(JZS) Journal of Zankoy Sulaimani, 2009, 12(1) Part A (103-107)
گۆڤاری زانکۆی سلێمانی ، 2009 بەرگ12 (1) بەشی A

Network Intrusion Detection System Based on Matching Logical Address and Port Number

Najmadin Wahid Abdulrahman Boskany
Department of Computer Science, College of Science Sulaimani, University Kurdistan Region\ Iraq.

Abstract

The aim of this paper is to design a significant system for detecting intrusion hosts inside computer networks. The goal is to let network administrators detect and discover if possible hackers (unauthorized hosts) that attempt to break into network infrastructure exist or no, who observe network traffic or try to cause service attack, by accident or with purpose.

Keywords: Network Intrusion Detection System (NIDS), Logical Address, Network Interface Card (NIC), Firewall, Application Programming Interface (API), Dynamic Link Library (DLL).

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. Protections involve inside and outside unauthorized accesses (intrusions), that result in either intentional or unintentional misuse or malicious alterations [1, 2].

An Intrusion Detection System (IDS) is a system for detecting such intrusions depending on network information that exists on the transmission medium at any given time. It can be broken down into some categories: System Integrity Verifiers (SIV), Log File Monitors (LFM), and Network Intrusion Detection System (NIDS). Network Intrusion Detection System (NIDS) is an important and integrated component of computer network infrastructure.

As a network security watchdog, NIDS is often deployed at the border of enterprise network to observe packets. Because of ever-increasing volume and speed of network packets, there is a need of better NIDS that can deliver result in real-time [3].

An NIDS system is one of most important techniques whose primary function is detecting intrusions in different ways. It monitors packets on the network wire and tries to discover whether an intrusion exists inside network system [4, 5].

Unlike most previous approaches of network intrusion detection system (i.e. signature-based, hardware-based), in this paper a new approach is proposed for designing network intrusion detection system based on detected abnormal traffics, especially some header fields like logical addresses and used secure port numbers fields of hosts via matching process.

This system has been designed using Visual Basic V6.0 programming language with socket Application Programming Interface (API), and it works under windows operating system environment.

The proposed NIDS system outline is depicted in figure (1).

Email:boskany@hotmail.com

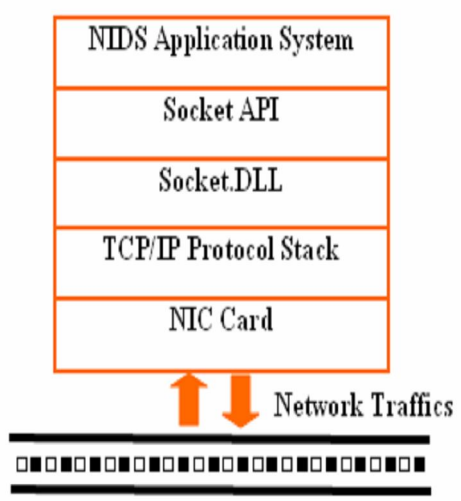

Fig (1) Proposed NIDS Outline

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

II System Architecture

The architecture of this NIDS system depends on taping into a network medium via the NIC of a host that is NIDS system runs on the host and capturing traffics. The host observes captured network traffics, which are generated by hosts inside the network. Afterwards the NIDS system analyzes partitions and distributes all parts of the captured traffics into fields. Then it distinguishes each part [6, 7].

After all parts of the traffics have been observed, the source logical address and destination port number will be compared with information in database that are already stored in the background of NIDS in a database file by network administrators. The stored information includes list of source logical addresses of permitted hosts and list of secured (closed) port numbers [5, 6].

The network intrusion detection system then detects anomalies of hosts that use the network. The idea behind this approach is to match such host information (i.e. intrusion IP address and port numbers), with information that is already saved by network administrator (i.e. legal IP addresses and secured port numbers) inside the NIDS system in two cases. Then, the system can trigger when there is a variation.

In the first case, after the NIDS gets the source logical address of hosts, it matches them with the list of logical addresses which are saved in a database file of authorized hosts to access the network, if detected logical addresses are in the same range of saved addresses, and then it means that the hosts are legal network hosts. Otherwise if it is not inside the list of addresses, it means that the hosts are intrusions and are not members of the NIDS network (i.e. the observed hosts have broken firewall of the internal network and accessed to network resources without authentication). Or they are internal intrusions with unauthorized host addresses. Here the system alerts the network administrator via a message and lets him/her know about these illegal host addresses.

