4.2 Components and Processes of IDs

Regardless of what IDS you select, they all have certain components in common. It is important to have a general understanding of these components.

The following terms will familiarize you with basic components and functions in all IDSs:

- An activity is an element of a data source that is of interest to the operator.
- The administrator is the person responsible for organisational security.
- A sensor is the IDS component that collects data and passes it to the analyser for analysis.
- The analyser is the component or process that analyses the data collected by the sensor.
- An alert is a message from the analyser indicating that an event of interest has occurred.
- The manager is the part of the IDS used to manage, for example a console.
- Notification is the process or method by which the IDS manager makes the operator aware of an alert.
- The operator is the person primarily responsible for the IDS. This is often the administrator.
- An event is an occurrence that indicates a suspicious activity may have occurred.
- The data source is the raw information that the IDS uses to detect suspicious activity.

Beyond these basic components, IDSs can be classified either based on how they respond to detected anomalies or based on how they are deployed. An active IDS, now called an IPS (Intrusion Prevention System), will stop any traffic deemed to be malicious. A passive IDS simply logs the activity and perhaps alerts an administrator. The problem with IPS/active IDS is the possibility of false positives. It is possible to have activity that appears to be an attack, yet in fact it isn’t. You can also define IDS/IPS based on whether a single machine is monitored or how an entire network segment is monitored. If it is a

single machine, then it is called a HIDS (host-based intrusion-detection system) or HIPS (host-based intrusion prevention system). If it is a network segment then it is called a NIDS (network-based intrusion-detection system) or NIPS (network-based intrusion prevention system).