Chapter 2
A Cloud Intrusion Detection Based on Classification of Activities and Mobile Agent

Nadya El Moussaid
Ibn Zohr University, Morocco

Ahmed Toumanari
Ibn Zohr University, Morocco

ABSTRACT

Cloud computing becomes the technology trend that attracts more and more both of the different forms of companies and attackers, for the reason that cloud computing provides a sharing pool of configured computing resources, such as servers, networks, applications, storage, and services, to end users. Therefore, securing sensitive data of companies from threats and attacks performed by internal or external attackers is a necessary requirement and exigency. For that purpose, in this paper presents an intrusion detection system that is based on mobile agent to collect and analysis gathered data from several virtual machines, in order to benefit from the advantages of mobile agents. The authors of this chapter propose to use C4.5 algorithm which is one of tree decision algorithms that classify data into normal and malicious one. The main purpose of our solution is creating a model of normal and abnormal behaviour.

DOI: 10.4018/978-1-5225-0602-7.ch002

INTRODUCTION TO INTRUSION DETECTION SYSTEMS

Information systems are vulnerable, and remain as long as users have the liberty to use internet and access secure or unsecure areas on the web, also as long as attackers keep on their malicious activities against systems and applications that contains sensitive data. Therefore, installing firewalls, sitting passwords and access control policies, to secure these systems, remains inadequate and not one hundred present efficient to protect those systems and the sensitive information within it from attackers. In order to detect computer attacks and react in case of any violation the intrusion detection systems came to existence. The first concept of intrusion detection system in general (IDS) was introduced by James Anderson in 1980, he introduced that audit trails contain important information that may be useful in tracking misuse or understanding the behaviour of the user, this work was the beginning of host-based intrusion detection system (HIDS). Later in 1987, Denning published a model of intrusion detection (1987). In the earlier stage of the IDS's development, the analysis of audit trails wasn't in real time, that's due to slow analysis. Therefore, intrusions were detected after they occurred. Herblein et al (1990) had developed Network Security Monitor that analysis, network traffic that provide a massive amount of information in real time, which in turn enables responses and react in real time. Then researches led to introducing Distributed Intrusion Detection System (DIDS) (1991) that combines distributed monitoring and data reduction with centralized data analysis to monitor a heterogeneous network of computers.

In general intrusion IDSs can be classified into two main categories depending on the type of analysed data: Host-based intrusion detection system (HIDS) and Network-based intrusion detection system (NIDS). HIDSs are characterized by the analysis of events and traces generated by the System, while NIDS analyse the data crossing the network. The performance of intrusion detection system, including its method of analysis, is related to two important concepts that assess its performance such as false negative and false positive.

According to the analysis method, IDS are classified into two classes: 1/ anomaly-based IDS and 2/ Signature-based IDS.

Anomaly-Based IDS

This approach proposed by Anderson (1980) and extended by Denning (1987), from a Simple finding that the exploitation of vulnerability in a system, or an intrusion attempt, involves behaviour modification in a service, an application, or a user.

This approach based on comparing the behaviour of users to a reference called a profile. Therefore, any activity or behaviour of a monitored entity (user, service, dif-