STUDIA INFORMATICA
Nr 1(12) Systems and information technology 2009

A project and implementation of the testing system for Intrusion Detection Systems Part 1

Andrzej Barczak
Andrzej Orzoł
Institute of Computer Science, University of Podlasie,
3 Maja Str. 54, 08-110 Siedlce, Poland

1 Introduction

In the first part of the article there will be described basic terms and problems concerning IDS discipline and penetration tests. The second part of the article will show the model of the testing system of the Intrusion Detection Systems.

In the time of a rapid development of the information technology (IT) many companies and organization, and even private people who decided to used it, still encounter new and extraordinary difficult challenges that is a protection of classified data from an unauthorised access. Every day, the battle with destructive power of crackers is taking place to keep the safety of information systems. Unfortunately, strengths of this fight are not balanced and a single gap in the system is enough to break it down. Operators of attacked systems encounter a difficult task of tracking the greatest number of security gaps and correcting them.

Recently, an increasing number of automated tools of attack used by the crackers started to appear on the market and advance defence systems. Even already known firewalls start to gain many new functions and they classify them under the name of Intrusion Detection Systems (IDS). The discipline connected with IDS is still new but extremely fast developing. The intensive development is encouraged by the demand of this type of solution, but also other disciplines in the range of IT discipline such as the cryptography and the artificial intelligence (AI). The features such as the speed of modern computers and multi-tasks operating systems allowed for introducing of real time protection which allows for effective blockade of attacks.

We cannot discus a wide issue such as IDS without a proper introduction of basic terminology. In order to begin, we should introduce key terms: a hacker and a cracker, which are often misunderstood. A hacker is a person who using his knowledge and skills solves specific and difficult problems. What is more, a hacker in opposition to a cracker does not act illegally.

Under the term of an attack on an information system we understand every even failed attempt of incursion into an information system. Only if the attempt is complied with success we can call it a breaking. In order to understand it clearly, we need to divide it into 3 phases:

- the introduction phase – collecting the data for attack. It is the most important of phases, which decides about the success of an attack. The attack in this phase is only planned and cannot be detected.
- the proper attack phase – it is an actual attack with usage of collected data. In this phase, there are attempts of breaking the system security programs in order to get the access to chosen resources. During this stage the attack if detected can be stopped, otherwise we call it a hacking into the system.
- the finale phase – a result of the hacking to the system is deletion of folders and a leak of classified data. Each operation leaves tracks in systems log and even in the folders with data. During this phase we can still establish who was an intruder and what data were lost.

To differentiate an attack from a breaking we need to differentiate a process of breaking detection from a process of intruder detection. The first one recognizes an attack, identifies its aim and effects. The second one recognizes its source i.e. people or organizations responsible for this attack.

2 The Classification of Intrusion Detection Systems

The Intrusion Detection Systems expand their areas of influence in an information systems by variety of solutions covering placement, runtime mode, reaction or form of data acquirement for analysis by IDS systems and introduces a classification. The IDS classification is non-uniform, one system may work on many levels and the other one may fulfil a single function. Using those aspects, we achieve following divisions according to:

Protected system's elements:

- the level of an application and a database
- the level of an operating system
- the level of a network

Placement in a network:

- an integration with a firewall
- inside of a network

Sources of data for analysis:

- a host based – data originated from a single host
- a network based – data originated from a local network

Manners of attack detection:

- a behaviour based
- a knowledge based

Frequency of a system usage:

- a real time
- a periodic runtime

Reactions during attack detection:

- passive
- active

The IDS differentiation of application levels and databases aims to point a new trend connected with attacks in past years. When servers become more and more protected and a front attack usually fails, the attention of hackers concentrates on incorrectly written applications running these servers. For instance the WWW servers, which are the targets of this types of attacks, where giving too long address or password may end up in access to classified documents. On this level, IDS operates mainly on data covering chosen applications.

The IDS level of an operating system, is most often acquired form the market, implemented by many anti-viruses systems. They inform about attack attempts on a host, not updated software, or an unauthorized attempt of communication.

A level of a network is the most broaden discipline in which IDS operates. Variety of communication protocols, applications and transferred data enforces huge amount of resources for this part of systems. IDS of this discipline are often specified separated devices attached into a network structure.