In the second case, the NIDS system will compare 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 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.

Both of above cases can be happen in the same time or each one in different time

(i.e. NIDS can discover intrusion depending on just IP address or just on port number also there are some cases the host is intrusion and try to open a secured port in the same time).

III NIDS Algorithm Steps

The steps of how NIDS works and its role in saving networks from intrusions are illustrated below 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].

After 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 NIDS database which contain a range allowed logical addresses and secure port numbers. If the host addresses are known as legal host (i.e. its address is inside the logical address range of 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. On the other hand, if any port numbers opened by network hosts and the network administrator list the ports as secured port address, then 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. This is shown below in figure (2), flow chart of how NIDS detect intrusion is based on logical addresses and port numbers.

Finally, the system can count the number of the observed illegal host addresses, that they accessed the network in any given time, also in the same way; number of opened ports can be counted. Depending on these statistics of anomaly traffics the network administrators can have reaction to prevent intrusions.

Detail of these processes is illustrated in the next section.

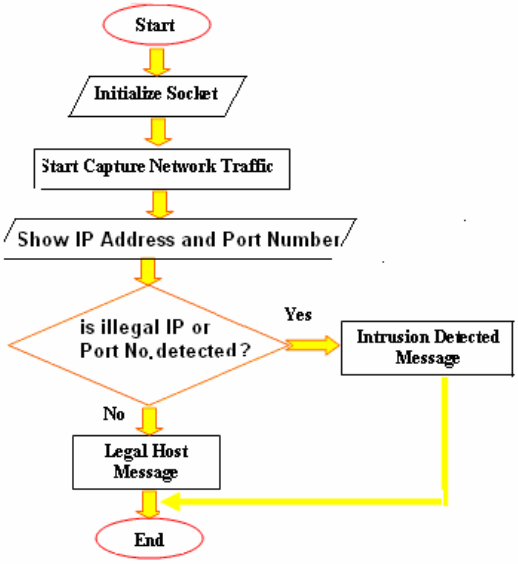

Fig (2) Flow Chart of Intrusion detected based on IP or port number

IV System Test, Result, and Discussion

When the network administrators wants to know who works inside the network, and what is going on in the background of the network, he/she can know that easily by running the NIDS system. The first step is to select the desired host logical address in the list of observed logical addresses, if the host that has been selected by the network administrator is a legal host (i.e. an authorized host), the system gives alert or message telling that this logical address is "Legal Host" Else, if the selected host is intrusion workstations (i.e. an unauthorized host) logged into local network and carried out tasks (i.e. using

ports that are already secured by the local network administrator), then the system gives a message that tells us "Intrusion Detected". Later, the system administrator can count the number of intrusions per time and can record this Information. This is something interesting to be noted and possibly taken action on.

In this test, about 165 hosts are used in local lab with 10.100.1.1 to 10.100.1.165 logical addresses range. The NIDS system discovered some intrusions based on their logical addresses like 10.100.1.188, when compared with a list of stored addresses and secured ports. The result is "Intrusion Detected"; because 10.100.1.188 is unauthorized host. Also port number 137 is located on the list of secure ports; as shown in figure (3) NIDS test result.

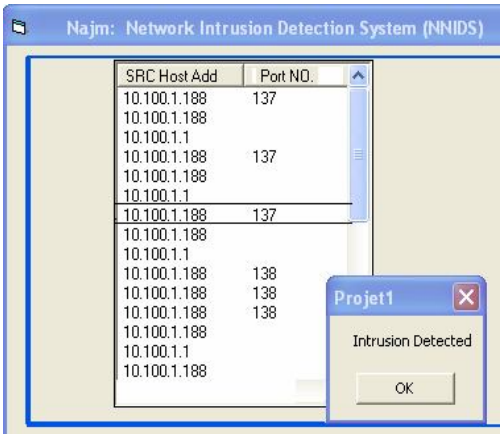

Fig (3) NIDS test result

The system has been tested with the network traffic that contains both normal and abnormal data and host. In experiments, after using this system in a specific organization for about 5 hours, the result proved that this system is effective because, as illustrated below, one can see clearly that all times intrusion exist without been noted, but when administrators and network managers use NIDS, they may see like this result. Here in this test, in a medium size local network (i.e. about 165 PC's the range of intrusion between 4 to 14 computers per time exists. This is illustrated in figure (4) detected intrusions per time.

