Chapter XII

Intrusion Detection and Prevention Systems

Introduction

Let us make a statement of fact here that three principles define computer network security. These principles are: prevention, detection, and response. The high degree of internetworking and our growing dependence on computers have both, along with others factors, created an insatiable demand for information on and about people and products. This, in turn, has created a new class of hackers and information thieves determined to raid computer networks for proprietary information. All of a sudden, computer networks have come to be pots of honey attracting many. Consequently, the stam-pede for information from computer networks must be met with strong mechanisms, first to detect those trying to penetrate the system, secondly to prevent them from trying, and thirdly to respond to the attempt, successful
or not. Although these three are fundamental ingredients of security, most resources have been devoted to detection and prevention, because if we are able to detect all security threats and prevent them, then there is no need for response. So we will focus on prevention in this chapter, but before we do, let us define the working terms.

**Definitions**

There are several definitions for intrusion detection. In general, *intrusion detection* (ID) is a technique of detecting unauthorized access to a computer system or a computer network. An intrusion into a system is an attempt by an outsider to illegally gain access to the system. It is essential that an ID detects illegal intrusions accurately. An *intrusion detection system* (IDS) is a collection of software or hardware designed to capture and log network or host activities, analyze them, and generate relevant alarms, queries, and reports for the system administrator. *Intrusion prevention* is the art of preventing an unauthorized access to a system’s resources.

**Intrusion Detection (ID) Alarms**

If it is well configured, an IDS will produce an *alarm*. The alarm is a warning message or signal to the system administrator for action. IDS normally works in one of two modes: passive or active. In a passive mode, the IDS captures the malicious activities and creates a log for them. Then periodically it sends these logs to the administrator. In an active mode, however, the IDS works interactively with the control console and it responds to every suspected malicious activity with an alarm that is sent to the control console or wherever it is directed to be sent. In either mode, the IDS produces alarms. There are two types of IDS alarms: false and true.

**False Alarms**

False is bad. A false alarm is produced when something goes against expectations. There two types of false alarms: positive and negative.