STUDIA INFORMATICA
Nr 1-2(14) Systems and information technology 2010

Intrusion Detection Systems. Model and implementation of module reacting on intrusion to computer system

Andrzej Barczak
Grzegorz Bereza
Institute of Computer Science
Siedlce University of Natural Sciences and Humanities
3 Maja Str. 54, 08-110 Siedlce, Poland

Abstract: The problems of intrusion detection capabilities are considered in this paper. The general idea of structure, model of IDS (Intrusion Detection System) and overall construction is presented with emphasize many problems which appear while creating procedures of such a tool.

Keywords: intrusion detection, vulnerability scanning, IDS architecture

1 Introduction

Informatics is one of the fastest growing fields of science. The opportunities offered by computer systems are huge therefore they are used in all areas of economic and private life. Economic units are exploiting them largely for storing financial and employee data, however on private computers it is often possible to find e-mail correspondence, valid personal and official documents and many different pieces of information which can be object of desire for many unauthorized persons called crackers.

These people in order to break into the computer system are using various advanced techniques to detect weaknesses in operating systems and use various types of software installed into it. Gaining unauthorized access to the computer unit cybercriminal can cause intense losses in it ranging from loss of data, and ending on breakdown of the entire computer system. There are various reasons, which guided computer criminals. Many of them break into systems and develop scenarios of attacks, just to impress the community dealing with this type of activity.

The largeness of dangers awaiting computer systems and their users causes that it is become necessary to competent and correct protect of them. The war taking place between cybercriminals, organizations and persons responsible for safety causes that it is one of, as not most important, field of the computer science. Intensive work and the fight against computer criminals have led to create many advanced tools and techniques to protect them, one of them are Intrusion Detection Systems.

2 Structure of IDS systems

Intrusion Detection System (IDS) can generally be described as a tool, whose task is to identify attempts to breach the security policy of the computerized system and respond to them. They consist mostly of some of the following components:

- Knowledge base that stores different types of information used in identifying attacks to be effectively exploited should be able to query processing, add, edit and delete data.
- Sensors receive data directly from the protected system. Because without information about activity of system it is impossible to detect intrusion this element is critical section of IDS. They may have the form of a computer program or a physical device redirecting network packets to the appropriate processing units.
- Alarm module which informing person responsible for the security about detected attack. Newer and more advanced IDS tools are not only transmitting the information to the administrator but also determined programmed activities, being able to prevent the attempt of the attack or restore the system to previous state. Despite the many different activities offered by this element information to administrators about the attacks can be considered as the most important, because without any information it is impossible to effectively protect secure system;
- Audit diaries, which are elements of protected system, store different types of data about activity of protected system such as utilization of authentication mechanisms, operation on objects and system files etc.
- Processing mechanisms responsible for analyzing data transmitted by sensors. Algorithms implemented within this component can be additionally equipped with various types of filter modules, whose task is to narrow the set of input information. Each of those mechanisms should be devoted to the analysis of only one type of data (for example: audit records, network packets, etc.);
- Management module, whose main task is coordinate the work of all components of the intrusion detection system. In addition, this element can be equipped with a variety of additional functions supporting its work, such as data sets management, mechanisms tracking source of attack, configuration, etc.;
- Control console which is a kind of overlay on the management module. With this console, the person responsible for security infrastructure has easy access to features and other capabilities of IDS. Often it has a form of graphical user interface (GUI).

