→ Difference b/w Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

1) Detection vs Prevention

- IDS - monitors network traffic and System activ to identify suspicious patterns or anomalies that may indicate a breach.
- IPS - It blocks and prevents malicious traffic from entering or leaving malicious traffic.

2) Passive vs Active response

- IPS - functions in an active mode, monotrs and insp network traffic in real-time.
- IDS - functions in passive mode, where it observes and analyze network traffic without interfering with it.

→ Hypothetical Network for a Medium Enterprise

- Internet gateway
- Perimeter Network - Demilitarized Zone, VPN gateways
- Internal Network
- Placements of Sensors
- Types of Detection Techniques
- Blocking or Mitigating Identified
- Security Analysts review

→ Impact of social engineering attacks

- Financial Losses
- Organizations losses
- Reputational Damage
- Compromised Data Security
- Identity Theft

→ Overview of key provisions related to IT act, Cyber security and effectiveness.

1) Key provisions of IT act

- Cyber-Crimes
- Security Breaches
- Liabilities
- electronic Signatures

- Digital Evidence

ii) Effectiveness in Prosecuting Cyber-Criminals

- Legal Framework
- Deterrent effect
- Challenges in Enforcement

iii) Protection of Individuals and organizations

- Data protection
- Security Awareness
- legal Recourse