Journal of Information and Knowledge Management
Information Impact
ISSN: 2141- 4297 (PRINT)
ISSN: 2360 - 994X (E-VERSION)
Vol. 2(1), 2011

INTRUSION DETECTION SYSTEMS:

COMPLEMENT TO FIREWALL SECURITY SYSTEM

By

Adam M. Saliu; Mohammed B. Abdullahi;
Mohammed I. Kolo&Abdullahi R. Ozigi

Abstract

The main purpose with firewall is to protect against unauthorized external attacks but it will normally leave the network unprotected from internal attacks or intrusions. Fire walls and access control have been the most important components used in order to secure network and its resources. They work to prevent attacks from taking place or getting into the internal network. However the attackers seldom get their way into the internal protected network, by bypassing the security systems offirewalls and other access control measures. These security measures do not know what happens inside once they are bypassed. There is, therefore needforanothersystem that - will help detect these threats and possibly remove them. This system, which this paper seeks to explore, is called Intrusion Detection System. This will make the network and its resources more secured.

Keywords: Intrusion, Firewall Security, Detection,Access control, network security.

Introduction

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, complete prevention of security breaches appears presently, unrealistic. We can, however, try to detect these intrusion attempts so that actions may be taken to repair the damage later. This field of study is called Intrusion Detection. Rebecca (1999) defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to access information; manipulate information, or render a system unreliable or unusable.

Intrusion detection could also be defined as the process of identifying and responding to malicious activities targeted at computing and networking resources. The malicious activities here refer to the actions that jeopardize the confidentiality, integrity or availability of information or resources. Thus, “an Intrusion Detection System (IDS) is a computer system (possibly a combination of hardware and

software) that attempts to perform intrusion detection". (Martin and Markus 2003). "A secure computer system is a system that can be depended upon to behave as it is expected to do" (Rebecca, 1999). In other to achieve this, the components that make up the system must, at some point, be trusted. In the first place, the hardware has to be trusted to behave as expected, thus minimizing the possibility of hardware failure. Secondly, the installed software must he trusted to behave as expected and thirdly, the users of the system must be trusted to behave as expected. The trust must be extended to all people connected to the Internet, that is, they must behave as expected. Since trust is a delicate virtue and often abused, a way to protect our computer systems, detect any malicious activity and react upon the detection mustbe found. Martin & Markus (2003) noted that prevention measures are measures that check assets from being damaged; measures that allow you to detect when an asset has been damaged, how it has been damaged, and who caused the damage; measures that allow you to recover your assets or to recover from damage to your assets. In other words, every protective measure must take into account prevention, detection and reaction (PDR). An Intrusion Detection System is required in spite of Firewall because ofthe following reasons:

- It is hard to configure firewall properly
- Hacker/Cracker can get some packets through most firewalls and firewalls don't know what happens once someone gets through them.
- The software contains a software bug (software always has bugs).
- Bad protocols can be blocked by the firewall but HTTP is allowed through and 'hack' in HTTP will pass through.
- The firewall can only protect against known problems.

Model of Intrusion Detection System

A multitude of configurations exist for intrusion detection systems and there are many different opinions designations on what an IDS looks like. Although, an existing model that was both complete and generic could not be found, figure I is an attempt to develop an Intrusion Detection system model.

