**Week 4: Firewalls, IDS, and IPS**

**Objective:** Set up and manage network defense mechanisms.

**Task#03: Set up Snort IDS on a Linux system — capture and view network alerts.**

**Solution:**

Snort is a widely used, open-source **Network Intrusion Detection System (NIDS)**. It operates by **monitoring network traffic in real-time** and comparing it against a comprehensive set of **rules (signatures)** that define known attack patterns or suspicious activities.

When Snort detects a match, it generates an alert, which can be displayed on the console or logged to a file for further analysis. It's primarily a signature-based system, making it effective at identifying known threats. While typically used for detection, it can also function as a Network Intrusion Prevention System (NIPS) when configured in inline mode to actively block threats.

 