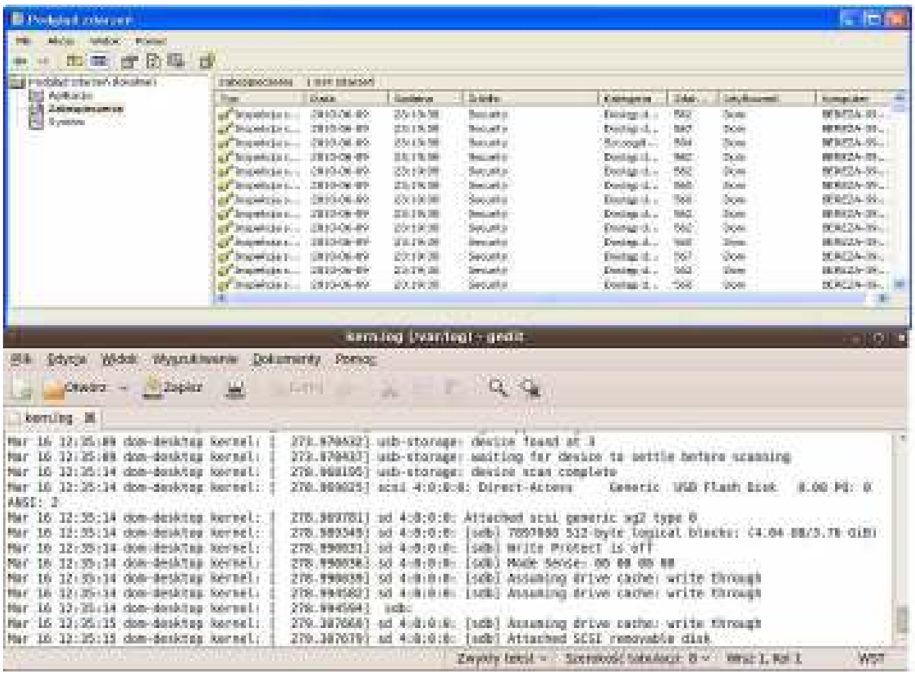
Considering the deployment of intrusion detection system elements we can distinguish the two main types. The first of these systems are hosts, which all individual components are on one computer system, while the latter are those whose elements are located in different nodes of the network. IDS network architecture requires an efficient communication medium. Reliable information transport causes that attack detection tools work effectively and efficiently, even when carrying out an attack on a given IDS communication infrastructure. Using a virtual private network (VPN), which provide encryption of transmitted information via special keys is the most common solution.

3 Intrusion Detection System model

Implementation of the project which creates an intrusion detection system is quite complicated and time-consuming process. First step which must be done at the beginning of any design work is the designation of such a tool, which largely determines its construction. One of these factors which can be taken into account is the used operating system, which may characterized by different security standards and data formats and their accessibility.

Type of system software reflected in significant degree on data collection techniques for analysis. Sometimes the access to the interesting information is straight and doesn't require great loads. In different operating systems downloading the same data can be impossible or to accomplish this is to use a number of additional tools and libraries.

Downloading and availability of relevant data is not the only problem. Information from one system can have completely different format than from the other one and because of this processing engine must be specially adapted. Great examples presenting this state of affairs are the audit logs of Windows and Linux. Both are holding various types of information about the functioning of the operating system, but the format is so different that it requires use of entirely different methods of analysis. Figure below shows the Windows audit log at the top and Linux at the bottom.



```
Mar 16 12:35:09 dom-desktop kernel: [  273.870432] usb-storage: device found at 3
Mar 16 12:35:09 dom-desktop kernel: [  273.870437] usb-storage: waiting for device to settle before scanning
Mar 16 12:35:14 dom-desktop kernel: [  278.868105] usb-storage: device scan complete
Mar 16 12:35:14 dom-desktop kernel: [  278.869025] scsi 4:0:0:0: Direct-Access     Generic  USB Flash Disk   8.00 PQ: 0
ANSI: 2
Mar 16 12:35:14 dom-desktop kernel: [  278.889781] sd 4:0:0:0: Attached scsi generic sg2 type 0
Mar 16 12:35:14 dom-desktop kernel: [  278.889349] sd 4:0:0:0: [sdb] 7897088 512-byte logical blocks: (4.04 GB/3.76 GiB)
Mar 16 12:35:14 dom-desktop kernel: [  278.890831] sd 4:0:0:0: [sdb] Write Protect is off
Mar 16 12:35:14 dom-desktop kernel: [  278.890836] sd 4:0:0:0: [sdb] Mode Sense: 00 00 00 00
Mar 16 12:35:14 dom-desktop kernel: [  278.890838] sd 4:0:0:0: [sdb] Assuming drive cache: write through
Mar 16 12:35:14 dom-desktop kernel: [  278.894582] sd 4:0:0:0: [sdb] Assuming drive cache: write through
Mar 16 12:35:14 dom-desktop kernel: [  278.894584]  sdb:
Mar 16 12:35:15 dom-desktop kernel: [  279.387668] sd 4:0:0:0: [sdb] Assuming drive cache: write through
Mar 16 12:35:15 dom-desktop kernel: [  279.387679] sd 4:0:0:0: [sdb] Attached SCSI removable disk
```

Figure 1. Difference between audit logs from Windows XP and Linux

However, type of system software doesn’t a major impact on the processes of analysis, if the proposed IDS scheme will base their work only on network packets. Any mechanism for analyzing network traffic for different operating systems may be the same because all the inputs from the network have the same format set out in special RFCs (ex TCP packets.). Very great popularity of operating systems from the Windows family caused the fact that the considerable number of attacks was being carried out to computers working under the control of this software. This is why IDS is a tool created for Windows XP. After the decision about choosing the operating system for which the intrusion detection system would be created it comes time to decide upon the methods used to recognize the attacks. The most popular are the processing of audit log records and analysis of the network traffic. These two ways to identify intruders will be used in the created IDS system.