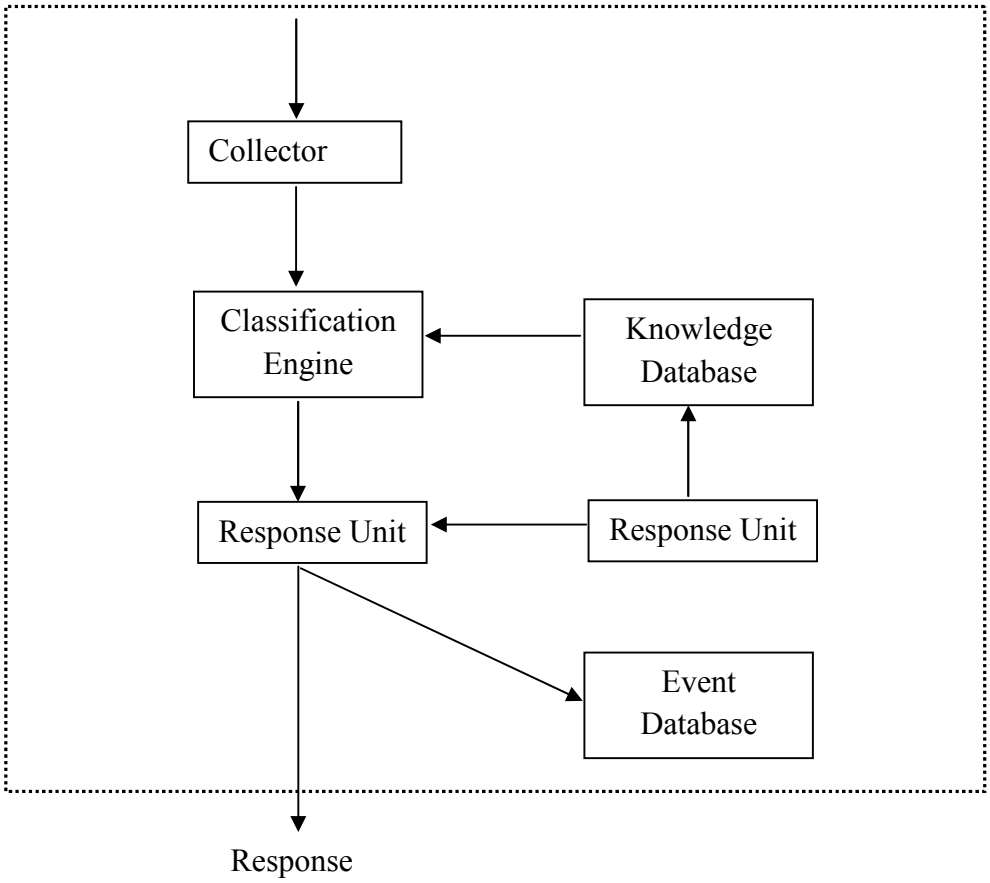

Figure 1: An IDS model *Source: Field work (2011)*

Each box is considered as a stand-alone component, which performs a single task. The arrows describe the information flow. The boxes with lighter outlines are not necessary for IDS to be operational, although almost every IDS today utilize them. The components can either be deployed separately or made to reside in the same physical system. The components are described as follows:

Audit Source

This serves as the input to the IDS. Input is the raw data, which can have several different formats depending on the type of IDS and where it is located. Instances of audit sources are application logs, system calls IP-packets and the output from otherIDSs.

Collector

The collector samples the audit source, either in real time or periodically, and preprocesses the information. In preprocessing exercise, the sampled information is transformed into an internal standard format, known by the analyzer. A preliminary reduction of data, e.g. the grouping of similar log entries, is often a part of the preprocessing step. If the IDS is monitoring some kind of connection-oriented protocol, the connection may cache the network packets for session reconstructions.

Analyzer

Classification engine and knowledge database constitute the analyzer. The analyzer is responsible for determining if the data sent by the collector contains signs of an attack. When an attack is found, the analyzer produces one or more events that are passed on to the response unit.

(a) Knowledge Database

The long-term memory of the IDS is the knowledge database. It contains detailed attack information that varies depending on the type ofIDS.

(b) Classification Engine

The classification engine determines if the data received from the collector is proof of attack. It does this by comparing the data with the information stored in the knowledge database according to one more detection methods. The method could be knowledge-based (which has some kind of knowledge about how attacks look), or behaviour-based (which uses normal behaviour as the basis to determine bad behaviour). If signs of attack are found, an event is constructed containing all the relevant attack-related information. The event is usually classified according to the severity of the attack and then passed on to the response unit.

Response Unit

This unit decides which actions to perform depending on the incoming events and the level of severity. The responses could be passive *alerting or response* (involves notifying the appropriate person or system of the actions to take regarding an attack that has taken place and detected by the IDS), *reactive response* (has to do with stopping the attacker from gaining further access to resources, thereby mitigating effect of an attack), or proactive response (intervenes and actively stops an attack from taking place).

Policy Rules

These rules allow the configuration of the IDS that should perform detections and react to intrusions. This it does by allowing one to select a subset of the knowledge database to use in the analyzer and choosing which responses a certain event should trigger in the response unit. Since this feature is optional, IDS without this module would always use the whole knowledge database for intrusion detection and always respond to attacks in a predefined way.

Event Database

The event information produced by the IDS is stored in the event database. The policy rule controls the decision taken from response unit regarding the logging of an event. The database can later be used in a number of ways (e.g. doing exhaustive searches, or for generating reports ofattack statistics).

Types of Intrusion Detection System (IDS)

Host based IDS

This type of IDS monitors activity on the hosts making up the network. They are responsible for examining user activity. An example of host-based TDS is Psionic HostSentry (http://www.ypsionic.com/products/hostséntry.html), which is a system that performs LoginAnomaly Detection (LAD). HostSentry keeps a record of login time and location for each user as well as activity during each session and uses this information to spot intruders masquerading as legitimate users. Tripwire (http://www.tripwire.com/downloads), is another host-based system. It detects changes to file systems on the host it is monitoring by creating a unique fingerprint for each file and generating an alert wheneverthe file's signature changes.

