**Module : 4 Wireless And Android Hacking**

1. Explain Mitigation in Reference to Cyber Security

Mitigation in cyber security refers to measures and strategies implemented to reduce the severity, impact, or likelihood of cyber threats.

* Examples:
  + Applying patches for software vulnerabilities.
  + Implementing firewalls and intrusion prevention systems (IPS).
  + Conducting regular security awareness training.

2. What is the Difference Between IDS & IPS?

| Feature | IDS (Intrusion Detection System) | IPS (Intrusion Prevention System) |
| --- | --- | --- |
| Purpose | Detects potential intrusions and alerts administrators. | Prevents intrusions by blocking malicious traffic. |
| Placement | Passive; monitors and analyzes network traffic. | Active; placed inline to inspect and filter traffic. |
| Response | Alerts only; requires manual intervention. | Automatically blocks or drops malicious traffic. |
| Impact on Traffic | Does not affect traffic flow. | Can affect traffic flow due to inline placement. |

3. Explain Network-Based IDS (NIDS)

NIDS monitors network traffic for suspicious activities and generates alerts for potential threats.

* How It Works:
  + Placed at critical points like routers or switches.
  + Analyzes packet data for signatures, patterns, or anomalies.
* Example Tools: Snort, Suricata.

4. Explain How SSL & TLS Work

* SSL (Secure Sockets Layer): An older protocol to encrypt data between a client and server.
* TLS (Transport Layer Security): The modern, secure version of SSL.
* How They Work:
  1. Handshake:
     + Client sends a "Hello" message to the server with supported ciphers.
     + Server responds with its certificate and chosen cipher.
  2. Key Exchange:
     + A session key is securely exchanged **using asymmetric encryption.**
  3. **Data Encryption:**
     + **Symmetric encryption is used for fast, secure communication.**

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

| **Feature** | **Symmetric Key Cryptography** | **Asymmetric Key Cryptography** |
| --- | --- | --- |
| **Keys Used** | **Single key for encryption and decryption.** | **Public and private key pair.** |
| **Speed** | **Faster due to simpler algorithms.** | **Slower due to complex calculations.** |
| **Use Case** | **Encrypting large volumes of data.** | **Secure key exchange or digital signatures.** |
| **Examples** | **AES, DES.** | **RSA, ECC.** |

**6. Explain How to Secure Servers and Personal Computers**

1. **Servers:**
   * **Use firewalls and IDS/IPS.**
   * **Regularly patch and update software.**
   * **Implement strong access controls.**
   * **Encrypt sensitive data.**
2. **Personal Computers:**
   * **Install antivirus software.**
   * **Enable operating system updates.**
   * **Use strong passwords and multi-factor authentication.**
   * **Avoid clicking on unknown links or downloading from untrusted sources.**

**7. Explain Suricata and SolarWinds**

* **Suricata: An open-source intrusion detection, prevention, and network monitoring tool.**
  + **Features: Signature-based and anomaly-based detection, multi-threading for high performance.**
* **SolarWinds: A suite of network management tools, often used for monitoring and managing infrastructure.**
  + **Features: Network performance monitoring, log analysis, and security event tracking.**

**8. Describe VPN and IPSec**

* **VPN (Virtual Private Network): A secure tunnel for transferring data between a user and a network over the internet.**
  + **Use: Hides IP address, encrypts traffic, and ensures privacy.**
* **IPSec (Internet Protocol Security): A protocol suite for securing IP communications.**
  + **How It Works:**
    1. **Authentication Header (AH): Ensures data integrity and authenticity.**
    2. **Encapsulating Security Payload (ESP): Provides encryption and optional authentication.**
  + **Common Use: IPSec is often used in VPNs for secure communication**