CS - Cryptography and Network Security

**1. Explain Mitigation in Reference to Cyber Security**

**Mitigation** in cybersecurity refers to the actions taken to **reduce the risk, impact, or severity** of cyber threats and attacks.

**Examples:**

* Installing **firewalls** and **antivirus software**
* Applying **security patches**
* Using **Multi-Factor Authentication (MFA)**
* Conducting **regular security audits**
* Employee **cybersecurity training**

**2. What is the Difference Between IDS & IPS?**

| **Feature** | **IDS (Intrusion Detection System)** | **IPS (Intrusion Prevention System)** |
| --- | --- | --- |
| Purpose | Detect intrusions | Detect and prevent intrusions |
| Action | Monitors and alerts | Monitors, alerts, and **blocks** |
| Placement | Out-of-band (passive) | In-line (active) |
| Response | No automatic blocking | Blocks suspicious traffic in real-time |
| Example | Snort (IDS mode), Suricata | Cisco IPS, Snort (in IPS mode) |

**3. Explain Network-Based IDS (NIDS)**

**NIDS** monitors **network traffic** for malicious activity in real time.

**How it works:**

* Placed at key points (e.g., gateway, DMZ)
* Analyzes packets for known attack patterns (signatures)
* Raises alerts when suspicious behavior is detected

**Examples:** Snort, Suricata

**4. Explain How SSL & TLS Work**

* **SSL (Secure Sockets Layer)** and **TLS (Transport Layer Security)** are cryptographic protocols that provide **encryption**, **authentication**, and **data integrity** over the internet.

**How they work:**

1. **Handshake Phase:**
   * Client sends a request with supported cipher suites
   * Server responds with its digital certificate
   * Client verifies certificate using CA
2. **Key Exchange:**
   * Shared secret is generated using asymmetric encryption
3. **Session Established:**
   * Secure communication continues with **symmetric encryption**

TLS is the **successor of SSL**. SSL is now deprecated.

**5. What is Symmetric Key Cryptography and Asymmetric Key Cryptography**

| **Feature** | **Symmetric Key** | **Asymmetric Key** |
| --- | --- | --- |
| Keys Used | Same key for encrypt/decrypt | Public & private key pair |
| Speed | Fast | Slower |
| Key Sharing Issue | Needs secure channel | Public key can be shared freely |
| Examples | AES, DES | RSA, ECC |

**6. How to Secure Server and Personal Computers**

**To Secure Servers:**

* Use **firewalls** and **IDS/IPS**
* Keep OS and software **updated**
* Disable **unused ports and services**
* Implement **strong password policies**
* Enable **logging and monitoring**
* Use **TLS/SSL** for secure connections

**To Secure Personal Computers:**

* Install **antivirus and antimalware**
* Enable **Windows Defender Firewall**
* Avoid downloading from untrusted sources
* Use **strong, unique passwords**
* Apply **software updates regularly**
* Use **VPN** on public networks

**7. Explain Suricata and SolarWinds**

**Suricata:**

* An **open-source IDS/IPS/NSM** (Network Security Monitoring) tool
* Supports **multi-threading**
* Detects malicious traffic using **rules/signatures**
* Can work as an **IDS or IPS**
* Supports protocols like HTTP, TLS, DNS, and SMB

**SolarWinds:**

* A commercial **IT management platform**
* Tools include:
  + **Network Performance Monitor**
  + **Security Event Manager (SIEM)**
  + **Log Analyzer**
* Monitors performance, detects threats, and helps in **network visibility and security**

**8. Describe VPN and IPSec**

**VPN (Virtual Private Network):**

* Creates a **secure, encrypted tunnel** between your device and the internet
* Hides IP address and encrypts data
* Used for secure remote access

**IPSec (Internet Protocol Security):**

* A protocol suite that **encrypts and authenticates IP packets**
* Used in **site-to-site** and **remote-access VPNs**
* Works in two modes:
  + **Transport Mode:** Encrypts only the data
  + **Tunnel Mode:** Encrypts data + header