The next step is to develop general architecture of IDS, which depends directly on the localization of individual components in the IT infrastructure. Due to hardware and software limitations, all components will be placed on a single computer, which will be the tool of IDS type.

Since all elements of intrusion detection system will be operated in a computer environment there is no need to use appropriate means of communication, such as VPN or SSL for messaging statements and data. Exchange of information between sensors and the processing mechanisms will be carried out through a specially designed buffers access to which will have a special manager, controlling all the operations performed on it. Sensors will write new data to the end of the buffer, and processing mechanisms will collect them from the beginning and then they will be kept by the order of their appearing in the protected system. After reading the item buffer will be removed.

Significant problem in designing such type of solutions is very large amount of data read by different types of sensors, and then forwarded for further processing. Peculiarly this problem can be visible during analysis of packages in webs with the very great bandwidth and traffic. Therefore, such elements are often fitted with filters that are able to narrow down a set of data to be checked. In the proposed system both network packets sensor as well as extracting and collecting of the audit log records will be equipped with simple filters. Trapped packets will be filtered in two stages. The first of these will provide further only TCP, UDP and ICMP packets, and the other will act as a firewall, which will verify that the sender of the package and the port does not appear on the "black list" and if the data will be matched it will be rejected, and then the sensor will attempt to break the connection with its sender. However, the sensor filter retrieves audit log records will send only those entries that define the error, warning, or failure complying with any operation, and the remaining will be rejected.

Data processing mechanisms will have the form of separate processes which will still check whether data is in appropriate buffers for charging. The audit log record analyzer after reading a single entry will select the most characteristic data describing it, and then based on the knowledge base will check whether a similar record is not found in it. All related records will be counted and the time interval since their last appearance will be checked. If this time will be fitting in the established period, system will treat the given record as the attempt of the attack and will no longer check the number of their instances. In the case, when none of records picked up from the base will be answering to this condition system will checking whether their number didn't exceed established threshold value. Exceeding this parameter will be treated by IDS as warning about the dangerous situation which can mean that in the protected system some peeped activity repeating itself can take place. Quite another action will be characterized network packet analyzer, which will take the decision about attack in basis of signatures contained in the knowledge base. When you run this item, it will read all the available signatures and group it by type of protocol. After loading the data it will start the main process of analyzing the data read from the buffer. Reading out the package of the determined type will cause induction of the appropriate analyzing method which will examine its suitability to any of the rules. Both mechanisms of data processing after the decision of the attack or the symptoms of it will provide all relevant information to the alarm module.

The element responsible for raise the alarm won't be, as previously discussed, in a separate process components, but only the function that will be caused by an appropriate analyzing mechanism. This module will be received from the analyzer all necessary information about the accident. Depending on the mechanism that raised the alarm this data will differ from each other. When the audit log record will provide information about the intrusion, then to alarm function except text message and the date of detection will be forwarded the entire analyzed record, which content will then be entered into the tables in the knowledge base and inserted in an e - mail that will be sent to the administrator. A similar situation will be in case of mechanism for analyzing network traffic. Then to the alarm function will be forwarded appropriate package, which is a source of danger.

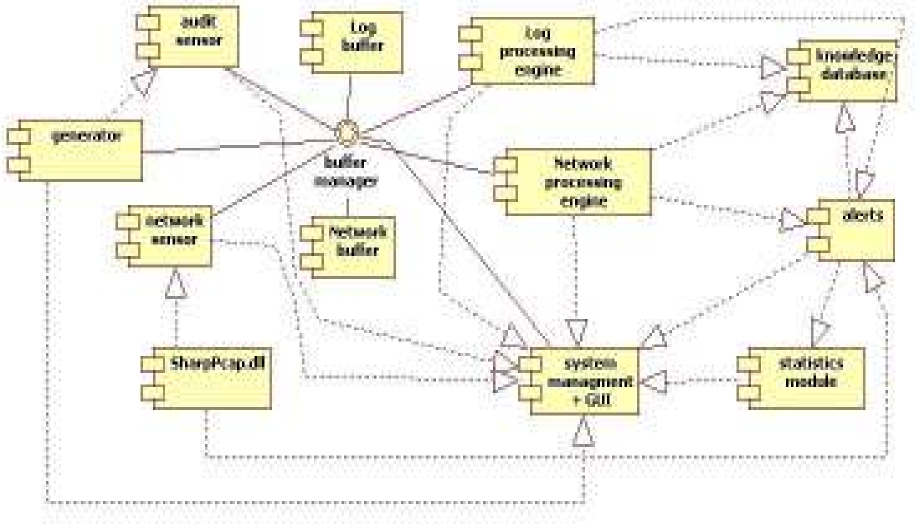


Figure 2. The overall construction of an intrusion detection system (source: own)

