Journal of Zankoy Sulaimani- Part A, Vol. 16 (2), 2014.

Design of Alarm Based Network Intrusion Detection System

Najmadin Wahid Boskany

Computer Science Department, School of Science, Faculty of Science and Science Education, University of Sulaimani, Kurdistan Region- Iraq, e-mail: boskany@hotmail.com.

Received: 2 Apr. 2014, Revised: 15 May 2014, Accepted: 29 May 2014
Published online: 7 June 2014

Abstract

Nowadays each computer network needs some tools in order to help their administrator for protecting network devices and data. These tools are ranging from firewall, antivirus, and intrusion detection systems. The main goal of this paper focuses on developing an applicable system for detecting intrusion and notifying network administrator from them (i.e. alert that there is unauthorized person attempts to break into network). The presented system can be used to detect intruders automatically depending on a signature file, and immediately notify onsite monitors and network administrator via alert message and short message. These different messages let them know who is going to access the network (i.e.; show the intruder IP address and used port number).

Keywords: Network Intrusion Detection, Short message, Logical Address, Socket Address, Application Programming Interface (API), Alert Message.

I. Introduction

Network security became ever increasingly critical elements of all types of network designs and implementations. A typical network security exercise involves the planning and design of networks, so as to protect its valuable applications, sensitive data, and network resources [1, 4].

Because the last few years have seen a dramatic increase in the number of attacks, intrusion detection has become the mainstream of information assurance. Also with the rapidly increasing network technology there is an increased need for security against unauthorized accesses, intrusion detection has become an important technology market. Intrusion Detection System (IDS) is one of most important techniques that it's primary function is detecting intrusions in different ways. It monitors packets on the network wire and tries to discover if an intrusion is existing inside network system or no [5, 7].

While firewalls do provide some protection and still need to be complimented by intrusion detection system.

The purpose of intrusion detection is to help computer systems deal with and prepare for attacks. Intrusion detection systems collect information from a variety of sources within computer systems and networks. For most systems, this information is then compared to predefined patterns of misuse to recognize attacks and vulnerabilities [3].

Furthermore intrusion detection systems monitor various events in a networked system and analyze them for signs of security problems. By extending the information security paradigm beyond traditional protective (e.g. firewalls) and reactive measures (e.g. virus detection), they increase the controlling ability of the system administrator, and help them manage system security [2].

In some cases there are capability to present some types of IDS systems with additional capability like providing alert and notifications. An alert is a warning issued by the IDS to the system operator that an intrusion is taking place or being attempted. On detecting an intrusion, the IDS will alert the analyst using a variety of methods. If the console is local to the IDS the alert would normally appear on the monitor [6].

Unlike traditional models of network intrusion detection system, in this paper a model of IDS with additional feature for notification is proposed. In this model the system has two main functions:

- The system has ability to detect intruder computer inside networks depending on intruder IP address and port number.
- In the same time the system has the ability to alert system administrator automatically about the intruder as soon as possible an intruder has been detected. This detection is based on abnormal appearances inside the network (i.e.; like using unauthorized logical addresses and accessed secure port numbers).

Detecting such intruder depends on matching process between signature-based file (i.e.; which contain the range of permitted IP addresses and opened port numbers) and discovered IP address.

This system; Alarm Based Network Intrusion Detection System (AB-NIDS) has been developed using Visual Basic for Applications (VBA) programming language with some features like socket Application Programming Interface (API), Mscomm object for connecting mobile devices using AT commands. This application works under Microsoft Windows operating system environment.

The rest of this paper is organized as follows: In section II, Related Work and Background has been written; while in section III; the architecture of proposed system has been illustrated, in section IV steps which are necessary to analyze AB-NIDS system work flow have been indicated. The system test, results and all relevant discussions appear in section V. Finally, the main conclusions and future work are summarized in section VI.

II. Related Work and Background

In the last years, we have seen many Network Intrusion Detection Systems by using different efforts and approaches; they were concerned in developing applications which can operate on different platforms. These systems are based on the statistical data analysis, expert systems, using artificial intelligence, network traffic or various forms of the attack manifestation in the network [9]. On the other hand Network Intrusion Detection

System (NIDS) embedded in a Smart Sensor have been proposed by Francisco et al [10]. Also there are some new intrusion detection systems which they have additional features like alarm and notification systems.

III. AB-NIDS System Architecture

The architecture of the proposed AB-NIDS system depends on taping into a network medium via the network interface card (NIC) of a computer which it hosts AB-NIDS application system. Whenever The AB-NIDS executed it acquire and observes captured network traffics, which are generated by other hosts inside its network. The structure of AB-NIDS system which is consists of five layers is depicted in figure 1.

