Model of an effective Intrusion Detection System On the LAN

Yousef Farhaoui
LabSiv, Equipe ESCAM
Faculty of sciences Ibn Zohr University B.P 8106,
City Dakhla, Agadir, Morocco.

Ahmed Asimi
LabSiv, Equipe ESCAM
Faculty of sciences Ibn Zohr University B.P 8106,
City Dakhla, Agadir, Morocco.

ABSTRACT
Despite the development of new technologies of information and communication following the advent of the Internet and networks, computer security has become a major challenge, and works in this research are becoming more numerous. Various tools and mechanisms are developed to ensure a level of security to meet the demands of modern life. Among the systems, intrusion detection for identifying abnormal behavior or suspicious activities to undermine the legitimate operation of the system. The objective of this paper is the design and implementation of a comprehensive architecture of IDS in a network.

Keywords
IDS, Architecture, model.

1. INTRODUCTION
Since their introduction, Cyber attacks have been a real threat. With their wide variety and specialty, they can have catastrophic consequences. To prevent attacks or reduce their severity, many solutions exist, but no one can be considered satisfactory and complete. The intrusion detection systems are one of the -the most effective solution. Their role is to recognize intrusions or intrusion attempts by users or abnormal behavior by the recognition of an attack from the stream network data. Different methods and approaches have been adopted for the design of intrusion detection systems. An IDS is a tool that complements a wide range of users used to have some level of security. We present here the different architectures of IDS. We will also discuss measures that help to define the degree of effectiveness of IDS and finally the very recent work of standardization and homogenization of IDS.

2. ARCHITECTURE OF IDS

2.1 Classical architecture of IDS
The intrusion detection systems have a common pattern, consisting of three modules (Figure1):

2.1.1 The sensor
The sensor observes the system activity through a data source and provides the analyzer a sequence of events that inform the evolution of the system state.

2.1.2 The analyzer
The purpose of the analyzer is to determine if the flow of events provided by the sensor contains features of malicious activity. Two main approaches have been proposed: the behavioral approach (anomaly detection) and the scenario approach (misuse detection)

2.1.3 The manager
The manager is responsible for presenting alerts to the operator (Function of management console).

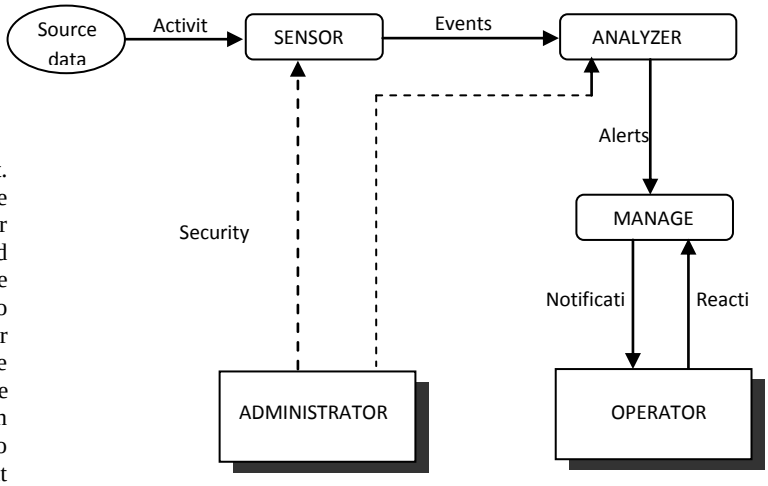

Fig1. Architecture of IDS

2.2 Architecture des IDS modern
The model in Fig1 is purely theoretical and does not necessarily correspond to implementations that are made by software developers. In practice, the architecture of IDS often resembles the following architecture in Fig2.