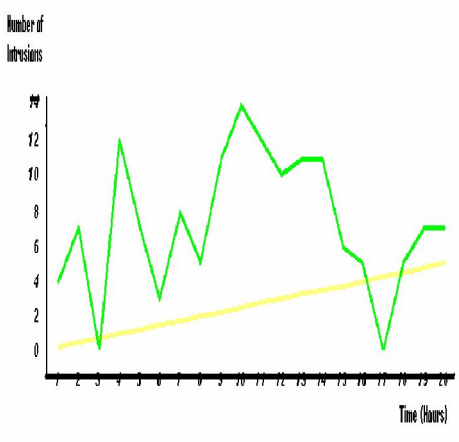

Fig (4) Detected Intrusions per Time

V Conclusions and future Work

The proposed NIDS system is used in anomalies detection; it can classify the normal an abnormal host on local networks. According this system is always used to find known and unknown 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 papers or works that are referenced in this field, this work's result is in good level, because every administrators can use it easily and can gets good result in short time and less cost and it cope small and medium size networks. Also other approaches that are mentioned before are in very good levels but may be they are more costly, complex using, or need more requirements like hardware.

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 firewall router.

References

1. Salim R. and Rao Radha Krishna G. S. V., "Design and Development of Network Intrusion Detection System Detection Scheme on Network Processing Unit", **2006,** ISBN 89-5519-129-4.,.
2. Najeeb A. A., "Development and Implementation of Network Security Manager" **2007,** M.Sc. Thesis ,University of Sulaimani,
3. Zhong C.and Chen Guo-Liang, "A fast determinate string matching algorithm for the network intrusion detection systems", **2007,**1-4244-0973-X, *IEEE*,
4. Blustein James, Fu Ching-Lung and Silver Daniel L. " Information visualization for and Intrusion detection System", *ACM*:, **2005**.
5. Salim Robin and Rao Radha Krishna G. S. V., "Software-Based packet Classification in Network Intrusion Detection System using network Processor", *IEEE*, **2006**.
6. Wang Y., Huang G. X. and Peng D. G., "Model of Network Intrusion Detection System based on BP Algorithm", *IEEE*, **2006**.
7. Bolzoni Damino, Etalle Sando, Hartel Pieter "POSEIDON:a 2-tier Anomaly-Based Network Intrusion Detection System", proceeding of the forth *IEEE* international on information assurance, **2006**.
8. Sekar R. guang Y. Verma S. and Shanbhag T., "A High Performance Network Intrusion Detection System", *ACM*, **1999**

سیستمی دۆزەرەوەی چونە ناوەوەی ڕێگا پێنەدراو بۆ ناو تۆڕی کۆمپیوتەری بە بەرواردکردنی ناونیشانی کۆمپیوتەر و ژمارەی پۆرت

نجم الدين واحد بۆسكانى/بەشی کۆمپیوتەر/کۆلێجی زانست/زانکۆی سلێمانی / هەرێمی کوردستان – عێراق

پوختە

مەبەست لەم تۆژینەوەیە دیزاین کردنی سستمێکی کارایە بۆ دۆزینەوەی بەکارهێنەرە ڕێگا پێنە دراوەکان لە ناو تۆڕی کۆمپیوتەرکاندا وە هەروەها یارمەتی دانی بەڕێوەبەری تۆڕەکان بۆ دەرخستی ئەم جۆرە بەکارهێنەرانە کە هەوڵ دەدەن ژێرخانی تۆڕەکان تێك بشکێنن وە بە بێ مۆڵەت بەکاریان بهێنن جا بە زانین یان نازانین

.

نظام كشف الدخول بدون إذن فى شبكات الحاسوب استنادا الى مطا بقة عنوان الحاسبة و رقم المنفذ

نجم الدين واحد بۆسكانى/قسم كومبيوتر/كليه‌العلوم/جامعة السليمانية /اقليم كردستان- العراق

الخلاصة

الهدف من هذا البحث هوتصميم نظام معنوى للكشف عن التداخل فى داخل الشبكات الحاسوبية و من خلال السماح لمسولى الشبكات باكتشاف المتسللين اللذين يحاولون اختراق البنية التحتية للشبكات بدون اذن .

وەرگیرا لە 22\4\2008 دا ، پەسەندکرا لە 5/11/ 2008 دا

Received , 22\4\4008 Accepted, 5\11\2008