ALLIANCE UNIVERSITY
Private University established in Karnataka State by Act No.34 of year 2010
Recognized by the University Grants Commission (UGC), New Delhi

Celebrating 25 SILVER JUBILEE years of Alliance Education

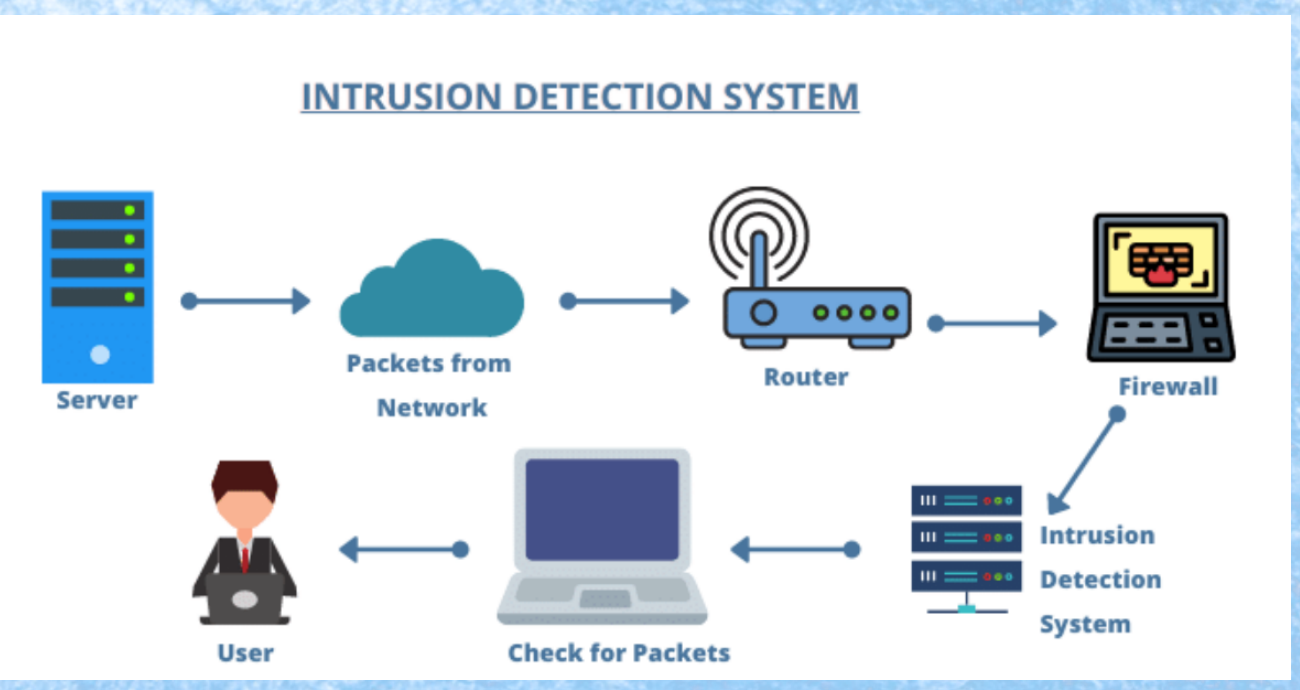
Intrusion Detection System

Presented By, Prem Kumar S (L20030141CSE107),
Nikesh Sharma (20030141CSE074)

What is IDS?

An intrusion detection system (IDS) is a system that monitors network traffic for suspicious activity and alerts when such activity is discovered.

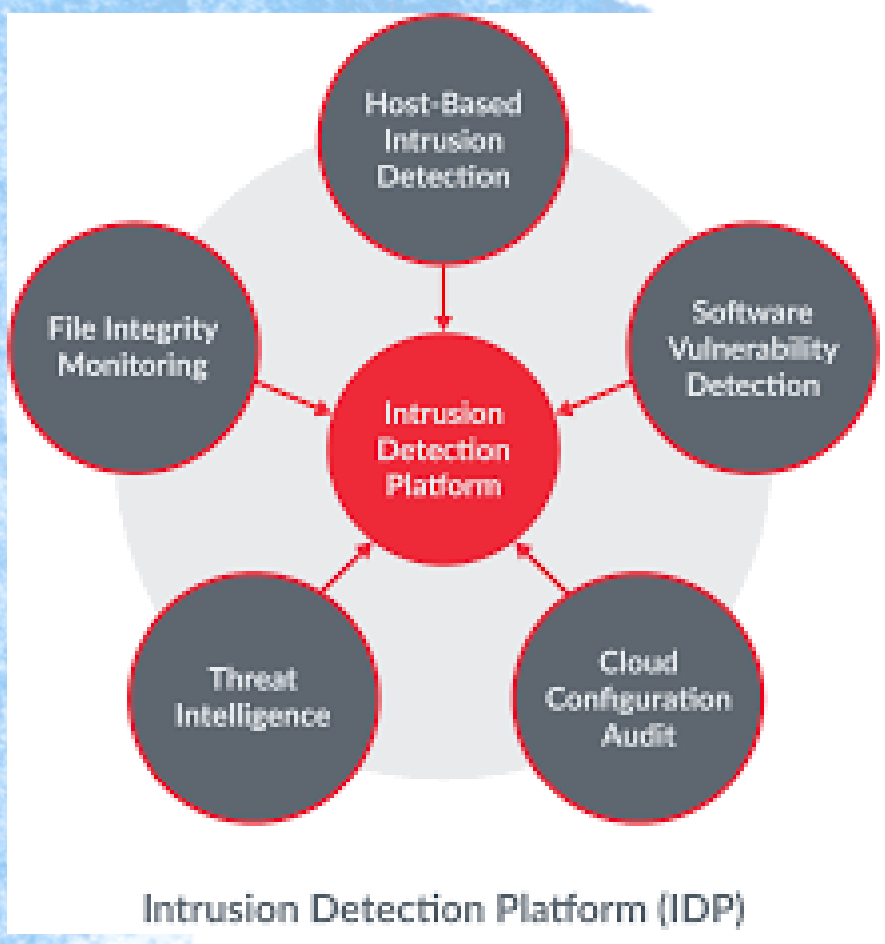
While anomaly detection and reporting are the primary functions of an IDS, some intrusion detection systems are capable of taking actions when malicious activity or anomalous traffic is detected, including blocking traffic sent from suspicious Internet Protocol (IP) addresses.



How do IDS work?

Intrusion detection systems are used to detect anomalies with the aim of catching hackers before they do real damage to a network. IDSes can be either network- or host-based. A host-based intrusion detection system is installed on the client computer, while a network-based intrusion detection system resides on the network.

Types of IDS



Intrusion Detection Platform (IDP)

Capabilities of IDS

- monitoring the operation of routers, firewalls, key management servers and files that are needed by other security controls aimed at detecting, preventing or recovering from cyber attacks.
- providing administrators a way to tune, organize and understand relevant OS audit trails and other logs that are otherwise difficult to track or parse.