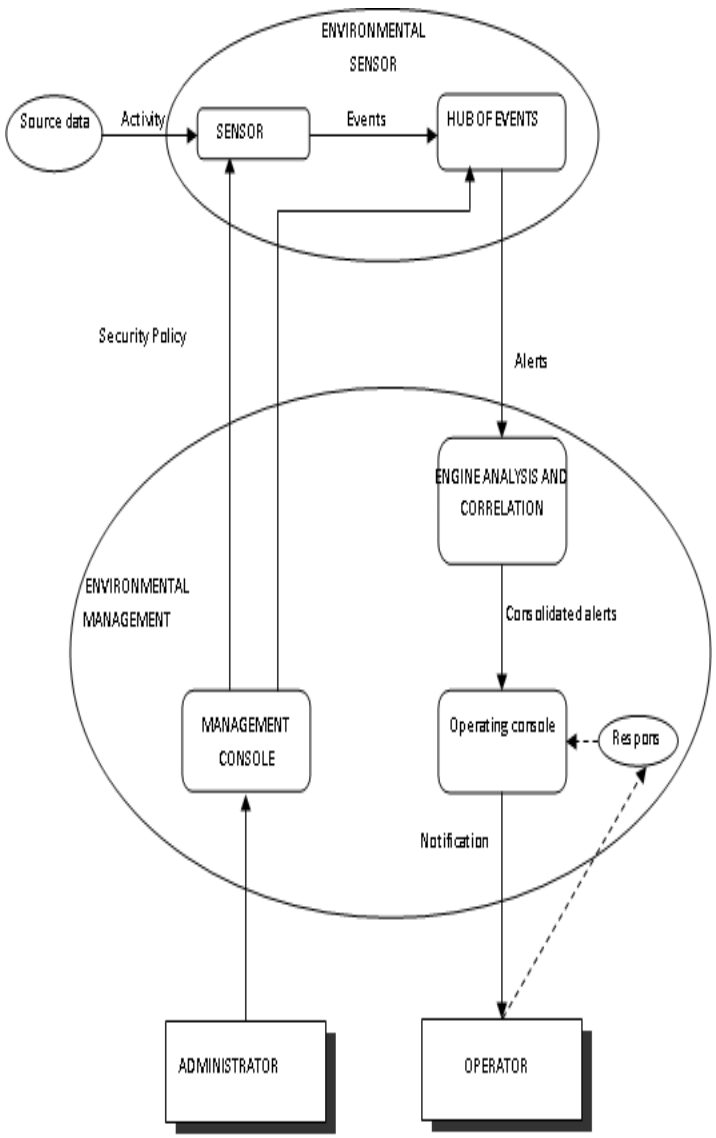

Fig 2. IDS architecture of a modern

2.3 Architecture of a network with IDS

The control strategy determines how to manage multiple sensors of the same IDS, or how to manage multiple IDS in a network. According to the arrangement of the various components of the IDS, multiple architectures may be adopted.

2.3.1 Centralized architecture

Some provision will control all the events from a central console, analyze, and decide the action to take. Different model of IDS can be used in the same network at different strategic points in order to gather information from different IDS and treat to a central point.

2.3.2 Partially distributed architecture

This provision allows the server to discharge of all duties. A hierarchy is established. Each sub network is managed by a local point. Measurements are taken by the console level.

2.3.3 Fully distributed architecture

In this case, the network is decomposed into several subnets, each of which is managed by its own IDS. The tasks of audit and analysis are made locally.

3. EVALUATION OF AN IDS

Measures used to compare and measure the effectiveness of IDS. IDSs are very important elements in a security strategy; why the choice of the IDS is very critical and must be based on its characteristics. Measures to better choose their IDS. Donations [1] [3] we can evaluate the IDS based on several criteria such as:

• The rate of false positive and false negative;

• Response by the IDS in a enveironnement overloaded;

• The ability to update the signature database or modify certain signatures;

4. STANDARDIZATION AND NORMALIZATION

The IDWG group participated in the standardization of IDS by setting the standard IDMEF (Intrusion Detection Message Exchange Format) format of messages exchanged between IDS and protocol IDXP (Intrusion Detection Exchange Protocol) which defines the procedures for transportation from IDS.

A committee of the DARPA [4] defined four blocks to describe the architecture of an IDS, and this model Fig1 which was subsequently adopted for all IDS:
• Generator of events: send events;

• Monitor events: analysis of the events received and generates alerts;

• Database events: for storing all types of information RELET events, alerts;

• System response: real-time response to the attacks.

The probe (analyzer) sends an alert to a collector; this model provides a heterogeneous communication environment except on how to pass the communication.

Many IDS consist of a single block that handles the entire analysis. This monolithic approach requires a lot of constraints such as [5]

• The use of system resources;

• Difficult to update;

• The core itself is the weak point if an attack is launched against the IDS;

• Need more of audit data.

To overcome these weaknesses, there are many new trends in the design of IDS. Current trends are oriented to distributed intrusion detection.

The first project that used this approach of information gathering of audit was the NADIR project that analyzed by an expert system [6].

