4.5 INTRUSION DETECTION EXCHANGE FORMAT

IDMEF (Intrusion Detection Message Exchange Format) is a data format used to exchange information between software enabling intrusion detection, intrusion prevention, security information collection and management systems that may need to interact with them. IDMEF messages are designed to be processed automatically

Systems that may connect with management systems and interchange format systems. In 2007 the working group released the following RFCs

RFC 4765: The Intrusion Detection Message Exchange Format. This document outlines the logic behind selecting a certain data model to represent the information exported by intrusion detection systems.

Extensible Markup Language (XML) implementation of the data models offered, together with an XML Document Type Definition and samples.

RFC 4767, the Intrusion Detection Exchange Protocol.

The Intrusion Detection Exchange Protocol (IDXP), an application-level protocol for data exchange between intrusion detection entities, is described in this chapter. Over a connection-oriented protocol, IDXP offers mutual authentication, integrity, and confidentiality

The major components of the model that forms the basis of the intrusion detection message exchange approach are shown in Figure . Standards are required to promote interoperability, which will make it easier to create distributed IDSs that can operate in a variety of contexts and platforms.

The goal of the IETF Intrusion Detection Working Group is to develop such standards.

The essential aspects of any IDS are its functional components, which are independent of any specific product or implementation.

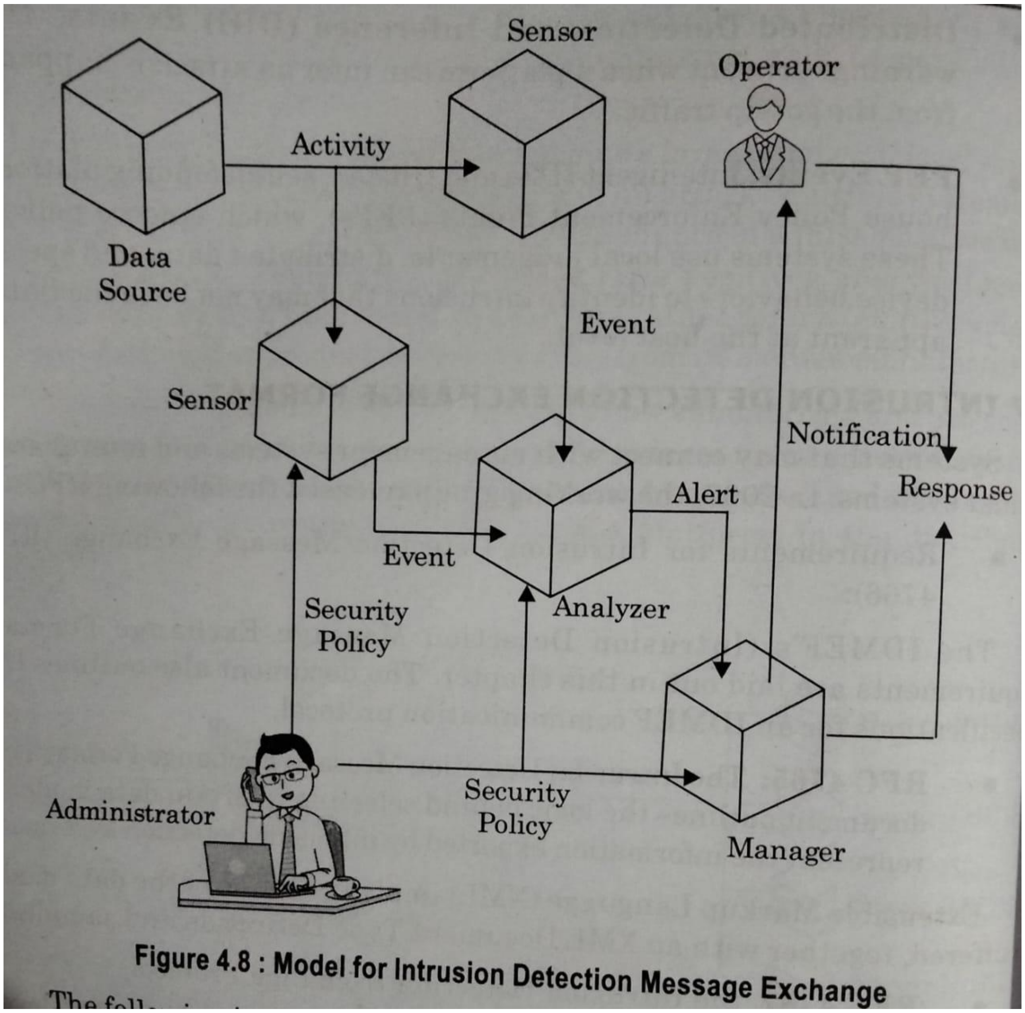

Figure 4.8 : Model for Intrusion Detection Message Exchange

Fig : Model for intrusion detection message format

The following is a list of the functioning parts:

Data Source: The unprocessed information that an IDS uses to look for suspicious or unauthorised behaviour. Network packets, operating system audit logs, application audit logs, and system-generated checksum data are examples of common data sources.

Sensor: Gathers information from a data source. Events are forwarded to the analyser by the sensor

Analyzer: This is the part of the ID system that examines the sensor data for any indications of unauthorized or undesirable behavior, as well as for any occurrences that would be of interest to the security administrator. The sensor and the analyzer are often included in the same component in existing IDSs.

Administrator. The person in charge of making choices regarding the IDS's deployment and configuration as well as the organization's overall security policy. The operator of the IDS may or may not be this individual. The network or systems administration groups may be connected to the administrator in some companies. It is an independent role in other organizations.

Manager: The ID process or component from which the operator oversees the different ID system components. Sensor configuration. analyzer configuration, event notification management, data consolidation, and reporting are examples of management functions.

Operator: The person who uses the IDS manager on a daily basis. The operator frequently keeps an eye on the IDS's output and suggests or starts new actions.

The following paragraph describes how intrusion detection works in this model. The sensor keeps an eye on data sources for any suspicious activity, such as network sessions with unexpected telnet activity, operating system log file entries with attempts to access files by users who are not authorized to do so, and application log files with persistent login failures. The sensor notifies the analyst of suspicious activity as an event, which describes an action taking place within a specific time frame. If the analyst decides that the event is important, it sends a notification to the manager component with details about the discovered odd activity and the circumstances of the incident.

The human operator receives a notification from the manager component. Either the human operator or the manager component can start a response automatically Among the possible actions are logging the activity, recording the raw data that best describes the occurrence (from the data source), ending a network, user, or application session, and changing network or system access controls. The security policy is the predetermined, officially recorded declaration that specifies what actions are permitted on a network or on specific hosts inside an organization in order to fulfil organizational needs. This involves specifying which hosts are to receive no external network access, among other things. The specification specifies message types, exchange protocols, and formats for event and alert messages that convey intrusion detection data.

The human operator receives a notification from the manager component. Either the human operator or the manager component can start a response automatically. Among the possible actions are logging the activity, recording the raw data that best describes the occurrence (from the data source), ending a network, user, or application session, and changing network or system access controls. The security policy is the predetermined, officially recorded declaration that specifies what actions are permitted on a network or on specific hosts inside an organization in order to fulfil organizational needs. This involves specifying which hosts are to receive no external network access, among other things. The specification specifies message types, exchange protocols, and formats for event and alert messages that convey intrusion detection data.