Multi-Layer Intrusion Detection Systems
by Nathan Einwechter
last updated July 6, 2004

Introduction

A business critical system has been breached by attackers. Responding to the event, you grab your gear and head down to where the system is. En route a red faced executive seemingly about to explode brushes past you in a hurry, suddenly turning around upon realization that you are the specialist responding to the very incident which has him on the brink. Already knowing the words about to come out of his mouth, the man begins to spout, "We need this system back up immediately!! We have a major demonstration today and can NOT afford to allow this system to be down! FIX IT NOW!" Politely, you force out a yes sir, and head to the server room where the system is located. As you login, you know time is against you.

Does it take you one hour to get together and analyze the various system logs spread across the system, or do you do this same time consuming task in just a few minutes? That's your choice, and a choice that a multi-layer Intrusion Detection System (mIDS) gives you.

More often than not, single security solutions merely scratch the surface of an entire security event. This surface of information can be equated to the crust of the earth, which only makes up barely one percent of the earth's total mass. Analyzing just this small surface area of event information is not a sustainable approach to protecting networks. One must dig deeper, into the mantle, and even further into the core in order to truly begin to monitor and understand security events within computer systems and networks.

It is the mIDS technology which allows analysts to dig beyond the crust, and into the mantle, giving you, the analyst, a significantly better situational awareness and understanding. The second part of this series will take us further down and into the core, giving you an even better view of what is going on across a large number of systems.

This paper will discuss the basics of mIDS technology, why it is potentially beneficial to implement, who should implement it, and how it works. Much of this paper is to serve as a basis upon which to build the next paper in this series.

Overview of mIDS

What are multi-layer Intrusion Detection Systems?

A mIDS brings together many layers of technology into a single monitoring and analysis engine. These layers work their way up from integrity monitoring software such as TripWire, to system logs (i.e. syslog, all /var/log types, httpd logs, etc..), IDS logs, and firewall logs. All of these separate and distributed log types are aggregated into a single monitoring and analysis source for the specific computer on which the mIDS system is running.

The concept of aggregating logs is one of the most important ideas related to mIDS. When we aggregate logs, we are bringing various log files with different formats and from different locations into a single location with a single file format. By doing so, we create a single source of information which is clear, concise, and comprehensive.

This process creates a situation where the human-in-the-loop (the IT/IS people) are able to skip a number of system processes and cognitive processes to get to the data they need to get to and know. By aggregating and providing event linkage for the person monitoring/analyzing this information, we make it easier and much quicker for them to understand and conceptualize the large amounts of information which are all in different formats and have different meanings. This cognitive aid functionality allows those people who require the information most to operate faster and more efficiently within their working environments -- without losing the capability to monitor system security events to their full extent.

Why mIDS?

Now that we've determined what mIDS is, generally the next question arises as to why anyone should or would implement an mIDS, as well as who would best benefit from an mIDS type of system.

Increased situational awareness

mIDS puts people and organizations into a more secure position by allowing increased situational awareness and improved detection time. It is this increased situational awareness that pushes your security monitoring beyond the crust and into the mantle of awareness, bringing a whole new view and depth to your operations.

mIDS' format makes it possible to have a better understanding of what is truly happening during an incident than looking at a single log type or a number of distributed, but un-connected logs.

With only one source of intrusion information we only get one piece of the puzzle. Sometimes we only need this single piece of the puzzle to determine what is going on. More often than not, however, having corroborating evidence/information makes the situation significantly clearer and allows for a certain amount of re-assurance about what is believed to have happened (or be happening) versus what is actually the case.

The increased situational awareness provided by an mIDS system allows a system to maintain a secure position and ensure that any intrusions or attempted intrusions are detected immediately and thus dealt with faster (via shorter detection time).

Incident handling and analysis

This shortened detection time plays directly into the hands of the Incident Handler/Analyst. If an intrusion is to take place, then detection time is of the essence. There is a common Incident Handling Saying/Formula;

> **"Your systems can be considered secure if your protection time is greater than the sum of the detection time and reaction time" (Pt > Dt + Rt)**

Following this line of logic if you reduce the detection and reaction times to a specific incident, than your systems can be considered inherently more secure. mIDS allows the technological and techno-logistical detection time restrictions of conventional security monitoring to be overcome, thus providing better protection through reduced detection and reaction time. The system is able to overcome these restrictions by providing a single source of all security logs, and changing all information into a standard format.

The response time is also shortened with mIDS due to the fact that Incident Handlers are able to have immediate access to all related security logs without having to scrounge across a system for logs. The logs they do view, through the mIDS, are also pre-aggregated and ready to go for the Incident Handler, thus allowing him/her to skip a number of often timely steps within the process.