A standard model for IDS, which was set up by the committee DARPA. Today, this model is adopted in the development of

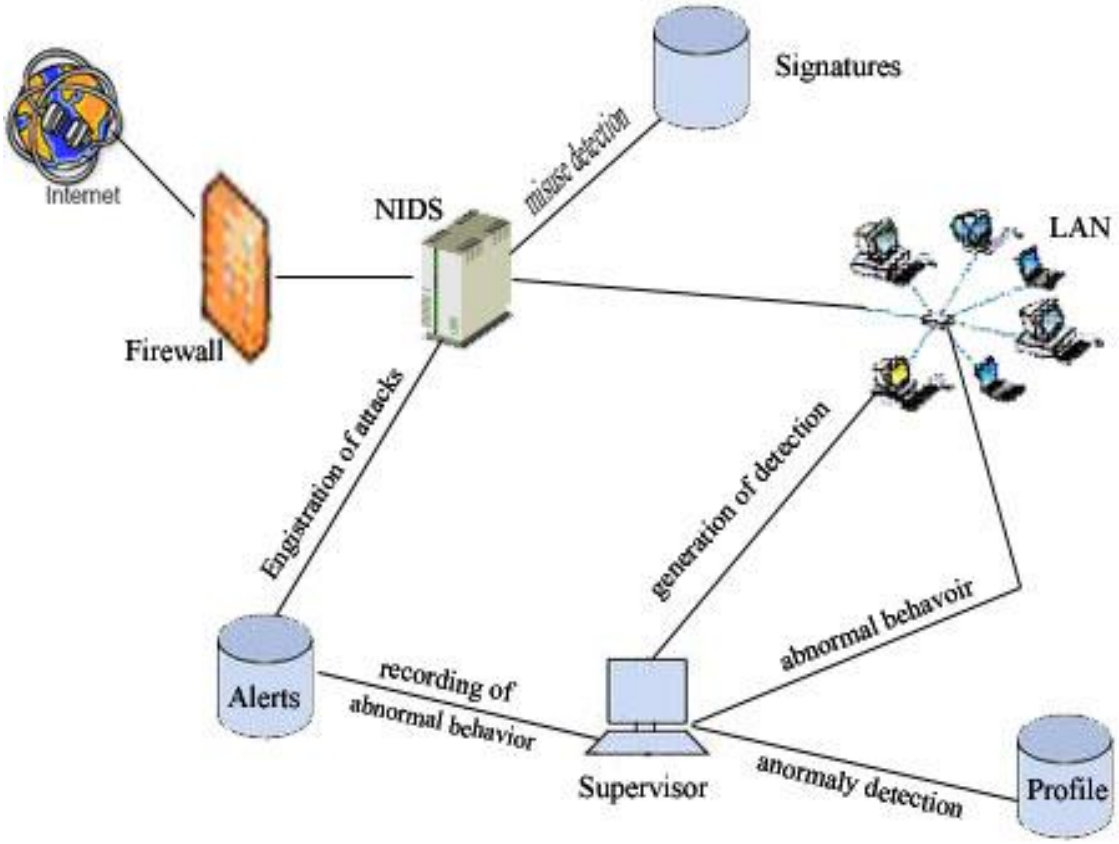

Fig3. Overall scheme of the solution

the majority of new IDS today. It consists of four components: the source of information, the sensor, the analyzer and the manager. For effective intrusion detection, it is important to remember that the characteristics must meet all IDS, such [1] [2]: distributivity, autonomy, communication and cooperation, responsiveness and adaptability.

5. OUR WORK

The study of intrusion detection systems has allowed us to realize the importance of the role. Of these to its own security policy. Different types of IDS (HIDS, NIDS), each characterized by a certain architecture and method of analysis. The characteristics of the IDS must meet certain requirements; the choice of adopting a certain type relative to another should

be based primarily on the needs and constraints of security software and hardware. We can determine the type of IDS according to [2]:

• The location of the IDS (NIDS, HIDS);

• Frequency of use (continuous or periodic);

• The detection method (behavioral or scenario);

• The response of the IDS (passive or active).

In this paper we propose a new architecture for intrusion detection, to mix the two approaches: anomaly approach and misuse detection.

The choice of this approach is essentially based on the fact that the IDS is composed of different modules to be distributed on a set of network station to perform different tasks. The various components of the IDS must be in continuous interaction.

