Chapter 26
Intrusion Detection System (IDS) and Their Types

Manoranjan Pradhan
GITA, India

Chinmaya Kumar Nayak
GITA, India

Sateesh Kumar Pradhan
Utkal University, India

ABSTRACT

Over the last two decades, computer and network security has become a main issue, especially with the increase number of intruders and hackers, therefore systems were designed to detect and prevent intruders. This chapter per the authors investigated the most important design approaches, by mainly focusing on their collecting, analysis, responding capabilities and types of current IDS products. For the collecting capability, there were two main approaches, namely host- and network-based IDSs. Therefore, a combination of the two approaches in a hybrid implementation is ideal, as it will offer the highest level of protection at all levels of system functions. The analysis capability of an IDS can be characterised by the misuse and anomaly detection approaches. Therefore, a combination of the two approaches should improve the analysis capability of an IDS i.e. hybrid of misuse and anomaly detection.

INTRODUCTION

Organizations usually wish to preserve the confidentiality of their data which is very vital to an organization.. With the widespread use of the internet, it has become a key challenge to maintain the secrecy and integrity of organizations' vital data. Network security has been an issue almost since computers have been networked together. Since the evolution of the internet, there has been an increasing need for security systems. Conventional techniques for network security include security mechanisms like user authentication, cryptography and intrusion prevention systems like firewalls.

DOI: 10.4018/978-1-5225-9866-4.ch026

One important type of security software that has emerged since the evolution of the internet is intrusion detection systems. Intuitively, intrusions in an information system are the activities that violate the security policy of the system, and intrusion detection is the process used to identify intrusions. Intrusion detection, is the attempt to monitor and possibly prevent attempts to intrude into or otherwise compromise your system and network resources. Simply put, it works like this: You have a computer system. It is attached to a network, and perhaps even to the internet. You are willing to allow access to that computer system from the network, by authorized people, for acceptable reasons. Consider a real life scenario: you have a web server, attached to the internet, and you are willing to allow your clients, staff, and potential clients, to access the web pages stored on that web server. You are, however, not willing to allow unauthorized access to that system by anyone, be that staff, customers, or unknown third parties. For example, you do not want people (other than the web designers that your company has employed) to be able to change the web pages on that computer. Typically, a firewall or authentication system of some kind will be employed to prevent unauthorized access. Sometimes, however, simple firewalling or authentication systems can be broken. Intrusion detection is the set of mechanisms that you put in place to warn of attempted unauthorized access to the computer. Intrusion detection systems can also take some steps to deny access to would-be intruders. Intrusion detection systems (IDS) address problems that are not solved by firewall techniques, as a firewalls simply act like a fence around a network. IDS is capable of recognizing these attacks which firewalls are not able to prevent. Also, newer attacks are being developed that are able to penetrate through firewalls. IDS provides a solution to this problem. As a result, IDSs, as originally introduced by Anderson (Anderson, 1980) and later formalized by Denning (Denning, 1987), have received increasing attention in the recent years. The IDS along with the firewall form the fundamental technologies for network security which is in the Figure 1.

BACKGROUND

Definitions and Terminology

Intrusion detection is the process of monitoring and analyzing events that occur in a computer or networked computer system to detect behaviour of users that conflict with the intended use of the system. An intrusion detection system (IDS) employs techniques for modeling and recognizing intrusive behaviour in a computer system. When referring to the performance of IDSs, the following terms are often used when discussing their capabilities:

Figure 1. A computer network with intrusion detection system