About integrated systems with firewalls, we speak when they have a certain influence on firewall's inference and defining of the rules. IDS of this type can be named “fore guard”. When placed ahead of a firewall, they acquire information about every incoming packet and behind the firewall they acquire information about a packet coming through.

IDS placed inside corporation's network help to identify an internal movement of an internal network motion and any legal operation of a user which is outside his/her privileges. Agent systems have a certain advantage in this discipline, they are distributed around whole infrastructure to decline the risk of system paralysis which appears in a classical architecture.

Behaviour based systems, also called anomaly detection systems, during the first phase of operation acquire information about typical behaviours of users and a network motion. After the learning phase is finished they start regular operations, which are to alarm about every abnormal behaviour and anomalies in system's operation not compliant with earlier registered knowledge. An advantage of this approach is the possibility of a attack detection not registered earlier. A disadvantage is a generation of amount of false warnings and possibility of errors during the learning, in case when the system was already attacked in this phase. Knowledge based systems are based on available databases of an attack signature. They generate lesser amount of false alarms but they do not recognize attacks which scheme doesn't fit to those in the base. The main problem in the systems of this type is a frequent actualization of signatures, which the base is still growing.

The Intrusion Detection Systems run base their operations mainly on reviewing firewalls’ logs or system’s logs. Their operations are often too slow to blockade an attack in its realizations. A disadvantage of this approach is possibility of system's performance decrease, cost by its uneven load in time.

The IDS operating in real time generate bigger system load but they bring many advantages. Attacks detected on real time strategy are classified immediately, that give the possibility to prevent them.

Passive systems limit themselves only to alert system's operators about events. In case of IDS active reaction, we speak about prevention of an attack which was earlier foresaw. The form of this reaction can be defined in an almost every possible way.

In practise, various hybrid approaches or applied, combining advantages of already mentioned solutions of which SNORT can be an example, is based on standard attack signatures, now with new module allowing for anomaly detection.

3 Intrusion Detection Systems as active form of defence

More and more IDS available on the market are characterised by real time mode and active reaction. Defining of reaction policy was simplified, often lead by automatic configuration system where a user answers questions in a questionnaire. More advanced systems allow for any role configuration and launch of any system command with correct parameters. Reconfiguration of a firewall, reconfiguration of hardware, or launching of additional protection mechanism could be an example of this kind of usage.

It allows not only for active defence but also for counterattack e.g. on a popular denial of service (DoS).In this case counterattack means to send back incoming packets to a sender or as in Distributed Denial of Service (DdoS) to the web page of an aggressor. Sending back of the packet to the sender doesn't arise any discussion but redirection of the motion into chosen target maybe illegal. What is more, a wrong defining of an intruder may result in blocking a random web site.

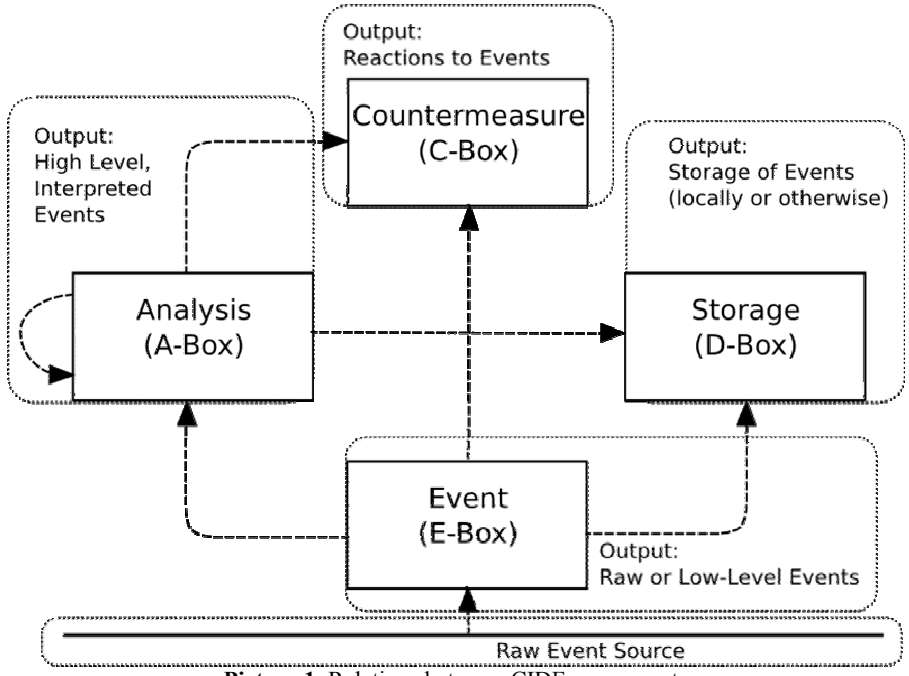
The interesting characteristic of an active form of defence are deceptive systems. Those systems are specifically crank out to look as valuable nodes in a network in the eyes of intruder, as being purely protected and with high privileges (e.g. DNS Server). The task of this kind of systems is to feint an intruder by making false data accessible and simultaneously acquirement of data about an attack and its source. A processing of this types of systems is quite effective, especially in the case of intruders with pure experience. An intruder not knowing about continuing monitoring of his steps feels confident in an apparent purely secured system, making many errors and giving its identity.

