Advanced Cybersecurity Concepts

1. Mitigation in Reference to Cyber Security

Mitigation refers to the strategies, tools, and processes used to reduce the impact of cyber threats and vulnerabilities. It includes:

Preventive measures (e.g., firewalls, antivirus, patching)

Detection (e.g., IDS/IPS, logging)

Response (e.g., isolating affected systems)

Recovery (e.g., backups, disaster recovery plans)

Goal: Reduce damage, restore normal operations quickly, and prevent future attacks.

2. Difference Between IDS & IPS

Feature	IDS (Intrusion Detection System)	IPS (Intrusion Prevention System)
Function	Detects and alerts	Detects and blocks
Placement	Passive (monitoring only)	Inline (between source & target)
Action	Sends alerts/logs	Stops malicious traffic
Impact on traffic	No impact	May introduce slight delay
Example Tools	Snort (IDS mode), Suricata	Snort (inline), Suricata, Cisco IPS

3. Network-Based IDS (NIDS)

A Network-Based IDS monitors traffic on a network segment to detect suspicious activity in real time.

Key features:

Placed at strategic points (e.g., near firewalls or routers)

Analyzes packets (headers and sometimes payload)

Detects anomalies like DoS attacks, port scans, and malware traffic

Examples: Suricata, Snort, Zeek

4. How SSL & TLS Work

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are cryptographic protocols used to secure communication over the internet, like HTTPS.

How they work:

Handshake Phase:

Client sends request to server.

Server responds with certificate (includes public key).

Client verifies certificate.

Key Exchange:

Client and server agree on a session key (symmetric key).

Encryption:

All further communication is encrypted using that session key.

TLS is the modern, secure version of SSL.

5. Symmetric vs. Asymmetric Key Cryptography

Feature	Symmetric Key	Asymmetric Key
Keys Used	Same key for encryption/decryption	Public key + private key
Speed	Fast	Slower
Example Algorithms	AES, DES, Blowfish	RSA, ECC
Key Management	Hard to manage at large scale	Easier for secure sharing
Use Cases	File encryption, VPNs	Email security, SSL certificates

6. How to Secure Server and Personal Computers

For Servers:

Keep software and OS updated

Use firewalls and intrusion detection

Implement access controls (least privilege)

Use SSL/TLS for secure connections

Regular backups

Monitor logs and alerts

For Personal Computers:

Install reputable antivirus/anti-malware

Keep OS and applications updated

Avoid downloading from unknown sources

Use strong passwords and 2FA

Use a VPN on public Wi-Fi

Enable firewalls

7. Explain Suricata and SolarWinds

Suricata:

An open-source IDS/IPS and network security monitoring engine.

Supports multi-threading, deep packet inspection, file extraction, and TLS/HTTP/SMTP inspection.

Developed by OISF (Open Information Security Foundation).

SolarWinds:

A company offering IT management software.

Known for tools like Network Performance Monitor, Log Analyzer, etc.

Gained attention during the SolarWinds cyberattack (2020) where attackers inserted a backdoor (SUNBURST) into its Orion software.

8. Describe VPN and IPSec
VPN (Virtual Private Network):

Creates a secure tunnel over public networks.

Hides your IP address and encrypts data.

Used for remote access and anonymity.

IPSec (Internet Protocol Security):

A protocol suite used to secure IP communications.

Works in two modes:

Transport Mode – Encrypts only the payload

Tunnel Mode – Encrypts entire packet (used in VPNs)

Provides:

Authentication

Integrity

Encryption