Intrusion Detection Systems

Bel G. Raggad[1]
Information Systems Department, Pace University
Pleasantville, NY, 10570, USA

Keywords: Intrusion detection systems, IDS, IDS engine, logging utility, information processing

Depending upon who you ask, the IDS may be a simple audit trail process, or a filter process using a traffic control system, like screening routers, packet filters, firewalls, etc. Some people use IDS to mean a logging utility. Others refer to IDS when they use a router-based access list, or an operating system monitor. For example, the file systems in your network environment contain a variety of software and data files. Unexpected changes in directories and files, especially those to which access is normally restricted, may be an indication that an intrusion has occurred. Changes may include modifying, creating, or deleting directories and files. What makes such changes unexpected may depend on who changed them and where, when, and how the changes were made

An intrusion detection system is a computer-based information system designed to collect information about malicious activities in a set of targeted IT resources, analyze the information, and respond according to a predefined security policy.

The IDS consists of at least the following subsystems:

1. IDS engine,
2. Monitoring subsystem,
3. Reporting subsystem,
4. Responding subsystem,
5. Storage,
6. Model base subsystem,
7. Database system, and
8. Feeders.

The IDS engine is the control unit of the intrusion detection system. Its main purpose is to manage the system, i.e., supervise all operations of the intrusion detection system. Its duty depends on the intrusion detection method used. These methods are addressed later in the full paper. In the case of an off-line processing method, feeding is initiated from a special-purpose storage, for example, the audit-trail archive subsystem.

If the method uses an on-the-fly processing, then the real-time analysis requires real-time feed directly from the monitoring subsystem. The IDS engine also initiates information feeding from other IDS units. The IDS engine is also in charge of reporting findings to relevant stakeholders and relevant subsystems as stated in the organization's security policy.

The IDS supervises all information-processing activities performed by selected models from the model base system. The IDS activates all types of reasoning, for example, pattern matching, statistical analysis, aggregation and processing of evidence, and so on, prior to any decision made regarding the need and type of response.

This work-in-progress proposes a common framework for Intrusion Detection Systems.

[1] braggad@pace.edu