There are two categories of deceive systems. The first of them are traps which work on a secured node. They can be defined as a set of some functional elements which uses deceit in order to divert the intruder’s attention from important system resources.

The second group are systems imitating existence of whole computers or network segments. They are mainly installed on separated and specifically chosen hosts. The systems of this class simulate services, operating systems and even imitate motion in the network in order to increase authenticity of this impression.

4 The architecture of Intrusion Detection Systems

The IDS architecture conception is very miscellaneous, the number of IDS equals the number of solutions. It's too difficult to state a common architecture of these systems which can reconsider all of them. The common intrusion detection framework project (CIDF) describes a set of components which defines IDS. Those components include event generators "E-boxes", analysis engines. "A-boxes", storage mechanisms "D-boxes" and event countermeasures "C-boxes". Each CIDF component maybe an independent software package or any package included in a bigger system. The diagram below (Picture 1) shows relations between CIDF components.



Picture 1. Relations between CIDF components

The aim of a "E-box" component is to provide information about events to the rest of the system. This can be a complex event or in the case of network intrusion detection system (NIDS) can be a anomaly taking place in a level of network's protocol. Those components perform a function of sensors of IDS, without them IDS is "blind".

A-boxes analyse input from the event generator. Majority of the attention in research on IDS is concentrated on designing and development of means of analysing data streams in order to acquire in real time security information on highly detailed level.

E-boxes and A-boxes may generate plenty of data. Those information must be stored in a way that allows for a fast and easy access of their system's operators. It is a D-box component that defines resources and means used to store data concerning security.

Majority of IDS is equipped in a form of event countermeasures ("C-box") in an automatic and defined form. The most frequent form being used is to shot TCP/IP connection, modifying firewall rules or even in critical situation – to shut down a system.

5 The criteria of Intrusion Detection Systems grading

Each system has some characteristic features and properties which in given situation are its disadvantages or advantages. While choosing IDS we need to use some norms, according to which we will grade systems. While speaking about a grading criteria of such a large and various group we need to dived it into smaller groups with similar characteristics. In this part of this article I will show the grading criteria for three basic groups described already at the beginning of the article. They are IDS of three levels: an application and a database, an operating systems and a network.

There is a general group of universal grading criteria for all of this levels, so there is no sense in their separated description. So, they will be enlisted below:

- The number of detected attacks in proportion to the number of attacks
- The number of false alarms in proportion to all attacks
- The number of blocked attacks in proportion to all detected attacks
- The frequency of updating of attacks signatures
- The number of used system resources with low, medium and high IDS load
- The configuration possibility (e.g. a possibility of defining own rules)
- Scalability to specific needs
- Enforcement, exploitation and conservation costs

Considering criteria for every single level we need to remember, that those enlisted above must be taken into account.

The Intrusion Detection Systems of the application and database level

In IDS of the application and database level, the division into two small groups takes place according to their operation. The first group – IDS –operates based on data analysis given mainly by chosen log files(e.g. Real Secure Server Sensor System). The main advantage of these programs is possibility of adapting them to all applications using log files to register their activities. However, their disadvantage is configuration difficulties cost by verity of used formats in chosen log files. The second group contains designed and implemented IDS for chosen applications. This activity decreases universality of these systems, increases effectiveness.