The work of all the above mentioned elements will be under control of a special manager, whose task will be monitoring the activities of all these components and in case of failure one of them trying to repair the fault. Management of IDS will be integrated into the control console, which will make available all the features offered by the application. Moreover it will be possible with her help observing the state of individual mechanisms and detected threats.

Attack generator would be an element in what will be equipped intrusion detection system, and which task will be creating different types of data transmitted to the analysis mechanisms in order to verify their effectiveness. It will consist of two separate processes, from which each of them will generate data for an entirely different method of intrusion detection.

In addition, IDS will have the statistical module, which will keep statistics of intrusion detection methods. The figure above shows the overall construction of an intrusion detection system.

An important element in the design of this type of solution is providing some degree of safety against other users. Therefore, this system will be equipped with authentication mechanism, which will ask for a password when you try to boot, shutdown and display the control unit console. Thanks to it unauthorized users won’t be able to shutdown system, or launch any application with additional features.

4 Problems encountered during implementation

During the programming work on the system it belonged of solutions of some major issues related to performance across application and protected system on which it is supposed to function. Exact tests of the first version of IDS have revealed a significant drop in speed of the whole computer unit. The reason for this was a very large number of internal processes initiated by the developed program, which took up computing resources for other applications such as word processors, web browsers and many other daily used programs, thus using this system was very cumbersome and tiring.

The solution for this situation was a deliberate slowing down of the process by stopping them for a short time. Of course, this method couldn’t be used for all processes. The only process which couldn’t be slowed down in this way was a sensor collecting network packets and a mechanism for handling them. It wasn't possible to artificially slow down these two elements since then would exist danger that they won't keep up in analyzing newly read network packages what after the certain time could supply to overflow network buffer, or breakdowns of system.

Eliminate the situation when the data buffers will be filled have been carried out by creating a special manager, which controls all operations performed on them. Eliminating the situation when buffers of data will be overfilled was made by creating the special administrator which is manipulating every of operations carried out on them. Before performing any write or read operations from the buffer manager checks if it is possible, and then just doing it.

Another very important problem that because of the functionality of the created system had to be resolved was to accelerate the work mechanism for analyzing the network packets. This situation was detected only during testing of this module in high network load. Large influx of packages caused need of very frequent resorting to the knowledge base to search for a suitable signature for a significantly efficiency decrease of the system. This problem was solved by the load while starting of this process all the rules for special tables and use of special mechanisms for filtering and searching for the appropriate rule.

Other activities that it had to be performed during the programming work were various problems of optimization and improvement of less efficient algorithms. Performing all steps described above led to the emergence of effective and efficient intrusion detection system.

5 Conclusion

Intrusion detection systems are very complicated and advanced tools, which may consist of many different kinds of programs as well as physical devices. The programs used in these schemes are often used to filter and analyze input and make decisions about the alarm and counter the effects of the detected attack. However, physical facilities form the basis for this type of software, including: servers with high processing power. Normal router which redirects traffic to a specific sensor can also be a very important part of the whole infrastructure of an intrusion detection system.

The creation of such tool is a very difficult and time-consuming task. In implementing such systems it should be solved many important problems. One of the most important is the performance of used algorithms, which has a direct impact on the speed of response to emerging threats. Host type IDS working in given environment, which are normally used by the users can't greatly slow down the speed of their work. You may find that their presence shouldn't be noticeable to user during normal use of computer unit. In designing such mechanism must be found the "golden mean" between speed and its effectiveness.

References

1. Amoroso Edward: *Sieci: Wykrywanie intruzów,* Wydawnictwo RM, Warszawa 1999, ISBN 83-7243-039-X
2. Alex Lukatsky: *Wykrywanie włamań i aktywna ochrona danych*, Wydawnictwo Helion, Gliwice 2004
3. Put Damian, Adamczyk Wojciech, Wróbel Adam: *Szkoła Hakerów – Podręcznik*, Wydawnictwo CSH, Kwidzyn 2006
4. http://www.symantec.com
5. http://pjwstk.wafel.com/bsi/BSI-09-wykrywanie%20wlaman.pdf