Advanced Cyber Security Concepts

## 1. Explain Mitigation in reference to Cyber Security.

Mitigation involves implementing measures to reduce the impact and risk of cyber threats through prevention, detection, and response strategies.

## 2. What are the differences between IDS & IPS?

IDS (Intrusion Detection System) monitors and alerts on suspicious activities, while IPS (Intrusion Prevention System) detects and actively blocks threats.

## 3. Explain NETWORK-based IDS

A network-based IDS monitors traffic across an entire network for malicious activity by analyzing packet data and network behavior.

## 4. Explain How SSL & TLS work?

SSL and TLS secure communications by encrypting data between client and server. They use certificates and key exchange to establish a secure session.

## 5. What is Symmetric Key Cryptography and Asymmetric Key Cryptography?

Symmetric uses one key for encryption and decryption; Asymmetric uses a public key to encrypt and a private key to decrypt.

## 6. Explain How to Secure Server and Personal Computers.

Use firewalls, antivirus, OS updates, strong passwords, encryption, and disable unused services to protect servers and personal computers.

## 7. Explain the Suricata, and SolarWinds.

Suricata is an open-source IDS/IPS tool; SolarWinds provides network monitoring and cybersecurity management tools.

## 8. Describe the VPN and IPSec.

VPN creates a secure tunnel over the internet; IPSec is a protocol suite used to secure VPN connections via encryption and authentication.