Network Based IDS

Network-based intrusion detection system (NIDS) monitors traffic between hosts. It is concerned with the examination of the output of a packet sniffer. A sniffer is a program that reads raw packets off a network, usually after putting the network interface (e.g. ethernet card) into promiscuous mode. In promiscuous mode, the network interface will receive all traffic on the local network segment rather than packets addressed to it.

An example of network-based IDS is Snort (Interpol 2004). The following is taken from the Snort documentation: "Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP network. It can perform protocol analysis, content searching/matching and can be

used to detect a variety of attacks and probes'. Snort can defend a single machine or an entire network segment as it can put the network interface into promiscuous mode (James, 2002).

Distributed IDS

When host-based and network-based elements are both employed by some systems, they can be categorized as hybrid intrusion detection systems. An example of a hybrid intrusion detection system is the Distributed Intrusion Detection System (DIDS). This system has both a host monitor that performs host-based intrusion detection and a LAN monitor that analyses packets on the network.

With a fixed centralized host for intrusion detection analysis, there is a problem of higher power demand for the host if the network is enormous. This makes itimpractical for large networks. Instead (Paul, Matt & Marcus 2004) suggests that each host runs a process, called a *Cooperating Security Manager* (CSM), which analyzes the activity on that host. The individual CSMs share informationon users who are active on more than one host. Each CSM is made up of five components:

- The Local Intrusion Detection System component, which detects intrusions on the host on which the CSM is running.
- The Distributed Intrusion Detection component, which communicates with other CSMs on the network.
- The User Tracking System, which keeps a record, of which hosts a user is logged into.
- The Intruder Handling System component, which works out the best course of action once an intrusion, is detected.
- The User Interface component, which interacts with the security officer.

A "suspicion level" is produced for every user on the network indicating how likely it is that the user is acting maliciously. This is crucial, as it is difficult to determine who is or isn't acting improperly. This kind of IDS will be useful to very large networks.

Techniques of Intrusion Detection System

The types of IDSs (host-based, network-based and hybrid or distributed system) described above, make use of either misuse detection or anomaly detection to make a distinction between legitimate and malicious use of computer.

Anomaly Detection Technique

This technique assumes that all intrusive activities are essentially anomalous. This implies that ifwe could establish a "normal activity profile" for a system, we could in theory; flag all system states varying from the established profile. That is, it works by building a model to represent normal system usage and then monitoring for anything that does not fit this model. This approach is good at detecting new attacks that the misuse technique would miss. However, if we consider that the set of intrusive activities only intersects the set of anomalous activities instead of being exactly the same, we find a pair ofinteresting possibilities:

Anomalous activities that are not intrusive are flagged as intrusive (false positives). Intrusive activities that are not anomalous result in false negatives (events are not flagged intrusive, though they actually are). (John,Alan & Julia 2000).

The block diagram ofa typical anomaly detection system is shown in figure 2 below

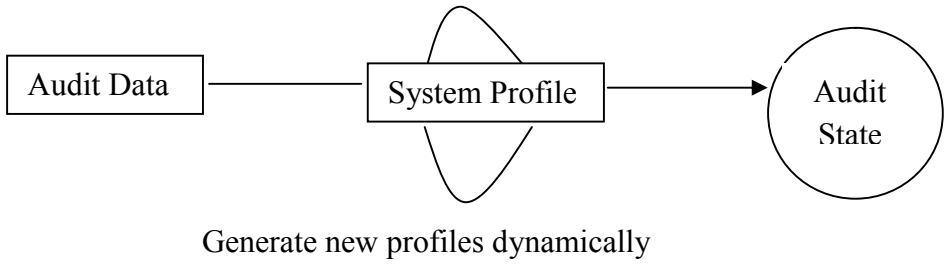

Figure 2: A Typical Anomaly Detection System

Thus, in anomaly detection systems, the main issues become the selection of threshold levels: so that neither of the above two problems become unreasonably magnified. and the selection of features to monitor.

These systems are relatively expensive, owing to the overhead of keeping track of, and possibly updating several system profile metrics. Some systems based on this technique are:

- Statistical Approaches, where behavior profiles for subjects are generated.
- Predictive Pattern Generation, which takes past events into account when analyzing the data.
- Neural Network, which predicts a user's next line of action or command, given the window of previous actions or commands.