Although some people dispute the validity of the Pt > Dt + Rt formula, it is hard to dispute that reducing detection and reaction times is a positive thing for enhancing security.

Economic advantages

There are also a number of intrinsic economic advantages to using a mIDS for system security monitoring and analysis. It goes hand-in-hand with an decreased detection and reaction time that the systems downtime due to security events will also be minimized substantially. This decrease in consumed employee time and increase in system uptime mean real dollars to companies that depend on computer systems for their daily operations. This is a plus for all sides, and is vital to maintaining a sustainable security solution.

Companies that benefit the most economically from the implementation of mIDS type of technologies are those who depend on a small number of critical systems or servers for the daily operation of their business (i.e. e-business, ISPs, Web Providers, ASPs, ERM/ERP providers, etc.).

All in all, mIDS is best suited for small-to-medium sized businesses with a need to keep a small number (such as 1 - 10) of critical systems in a secure monitoring state while keeping wasted employee time to a minimum, without sacrificing the security monitoring depth/scope often associated with a reduced employee monitoring time.

Technology/mIDS Process Overview

mIDS is designed in such a way as to allow for any type of technologies to be integrated and implemented into the system and work with each other. There are only two limiting factors as to which technologies can be implemented within an mIDS system. The first is if the technology has proprietary logging methods which prevent a system from accessing and interpreting its log. Naturally if the system can not monitor these logs, than there is no hope to implement it into any type of realistic monitoring solutions of any kind. The second limiting factor is the creativity of the person who is putting together the mIDS, as well as the analysts who will be using it. Technology can be pushed as far as the creativity and ingenuity of the humans operating it can stretch. The more links and connections among technologies that the person designing and implementing the system can see, the better the results coming from the system will be.

Due to these limiting factors, and the custom design and flexible nature of mIDS, this section will cover the general processes involved within mIDS systems, but will not specify actual technologies or precisely how to design and implement such technology. The steps within the design are loosely based around a nine step intelligence information processing model, summarized here in four larger steps:

Step 1 - Measurement/Instrumentation
Monitoring software watches all user defined logs and obtains new log entries in real time as they are added to the logs

Alternatively, software can be setup to send this information to a central server for offline analysis. More about this will be covered in part two of this series, which discusses Multi-Layer Distributed IDS (mdIDS).

Step 2 - Representation and Encoding
All incoming data is converted into a standard format, encoded into storage. This stage is vital and the actual encoding of information is critical to the rest of the process. As such, extreme care in planning the encoding type must be taken while designing this stage, as it is one of the most important.

Step 3 - Discovering Relationships
During encoding, relationships among log events can be automatically generated by a pre-defined set of rules and conditions. These relationships are the key to allowing information to be aggregated at multiple levels, while providing a cognitive aid to analysts.

Step 4 - Alarm Engine
This is a rule based alarm engine which can use metrics from relationships discovery or specific occurrences within logs, as defined by user-created rules. Dynamic rule sets and model matching are also within the domain of this system, but are not likely to be implemented in mIDS.

Step 5 - Reporting
It isn't until this stage that the analyst actual begins to see any information. The reporting stage can consist of any number of technologies from simple displaying of aggregate reports on activity, to visualizations, shallow link analysis tools, or the results from the rule based alarm engine built into the system.

As always, these reports are accessible from a single location and in a single easy to understand aggregate format, thus increasing the ease of use and readability of these reports.

The true flexibility of the system can be seen by the range of possible technology implementations after the first two steps of the process are complete. Once Instrumentation/Measurement and Encoding and Representation have been completed, one can apply any number of statistical, ontological, rule engine based, or decision making technology. The options are really limitless. Should the first two steps be done correctly, then the possible technology which can report back to this system are also nearly limitless.

Conclusion

Implementation of an mIDS system can bring an organization's situational awareness over a small set of critical systems to a peak level while providing economic benefits and few shortcomings. Its overall design premise is relatively simple and can thus be implemented into any number of diverse situations easily and with little complication.

The mIDS design is, however, a mere stepping stone to a more powerful system with greater capabilities, functions, and applications. Although the design allows for increased situational awareness, total awareness is not gained through this system alone. It is within the next paper in this series that we will begin to discuss how to gain a total situational awareness of all sizes of networks, from small workgroups to large multi-national corporate networks that span the globe. Networks, after all, don't seem to be getting any smaller or less complex.

Related IDS articles

View more articles by Nathan Einwechter on SecurityFocus.