Creating a Complete Model of an Intrusion Detection System effective 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*— the Intrusion Detection Systems (IDS) are now an essential component in the structure of network security. The logs of connections and network activity, with a large amount of information, can be used to detect intrusions.**
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 is 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*—*Intrusion Detection System; Characteristic; Architecture; modele.

I. INTRODUCTION

Today, information systems and computer networks are central in modern society. The more data stored and processed, it is more important to secure computer systems. An intrusion is defined as a series of actions that attempt to compromise the integrity, confidentiality or availability of a resource [1]. The intrusion detection Systems (IDS) can be hardware and software that automate the process of observation and analysis of events.

For an IDS to be effective it must run continuously adapt to behavioral changes and large amounts of data, be configurable, do not use too much memory resources of the machine and after system failures, be reusable without new learning [2].

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.

II. METHOD FOR DETECTING INTRUSION

Currently, there are two main approaches for intrusion detection. Anomaly detection and misuse detection (Misuse Detection). In the first approach, the normal behavior of network users are known and it is therefore possible to construct profiles representing these behaviors with several features such as network activity, etc.. Once these profiles defined, the intrusions are identified as deviations from normal behavior [1][3][4].

The approach detection of abuse (Misuse Detection) is based on the direct identification of attacks. A signature is a type of attack already known. Intrusion detection is done by comparison of network attacks with signatures [1][3][4].

The advantage of methods based on anomaly detection is the ability to find the unknown intrusions. Once all these methods produce a high rate of false alarms since all deviations from the general behaviors are not necessarily intrusions. For example, a new normal behavior can be seen as a deviation and treated as an intrusion.

On the other hand, in the case of misuse detection, each instance in the data set is labeled "normal" or "intrusion". A learning algorithm is applied to the data labialised, so that each intrusion is characterized as a model (intrusion signatures). We identify a new instance as an intrusion if it looks like an intrusion model. Models (signature) can be created by domain experts.

This is the case in systems based intrusion signatures (signature-database intrusion detection) [5]. These systems are effective to search for already known intrusions. However, these systems are not able to find new intrusions or intrusions for which signatures do not exist.

III. IDS AND CLASSIFICATION

The IDS-based classification techniques are intended to classify network traffic into two classes: "general" and "intrusion". Classification requires learning.

The accuracy of this learning provides lower false positive rate (normal cases classified as intrusions) and false negative rate (intrusions classified as normal).

Measures used to compare and measure the effectiveness of IDS. The IDS 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 [6] [7] [8] we can evaluate the IDS based on several criteria such as:

•The rate of false positive and false negative;
• Response by the IDS in an enveironnement overloaded;
• The ability to update the signature database or modify certain signatures;
• …

IV. Our Intrusion Detection Systems Model

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 [7]:

• 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 are 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.

A. 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.

B. Overall architecture of IDS model

Our IDS is composed of (figure 1):

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.