Misuse Detection Technique

The misuse detection approach to intrusion detection is based on somehow defining what malicious behaviour is and then monitoring for it. The concept behind this scheme is that there are ways to represent attacks in the form of a pattern or signature so that even variations of the same attack can be detected. These systems are similar to virus detection systems- they can detect many or all known attack patterns, but they are of little use for as yet unknown attack methods. A crucial point to note is that anomaly detection systems try to detect the complement of "bad" behaviour. Misuse detection systems try to recognize known "bad" behaviour. The main issues in misuse detection systems are:

How to write a signature that encompasses all possible variations of the pertinent attack, and how to write signatures that do not also match the non-intrusive activity.

A typical misuse detection system is shown in figure 3 below

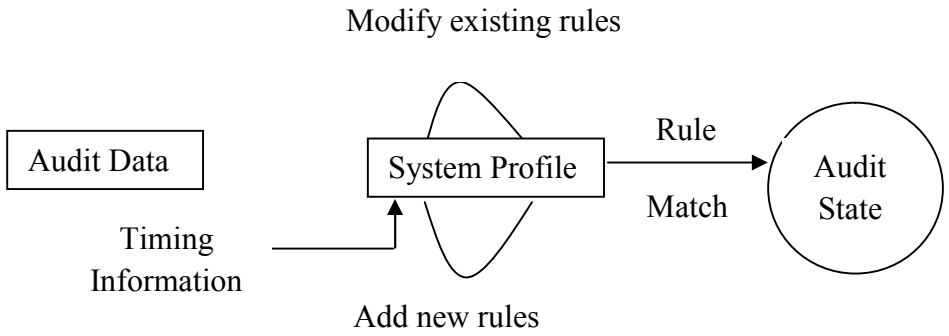

Figure 3: A Typical Misuse Detection System

There are a number of approaches to misuse detection.

- Expert Systems, separates the rule-matching phase from the action phase, with the matching done according to audit trail events.
- Keystroke Monitoring, system monitors keystrokes for attack patterns and is very simple in nature.
- Model Based Intrusion Detection, here certain scenarios are inferred by certain other discernible activities.
- Pattern Matching, encodes known intrusion signatures as patterns that are then matched against the audit data. It attempts to match incoming events to the patterns representing intrusion scenarios.

Conclusion

Irrespective of the type or techniques employed by an intrusion Detection System, it is serves to benefit us in the following ways:

- Most attacks come from inside, which cannot be prevented by the firewall systems. The Intrusion Detection Systems help to detect such attacks with appropriate measures to remove them.
- Firewalls sometimes even fail to protect against the external attacks. In such occasions, Intrusion Detection Systems serve as an alternative to detection of attacks or intrusions.

Although, intrusion detection technology is new (when compared to other security measures, such as firewall systems), it should notbe considered as a complete defense, in the field of network security, its role is indispensable in Internet security architecture. It is, therefore, recommended for the following reasons:

- Firewalls are not capable ofdetecting what happens behind them, that is, what goes on in the internal network.
- No one security measure is capable of completely combating the danger of insecurity in the network today, and as such, the intrusion detection systems would contribute their quota to strengthen the network security efforts.
- It is true that security issue is a very difficult topic of discussion. It means different things to different people. Defining what security means to your organization is the key to building a secure network. The activities going on the network are then evaluated based on this policy. The business of security is that of everyone. And it is only with the cooperation of everyone coupled with the necessary tools such as Intrusion Detection Systems, a formidable security could be built.

References

Interpol (2004).*IT Security and Crime Prevention Methods*. http://www.interpol.int/Public/TechnologyCrime/CrimePrev/lTSecurity.

James F. (2002). *Combination of Misuse andAnomaly Networkintrusion Detection Systems.* research@kaleton.com., http://www.kaleton.com.

John, M., Alan, C. and Julia A. (2000). Defending Yourself: The Role of Intrusion Detection Systems. IEEE Software. imchugh@cert.org.amc@sei.cmu.edu hilp://www.sei.cmu.edu/staff/amc/.jhw2isei.cmu._edu.

Martin A. and Markus C. (2003).*Intrusion Detection Systems Technologies, Weakness and Trends,*Stochholnm; Urwin

Paul, D. R., Matt, C. and Marcus J. R. (2004). Internet Firewalls: paul(dcompuwar.net cmcurtincinterhack.net, mjr@ranum.com.

Rebecca G. B. (1999). *Intrusion Detection.* London; Pearson Higher Education,

Adam M. Saliu; Mohammed B. Abdullahi; Mohathmed I. Kolo&Abdullahi R. Ozigi are Lecturers in the Department of Computer Science Federal University of Technology, Minna, Nigeria