Independently from an above division on a general level we can distinguish a grading criteria:

- A degree of system's flexibility according to a concrete group of unwanted specific invents in a given discipline.
- The number of detected attacks overlooked by a lower level IDS.
- Complexity of solutions according to a chosen product group.
- A range of served products according to a version of the product.
- Resistance against errors and gaps of used applications.

In the case of a application and data bases level systems, there are many difficulties in defining an uniform grading criteria, which function on the highest OSI model layer.

The Intrusion Detection Systems of the operating system level

Very popular and most frequently installed operation level systems are characterised by a firm connection with a chosen operating system during designing phase. Highly integrated occurs in the operating system kernel level. It influences positively increase of efficiency of this level IDS. The main factors influencing effectiveness of the IDS operation of this group are:

- Access control manners to system resources.
- Registration manners of users operations.
- The number of detected abnormal user and applications behaviour.
- Security management of users accounts.
- Detection of intrusion to protected runtime modes.
- Possibility of activities in environments using encoding.
- Security against attempts of performing reserved operations.
- Full system scan in order to state up to date and detecting of security gaps of used system version.
- Effectiveness of used compression manners in case of used log files.

The Intrusion Detection Systems of the level of network

Network's level IDS is the most effective among the last two groups. It results from a lower abstraction level. A limited number of protocols result in an easy manner of system scaling and is characterised by high resistance against errors. Another characteristic of this type of IDS is a possibility of their implementation independently from a platform. In this case a grading of IDS is influenced by factors:

- The number of protocols served by IDS.
- The types of scanning degree of packets
- Sensitivity for periodically repeated attacks
- Sensitivity for distributed attacks
- IDS effectiveness in blocking DoS and DDoS attacks

For above mentioned characteristics IDS of the level of network gained testing methodology. It is included in a document called "Open-Source Security

Testing Methodology Manual 2.2.(OSSTMM 2.2.)" in section "C - Internet Technology Security".

According to given specification for the full test of IDS of this level we need to perform following steps:

IDS and features identification

- Verify the IDS type with information collected from intelligence gathering.
- Determine its sphere of protection or influence.
- Test the IDS for alarm states.
- Test the signature sensitivity settings over 1 minute, 5 minutes, 60 minutes, and 24 hours.

Testing IDS configuration

- Test the IDS for configured reactions to multiple, varied attacks (flood and swarm).
- Test the IDS for configured reactions to obfuscated URLs and obfuscated exploit payloads.
- Test the IDS for configured reactions to speed adjustments in packet sending.
- Test the IDS for configured reactions to random speed adjustments during an attack.
- Test the IDS for configured reactions to random protocol adjustments during an attack.
- Test the IDS for configured reactions to random source adjustments during an attack.
- Test the IDS for configured reactions to source port adjustments.
- Test the IDS for the ability to handle fragmented packets.
- Test the IDS for the ability to handle specific system method attacks.
- Test the effect and reactions of the IDS against a single IP address versus various addresses.

Reviewing IDS logs and alerts

- Match IDS alerts to vulnerability scans.
- Match IDS alerts to password cracking.
- Match IDS alerts to trusted system tests.

6 The Conclusion

The Intrusion Detection Systems is a still developing discipline. Availability of many market solutions with various parameters pushes system administrators to fallowing its development.

The grading criteria shown in this article are only general guidelines. The basic condition of full success of choosing ideal IDS is a description of security need

for used system, to conduct complex security audit. Only clear and precise grading criteria based on report of complex audit allows for optimal choice of IDS.

Before launching a new Intrusion Detection System, it needs full testing, as was shown in the case of network level they are not difficult to run but laborious. Testing of various configuration using the same tests may take even several days. Existing security scanners give only a kind of draft of possible gaps without giving information about important IDS characteristics resulting from log files analysis. There is a need to automatise laborious but necessary activities which lead to increase of effectiveness of IDS.

References

1. Dhanjani N., Clarke J., *Network Security Tools: Writing, Hacking and Modifying Security Tools*, paperback - Apr 4, 2005,
2. Bauer M.D., *Linux Server Security*, paperback – Jan. 18, 2005,
3. Rash M., Linux Firewalls: *Attack Detection and Response with iptables, psad and fwsnort*, paperback - Sep 15, 2007,
4. Erickson J., Hacking: *The Art of Exploitation, 2nd Edition*, paperback – Jan. 11, 2008,
5. Lukatsky A., *Protect Your Information: With Intrusion Detection*, paperback - May 30, 2004.