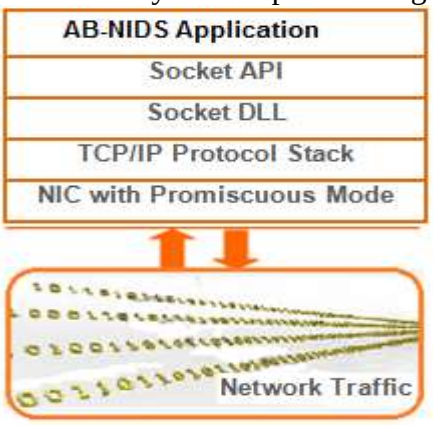

Fig. (1): AB-NIDS Structure

Afterwards the AB-NIDS system analyzes packet header, separates each part and distributes all parts of the captured traffics into fields. Then source logical address and port number will be compared with information that is already stored in the background of AB-NIDS in a database file. The information includes list of source logical addresses of permitted hosts and list of secured (closed) port numbers.

The system then detects anomalies of hosts that use the network. Then notify both network monitor and administrator with a alert message and short message in order to let them about an intruder inside the network. The idea behind this approach is to match such host information (i.e. intrusion IP address), with information that is already saved by network administrator (i.e. legal IP addresses and secured port numbers) inside the AB-NIDS system in two cases. Then, the system can trigger when there is a variation.

In the first case, when the AB-NIDS gets the source logical address of hosts, it matches them with the list of logical addresses which are already archived in a database file of permitted hosts to access the network; if detected logical addresses are in the same range of saved addresses it means that the host is legal. Otherwise if it is not inside the list of addresses, it means that host is intrusion and it is not permitted to access the network (i.e. the observed hosts have reached the internal network and accessed to network resources without permission). Or they are internal intrusions with unauthorized host addresses. Here the system alerts both onsite monitor and network administrator about these illegal host addresses.

In the second case, the AB-NIDS packet is compared to the port numbers that are observed, with a list of closed port numbers which known by the administrator of the network. If a port number is in the list and the AB-NIDS detected this port number is used, it means that this port is opened by this host; in other words it indicates that there are intrusions on this network. Again the system alerts both onsite monitor and the network administrator via a short message and let them know about these illegal host addresses.

IV. AB-NIDS Work Flow

The steps of how AB-NIDS works and its role in saving networks from intrusions are illustrated in detail:

First, the system starts capturing traffics inside the transmission medium of local network by calling (socket.dll) library, via some socket application programming interfaces (API's), which already exist inside the core of Windows based operating systems [8].

While the system finishes packet capturing, it then analyzes these traffic headers in order to distinguish source logical addresses and destination port addresses fields.

Later, it starts to compare captured data with AB-NIDS database which contain a range allowed logical addresses and secure port addresses. If the host addresses are known as legal host (i.e. its address is inside the logical address range of AB-NIDS database), then the system shows "**Legal Host**" message. Otherwise the captured logical addresses are not inside the list of stored logical address, then it shows "**Intrusion Detected**" message. In the same time it sends a notification message to the both onsite monitor and network administrator mobile device as a short message. This is illustrated below in the figure 2 flow chart of how AB-NIDS detect intrusion is based on logical addresses.

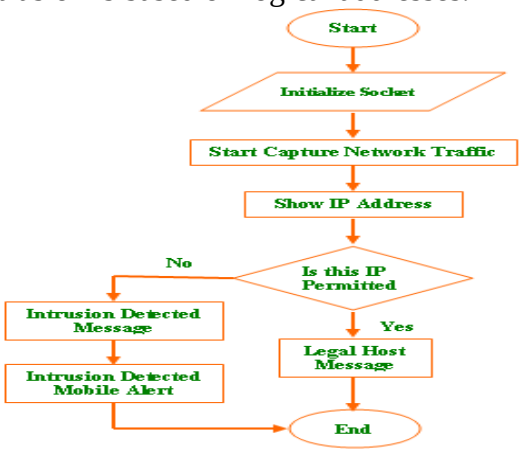

Fig. (2): IDNS Flow Chart

On the other hand, if any secured port opened by any host it means that intrusion detected. The system shows "**Intrusion Detected**" message; otherwise, if the opened port is not on the list of secured ports, it indicates that the host that used specific port number is a legal host, and the system shows "**Legal Host**" message, as shown in figure 3 AB-NIDS Interface. Finally, the system can count the number of the observed illegal host addresses which they accessed the network in any given time. Depending on these statistics of anomaly traffics and received short messages the network administrators can react to prevent intrusions. Detail of these processes is illustrated in the next section.

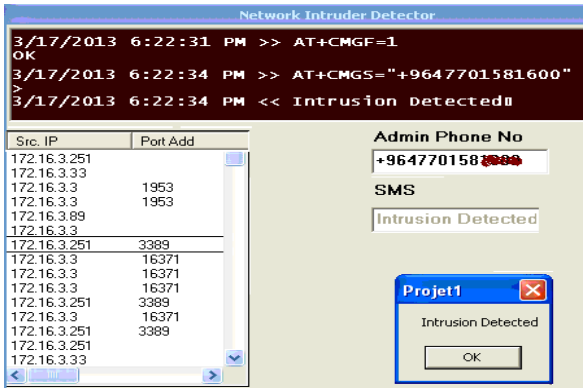

Fig. (3): AB-NIDS Interface

V. AB-NIDS Test and Result

AB-NIDS have been installed on local network which contain about 130 computers (i.e.; IP addresses are ranged from 172.16.1.1. to 172.16.1.131), then AB-NIDS have been tested many times for checking its performance, reliability, knowing who accessed the network (i.e.; which IP addresses are used), and what's going on in background.