Our model consists of a primary IDS, its role is to organize tasks and manage the various second IDS, which have for role to capture events and the transmissions of the conclusions. The HIDS should be based on user profiles describing their normal behavior. This solution is very interesting since the only information required is the behavior of users in the network. This source of information can be kept updated only in learning phases. However, the disadvantage of this solution is the rate of false positives due to abnormal or unusual behavior of users, who are not necessarily harmful. The NIDS using the scenario approach (misuse detection) uses essentially a database of signatures of known attacks. This source of information allows us to significantly reduce the false positive rate. However, the disadvantage of this solution is the source of information that must be regularly updated. An attack not listed has no chance of being detected by the NIDS.

At the end to take advantage of both approaches (behavioral and scenario) that seem complementary, we chose the design of a hybrid IDS.

5.1 The solution description

The core of our IDS generates variations of attack signatures and user profiles in a pseudo-random. This methodology

allows us to upgrade the analyzer to discover possible new attacks or variations of attacks.

5.2 Overall architecture of IDS model

Our IDS is composed of (fig 3):

a. NIDS generate detection based on signatures. These detectors will be used to analyze network traffic.

b. HIDS based on the profiles of normal behavior of users.

HIDS generate detectors able to recognize unusual behavior of users.

c. Administrator can configure the various parameters of IDS, see the different alerts, and run the learning command. The components of our solution should be deployed on the output: the NIDS will be installed on the machine that is the proxy network in order to analyze network packets. The HIDS will be deployed on all the machines that consist of the local network.

The use of databases is very important in our model, we opted for the use of three databases:

a. Profiles database contains all information relating to user profiles. The data contained in this database are generated by the HIDS during the learning phase.

b. Database of signatures is the basis of NIDS. It includes all the known attacks by using a certain format. There is no standard for the coding of signatures. The attributes used to represent an attack must be based on the information contained in the packages [6].

c. Database alerts to list all alerts generated by the detectors of the two components of the IDS (HIDS and NIDS). This database will be accessed by the administrator to meet the traces of attacks or the anomalous behavior.

5.3 The HIDS architecture

The first step in deploying HIDS is learning phase [8], during which we save the traces of the normal behavior of users by creating a profile for each.

Our HIDS will consist of a supervisor and a set of HIDS slaves to be deployed on all machines the network components.

a. HIDS supervisor's role:

• Extract user profiles database;
• Generate the sensors and send them to HIDS slaves;
• Analyze the relationship of slaves and directories HIDS and alerts in a database;
• Sends commands to start the learning phases, analysis, start and stop HIDS slaves.

b. HIDS slave for:

• Generate user profiles during the learning phase;
• Use of event sensors to extract the current behavior of the user.

5.4 NIDS architecture

Using the analysis with the scenario approach. The analysis function of our NIDS contains two generation process sensors and their installation for the analysis of packet flows. The stages of execution are:

• Capture packets;
• Extraction and formatting attributes;
  Structuring the data;
  Summarize the data;
  Provide attributes.
• Analysis of attributes;
• Send of reports.

6. CONCLUSION AND OUTLOOK

The choice of the IDS implementation is very important, especially if we consider that the IDS will be deployed on a network with multiple machines using different hardware and software. The fact that the IDS is designed to be hierarchical and distributed across multiple machines and requiring analysis of data from different sources.

So, we propose to give some perspective:

• The maintenance of profiles, automatic update of profiles;
• Generation of profiles.

7. REFERENCES

[1] Y. Fargaoui, A. Asimi, "Performance method of assessment of the intrusion detection and prevention systems," *IJ E ST , Vol. 3 No. 7 July 2011*

[2] Y. Farhaoui, A. Asimi, «Performance Assessment of the intrusion Detection and Prevention Systems: According to their features: the method of analysis, reliability, reactivity, facility, adaptability and performance», The 6th IEEE international conference Sciences of Electronics Technologies Information and Telecommunication (SETIT 2011), Sousse, Tunisia, 2011.

[3] Y. Fargaoui, A. Asimi, "Performance Assessment of tools of the intrusion Detection and Prevention Systems," IJCSIS , Vol. 10 No. 1 January 2012

[4] MIT Lincoln Laboratory, DARPA Intrusion Detection Evaluation Data Sets,

www.ll.mit.edu/IST

[5] K. Boudaoud, "Un systeme multi_agents pour la détection d'intrution » Institution EURECOM Sophia-Antipolis.

[6] J. Hochberyn K. Jackson, C Stallings, J.F Mclary, D. Dubois, J. Ford, NADIR "An automated system for detection network intrusion and misuse" , Cpmputers and Security.

[7] The UCIKDD archive, Information and Comuter Science, university of california.