Intrusion Detection System

# Types of IDS:

* Host Based IDS
* Network Based IDS

# Host Based IDS (HIDS):

## What is Host Based IDS?

* Makes use of log files or auditing agents of the system in the form of sources of data
* Monitors as well as analyzes a system’s internals along with the network packets
* Looks at communication traffic and checks the integrity of the system files

## How Host Based IDS Works?

* Analyzes several areas to determine misuse or intrusion
* Consults several types of log files (kernel, system, server, network, firewall, and more)
* Compares the logs against an internal database of common signatures for known attacks
* Runs directly on a server or desktop system and uses its resources to examine log and audit files together with network traffic entering and leaving the system
* Can monitor the log files for specific services such as web or ftp servers
* Looks for anomalies such as multiple failed login attempts, logins occurring at unusual times and access to system files not usually accessed by users

## Techniques of HIDS:

* Knowledge-Based (Signature-Based) IDS
* Behavior-Based (Anomaly-Based) IDS

### Knowledge-Based / Signature-Based IDS:

* References a database of previous attack signatures and known system vulnerabilities
* Recorded evidence of an intrusion or attack are called Signature
* Each intrusion leaves a footprint behind (e.g., nature of data packets, failed attempt to run an application, failed logins, file and folder access etc.). These footprints are called Signatures
* Based on these signatures Knowledge-based (Signature-based) IDS identify intrusion attempts

#### Advantages of Signature-Based IDS:

* Will not generate many false identifications

#### Disadvantages of Signature-Based IDS:

* Signature database must be continually updated and maintained
* May fail to identify a unique attacks

### Behavior-Based / Anomaly-Based IDS:

* Assumes that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users
* The model of normal or valid behavior is extracted from reference information collected by various means
* Compares this model with the current activity and notify when deviation is observed

#### Advantages of Behavior Based IDS:

* All attacks can be identified
* Detects attempts to exploit new and unforeseen vulnerabilities
* Less dependent on operating system-specific mechanisms

#### Disadvantages of Behavior Based IDS:

* May generate many false notifications