# Assignment -3

1) Describe the key differences between intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Ans:

**IDS vs. IPS: Key Differences**

- **Response:** IDS detects, IPS prevents attacks.
- **Use Cases:** IDS for monitoring, IPS for critical systems.
- **Pros/Cons:** IDS - no disruption, manual work; IPS - proactive, potential slowdowns.

2) Design a hypothetical network architecture for a medium-sized enterprise and outline how you would integrate both intrusion detection and prevention mechanisms. Consider factors such as placement of sensors, types of detection techniques (e.g., signature-based, anomaly-based), and strategies for blocking or mitigating identified threats.

Ans:

**Network Architecture with IDS/IPS**

**Scenario:** A medium-sized enterprise with a central office and remote workers.

**Network Design:**

- Core router for internet and internal traffic.
- Distribution switches manage departments.
- Access controls wired/wireless access (incl. VPN).
- Firewalls at perimeter and between segments.
- Optional DMZ isolates public servers.

**IDS/IPS Integration:**

- Placed at key points:
  - Inline on core/distribution for blocking (IPS).
  - Sniffing on dedicated tap for monitoring (IDS).
- Uses signature-based and anomaly-based detection.
- Blocks threats (IPS), alerts for investigation, or integrates with firewalls for automatic blocking.

**Management:**

- Centralized console for IDS/IPS devices.
- Alert prioritization and logging for analysis.

- Regular updates for signature and software.

3) Analyse the impact of social engineering attacks on individuals and organizations, considering factors such as financial losses, reputational damage, and compromised data security.

Ans:

Social engineering attacks exploit human psychology to manipulate individuals into compromising security. These attacks can have devastating consequences for both individuals and organizations.

**Individuals** face financial losses (stolen money, identity theft), emotional distress, and data breaches.

**Organizations** suffer financial losses (fines, stolen data), reputational damage, data breaches, and operational disruption (ransomware).

**India**'s culture of respect and limited awareness make it especially vulnerable.

**Mitigation:**

- Educate individuals and organizations about social engineering tactics.
- Implement strong security policies (emails, attachments, phone calls).
- Combine technical security (firewalls) with user education.
- Promote a culture of security within organizations.

4) Compare and contrast the characteristics of malware and ransomware attacks, including their methods of propagation, objectives, and potential consequences for victims. Evaluate the effectiveness of proactive measures such as regular software updates, antivirus software, and user awareness training in preventing and mitigating the impact of these types of cyber threats.

Ans:

**Malware vs. Ransomware: A Comparative Analysis**

While both malware and ransomware wreak havoc on computer systems, they differ in their functionalities and objectives. Here's a breakdown:

| Feature | Malware | Ransomware |
|---|---|---|
| Objective | Disrupt, damage, steal data | Encrypt data, extort ransom payment |
| Propagation methods | Phishing emails, infected attachments, USBs, downloads | Phishing emails, infected attachments, exploit kits |

| | | |
|---|---|---|
| Impact on victim | Data loss, system crashes, identity theft | Encrypted data, inaccessible systems, financial loss |
| Financial Impact | Varied (data recovery, lost productivity) | Ransom payment, potential data loss recovery |

**Effectiveness of Proactive Measures:**

- **Regular Software Updates:** Patch vulnerabilities.
- **Antivirus Software:** Real-time protection, may miss new attacks.
- **User Awareness Training:** Reduces infection risk.

**Combined Approach is Key:**

A layered defence with updates, antivirus, and training is crucial. Backups and incident response plans aid recovery.

**Concise Comparison:**

- **Malware:** Disrupts, damages, steals data. Spreads through various methods. Impacts vary.
- **Ransomware:** Encrypts data to extort ransom. Spreads similarly to malware. Encrypted data and potential financial loss.

5) How has the IT Act of 2000, along with its subsequent amendments, shaped the legal landscape for addressing cyber-crime and offenses in India? Discuss the key provisions of the Act related to cyber-security and examine their effectiveness in prosecuting cyber-criminals and protecting individuals and organizations from cyber threats

Ans:

The IT Act of 2000, with amendments, shapes India's cybercrime landscape.

**Key Provisions:**

- Legalizes electronic transactions.
- Defines cyber offenses (hacking, data breaches, etc.).
- Limits intermediary liability (controversial).
- Enables digital forensics.
- Mandates data security for some sectors.

**Effectiveness:**

- Established a foundation for prosecution.
- Promoted digital commerce.

- Intermediary liability creates ambiguity.
- Data security measures fall short.
- Doesn't address new threats fully.

**Challenges:**

- Keeping pace with cybercrime evolution.
- Shortage of trained cybercrime professionals.
- Data localization debates add complexity.

**Looking Ahead:**

- Regular amendments are necessary.
- Strengthen enforcement capabilities.
- Public-private collaboration is key.