C. 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.

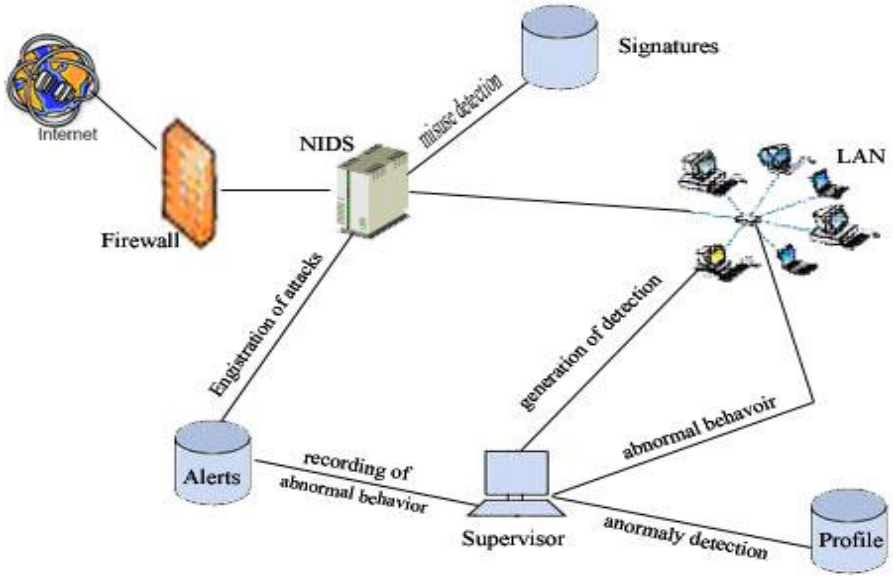

Figure 1. Overall scheme of the solution

D. 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.

V. THE LIMITATIONS OF IDS

The limits apply to misuse detection techniques like those of anomaly detection. Attacks on the TCP flags. IDS are vulnerable to certain attacks on the TCP flags (TCP flags), such as:

- Sending a SYN false;
- Integration of data with bad sequence number;
- FIN / RST spoofing with wrong sequence number;
- Synchronization after connection;
- Desynchronization before connection [SYN (bad checksum + bad sequence number) and SYN];
- FIN / RST spoofing with bad checksum;
- Data spoofing with bad checksum;
- FIN / RST spoofing with short TTL;

Integration of data with a short TTL, etc.. Placement of the IDS. Without going into details, at the placement of the IDS (Design and implementation), it is interesting to make intrusion detection in the demilitarized zone (attacks against government systems), in network. Private (intrusions into or inside) and behind the firewall (detection of signs from all incoming and outgoing traffic). Each of these positions has its advantages and disadvantages.

The important thing is to identify resources to be protected (major business risks) and what is most likely to be attacked. It should then carefully implement the IDS (settings, etc..) Depending on the investment chosen. Pollution / overload. The IDS can be overloaded or contaminated, significant traffic (the most difficult and cumbersome to analyze possible). A significant amount of Mild attacks can also be sent in order to overload the IDS alerts. Possible consequence of this overload may be the saturation of resources (disk, CPU, memory), packet loss, denial of service or partial.

- Consumption of resources: in addition to the size of log files, intrusion detection is extremely resource-intensive;
- Packet Loss (performance limitation): the transmission rates are sometimes as far exceed the write speed of the fastest hard drives on the market, or even the processing speed of the processors. It is not uncommon for packets are not received by the IDS, and some of them are still received by the destination machine.
- Vulnerability to DoS: An attacker may attempt to cause a denial of service system-level intrusion detection, or at worst operating system of the machine supporting the IDS. Once disabled the IDS, the attacker can try all he likes. For example, the Stick attack is an attempt denial of service attack against the IDS overloading the IDS work at the point of disabling it or at least make it less effective.

Detection time: The detection time is a crucial element for IDS: Intrusion Detection is it done in real time or does it require a delay? What time (a few days ...)? Experience shows that it usually takes some time to identify or reconstruct an attack (analysis time, reaction ...).

Specific limits to the detection of abuse: The main challenges of this technique are as follows.

Definition and maintenance of signatures: All attacks are not detected, depending on the features of the system, the definition of signature, the update of the database, the system load, etc..:

- Limits "human" signatures outdated or poorly designed. Detection of abuse has good design imperatives for attack signatures and a continuous updating of the list of signatures.
- Context of use: sometimes the technology is based on signatures that are not based on the context of use. The result is twofold: many false positifs19 and significant degradation of system performance.
- Even if the method signatures of the body seem to be quite reliable, there are ways to circumvent them.
- Vulnerability to changes: due to its lack of flexibility, detection attack signatures are very vulnerable to mutations. First, in order to define a signature, you must have already faced the attack considered.

On the other hand, some of these signatures are based on characteristics "volatile" a tool, such as wearing a Trojan opens by default or the value of ISN chosen by some hacking tools. But these programs are often either highly configurable, open source is so readily modified. The characteristics used to define the signature are fragile and highly sensitive to changes signatures.