Among many tests which have been done, here three of them are explained. The tests done in three days:

First day AB-NIDS executed for 4 hours durations to detect intruder, from 8:00 am to 12:00 am.

Second day second test done for 3 hours duration from 10:00 am to 1:00 pm.

The last test done in third day from 12:00 am to 4:00 pm respectively.

In first test at 9:00 am to 10:00 am AB-NIDS detected 2 intruders with 172.16.1.232 and 172.16.1.251IP addresses (i.e.; which are not in the range of authorized IP address) immediately the system alerted the system monitor about these intruder by alert message "INTRUDER DETECTED with IP: 172.16.1.232 and Port: 3389" and after short time (7 to 9 seconds) same message sent by the system to the second monitor (i.e.; remote or mobile monitor) to their mobile device by short message as illustrated in figure 3. In the same way for second intruder IP these alerts allow onsite monitor persons to have knowledge about the system users and online monitor can take control and do necessary procedures to block the intruders. Second and third tests are done in second and third days with duration of 3 hours and 4 hours respectively. In second day test 3 intruders and in third day test 2 intruders are detected. Table 1 explains detected intrusions per time.

Table 1: Detected Intrusion per Time

Date	Test No.	Duration	Time	No. Of Intruder	IP Address	Port No.	Mobile Alert	Alert Time in
First	1	4 hr	8:00 am	0	null	null	no	null
			9:00 am	2	172.16.3.232	3389	yes	7 sec
					172.16.3.251	3389	yes	8 sec
			10:00 am	1	172.16.3.251	7016	yes	8 sec
			11:00 am	1	172.16.3.251	16371	yes	7 sec
Second	2	3 hr	10:00 am	2	172.16.3.227	3389	yes	9 sec
					172.16.3.235	16371	yes	8 sec
			11:00 am	1	172.16.3.235	3389	yes	7 sec
			12:00	0	null	null	no	null
Third	3	5 hr	12:00 am	1	172.16.3.235	16371	yes	8 sec
			2:00 pm	1	172.16.3.235	16371	yes	8 sec
			4:00 pm	0	null	null	no	null

VI. Conclusions and Future Work

The proposed AB-NIDS system can be used for anomaly detection; it can classify the normal an abnormal host on local networks and it is always used to find

intrusions. It has a good role in network security field because administrators of networks can depend on it to indicate the unauthorized access.

With compare to other works that are referenced in this field, AB-NIDS can be considered as a good system for detecting intruder and alerting system caregivers. On the other hand it gives good performance and reliability. Another advantage of this system is it automatically send alert to network monitor and short message to network administrator's mobile device as soon as possible it detects intrusion inside networks.

Future work can be concerned with the study of behaviour of intrusions depending on their generated traffic by analyzing their used protocols; we can get how they can attack local networks behind a firewalled router.

References

[1] Robin S. and Rao G., "Design and Development of Network Intrusion Detection System Detection Scheme on Network Processing Unit", ISBN 89-5519-129-4, 2006.

[2] Tansu A. and Tamer B., "An Intrusion Detection Game with Limited Observations", Technische Universit¨ at Berlin, Germany 2006

[3] Harley K., "Intrusion Detection Host-Based and Network-Based Intrusion Detection Systems', Thursday, September 11, 2003.

[4] Najeeb A."Development and Implementation of Network Security Manager", Master thesis applied to the University of Sulaimani, 2007.

[5] Wang Y., Huang G. and Peng D.," Model of Network Intrusion Detection System based on BP Algorithm", IEEE, 2006.

[6] kuiper A."SMS ALERT SYSTEM FOR WEB INTRUSION DETECTION SYSTEM", 2009**.**

[7] Robin S. and Rao G., "Software-Based packet Classification in Network Intrusion Detection System using network Processor", IEEE, 2006.

[8] Cheng Z. and Guo-Liang C., "A FAST DETERMINATE STRING MATCHING ALGORITHM FOR THE NETWORK INTRUSION DETECTION SYSTEMS", 1-4244-0973-X, IEEE, 2007**.**

[9] Milan T., Dusan B., "Design of an Intrusion Detection System Based on Bayesian Networks", WSEAS TRANSACTION on COMPUTERS ISSN: 1109-2750, Issue 5, Volume 8, May 2009.

[10] Francisco M., Francisco J., Diego M., Juan A., Héctor R., and Iren L.,'Network Intrusion Detection System Embedded on a Smart Sensor', IEEE, 2010.