and Auditing (AAA)

- **Authentication**: Verifies the identity of a user.
  - **Multi-Factor Authentication (MFA)** includes:
    - **Knowledge**: Something you know (e.g., password).
    - **Possession**: Something you have (e.g., smartphone).
    - **Inherence**: Something you are (e.g., fingerprint).
- **Authorization**: Defines what authenticated users can access.
  - Specifies user permissions to access specific resources or data.
- **Auditing**: Logs security events to detect unauthorized activities.
  - Enables tracking of user actions to verify compliance and detect abnormal behaviors.

7. Encryption

- **Purpose of Encryption**:

    - Secures data in transit and at rest by converting it into unreadable ciphertext.
    - Protects data against unauthorized access and ensures data integrity.
- **Types of Encryption**:
    - **Symmetric Encryption**: Uses the same key for both encryption and decryption.
    - **Asymmetric Encryption (Public Key Cryptography)**: Uses a public key for encryption and a private key for decryption.
- **Digital Signatures**:
    - Verifies message authenticity and integrity.
    - Created by hashing a message and encrypting the hash with the sender's private key.

8. Public Key Infrastructure (PKI)

- **PKI Purpose**:
    - A framework of policies and technologies for creating, managing, and distributing digital certificates.
- **Certification Authority (CA)**:
    - A trusted third party that issues digital certificates to verify a public key's ownership.
    - Ensures each public key is correctly linked to its owner, preventing identity substitution.
- **Digital Certificates**:
    - Digital documents that confirm the ownership of a public key, containing information like the issuer, validity period, and owner's public key.

9. Virtual Private Networks (VPNs)

- **Purpose of VPN**:
    - Creates a secure "tunnel" over the internet, allowing secure access to a private network.
    - **Types of VPN Connections**:
        - **Site-to-Site**: Connects two networks securely over the internet.
        - **Client-to-Site**: Allows individual clients to connect to a network remotely.
- **Benefits of VPN**:
    - Ensures data confidentiality and integrity through encryption.
    - Reduces the need for expensive leased lines by providing secure internet-based connections.

10. Firewalls

- **Firewall Purpose**:

- A firewall monitors and controls incoming and outgoing network traffic based on security rules.
- **Types of Firewalls**:
  - **Hardware vs. Software**:
    - **Hardware Firewall**: Dedicated device between LAN and external network.
    - **Software Firewall**: Installed on individual devices to protect them directly.
  - **Stateless (Packet Filtering)**: Filters packets individually based on header information.
  - **Stateful**: Tracks active sessions, allowing packets that are part of valid connections.
  - **Application Layer**: Inspects the application data for malicious content.

11. Intrusion Detection and Prevention Systems (IDS/IPS)

- **Intrusion Detection System (IDS)**:
  - Monitors network traffic for malicious activities and sends alerts.
  - **Types**:
    - **Network-Based IDS (NIDS)**: Protects entire networks by analyzing traffic at the network perimeter.
    - **Host-Based IDS (HIDS)**: Protects individual devices by monitoring OS and application logs.
- **Intrusion Prevention System (IPS)**:
  - An active system that takes action to block or counter detected threats, such as resetting connections or reconfiguring firewalls.

12. Types of Security Solutions

- **Preventative**:
  - Blocks unauthorized network activities before they occur (e.g., firewalls, IPS).
- **Detective**:
  - Identifies and alerts on unauthorized activities in progress or after occurrence (e.g., IDS, honeypots).
- **Corrective**:
  - Repairs damage or restores functionality after a security breach (e.g., patching, rebooting systems).

Summary

- An SLA defines the service standards and expectations between a client and provider, including

remedies for underperformance.

- Network security relies on policies, controls, and security mechanisms to protect data and systems.
- Key mechanisms like authentication, encryption, VPNs, firewalls, IDS/IPS, and auditing are crucial for ensuring network integrity, confidentiality, and availability.