- Lack of definition, new attacks are the IDS without being detected. False positives. Normally, the advantage of detection of abuse should be a low rate of false positives (false alarms) as the criteria of signatures can be precisely defined. Nevertheless, according to sources of information, we read that there is little to a lot of false positives resulting from this technique, particularly regarding:
- The sensitivity / specificity of the IDS: by nature, IDS alerts will go up enormously if they are not configured properly. Full attention must be paid to the establishment of signature rules. The compromise made between the amount of recovery alerts and finesse of the latter is crucial. We must take care to include in the configuration file the file. "Rule" necessary, according to rules established by the firewall. For example, if a service is totally forbidden, it is almost unnecessary to include the signatures associated.

Specific limits on anomaly detection. This technique also involves many complex problems to be solved here is the most commonly mentioned.

Learning / configuration of the IDS: Learning the "normal" behavior is not easy. Automate the reasoning used to think that behavior is "deviant" in relation to that known is a difficult task. By cons, this technique is applied by default by the system or network administrators: If something seems unusual (peak bandwidths, services that fall, file systems that fill faster than usual), the practice is that further research be undertaken. In addition, any abnormality does not necessarily correspond to an attack; it may be a change in user behavior or a change in network configuration. Typically, convergence to a behavioral model "normal" is quite long. When setting up the IDS, the challenge for the effective detection lies in the choice of metrics, models and in defining the different profiles. For all these reasons, the IDS running through anomaly detection are known to be very long and tedious to configure. Even after an effective configuration, nothing prevents an attacker from knowing guarded "reeducate" such a system by changing its model of progressive convergence towards an abnormal behavior for the analyst, but to actually "normal" to a statistical point of view. False positives. Anomaly detection can detect unknown attacks, but it is not as effective as misuse detection for known attacks. Particular, a high rate of false positives can be met if the setting of the IDS was not carried out carefully

VI. Conclusion

In general, the effectiveness of intrusion detection system depends on its "Configurability" (Ability to define and add new specifications attack), robustness (fault tolerance) and the small amount of false positives (false alarms) and false negatives (undetected attacks) it generates. The foregoing paragraphs are aimed both to illustrate the sophistication of today's attacks, to show the complexity of intrusion detection and explain the limitations of current IDS. A struggle between intrusion techniques and IDS is committed, the IDS resulting in a more technical nature of the attacks on IP, and the current attacks requiring IDS to be more complete and powerful. To conclude this article, IDS provide a definite plus for networks in which they are placed. However, their limitations do not guarantee 100% security, unobtainable. You must then tender ... The future of these tools will help fill these gaps by avoiding "false positives" (for IDS) and refining the access restrictions (for IPS)

References

[1] Abhinav Srivastava, Shamik Sural, and Arun K. Majumdar. Weighted intratransactional rule mining for database intrusion detection. In PAKDD, pages 611-620, 2006.

[2] J. S. Balasubramaniyan, J. O. Garcia-Fernandez, D. Isaco_, Eugene H. Spa_ord, and Diego Zamboni. An architecture for intrusion detection using autonomous agents. In ACSAC, pages 13_24, 1998.

[3] Wenke Lee, Salvatore J. Stolfo, and Kui W. Mok. Mining audit data to build intrusion detection models. In Knowledge Discovery and Data Mining, pages 66_72, 1998.

[4] Karen Scarfone and Peter Mell. Guide to intrusion detection and prevention systems (idps). Technical Report SP800-94, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, U.S. Department of Commerce, February 2007.

[5] Paul Dokas, Levent Ertoz, Vipin Kumar, Aleksandar Lazarevic, Jaideep Srivastava, and Pang-Ning Tan. Data mining for network intrusion detection. University of Minnesota, Minneapolis, MN 55455, USA, 2002.

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

[7] 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.

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