

Configuration of IPS using Event Analysis Data to improve the Performance and Incident Response Time

by: Ramesh Sripathy Rao and Elango Krishnasami, 08/31/2005

<http://www.securitydocs.com/library/3552>

Abstract

This paper discusses about advanced configuration of IPS to reflect the changing network topology using feedback from an event analysis tool. The events analyzed by incident response tool can be used to find out the false positives and the signatures required in the IPS. Using the analyzed event pool data, IPS can be dynamically configured to reduce the false positives, improve the incident response time and improve the performance by reducing the load on the IPS.

Introduction

Intrusion Prevention System (IPS) is the device that monitors the network traffic passing through it and takes the appropriate actions in accordance to the nature of the attack found in the network traffic.

IPS Management Software is used to manage the IPS devices in the large deployment. IPS Management Software widely has default/common set of configuration for the devices and have minimal configuration customized for each device.

Monitoring center is the application used to collect all the IPS events from various IPS devices and correlates the events using different methodologies.

Incident Response is a feature added in the newer generation of the IPS devices. Incident response does analysis on the events to find out whether the victim system is compromised for the attack. Based on the findings the event severity is upgraded or downgraded to prioritize the network-administering task for investigation.

IPS Configuration Issues

The sensor configurations are not changed dynamically to reflect the network dynamics and nature of network traffic. Unlike Humans, IPS systems are not ALIVE by nature since they don't understand what happens to their neighbors. IPS analyzes all the network traffic for the entire set of signatures loaded, even though the network is updated to address the threat for the applied signatures. Number of signatures is increasing day by day and doing analysis for the signatures, which are not required is an overhead on the device performance.

Upon detection of a threat, an alarm is sent to the monitoring application even though the host may not be vulnerable to that threat. Network administrator or incident response applications have to go through each alerts based on their priority to respond to the alerts. This leads to a situation where in, real attacks with lower priority/severity to be put in the analysis-queue and there by false positives get more priority during analysis just because they have default – high priority!

False Positives will be generated by IPS, when default configuration provided by the vendor is applied on the device, which in most cases will not fit for the unique network topology of the customers. This is because normal activity in one network might be an attack under certain circumstances for another network. False Positives will be generated by IPS even if configuration is created without enough knowledge on the network topology and applications running on the network.

These False Positives & improper configuration leads to two main issues in the IPS.

1. **Performance degradation on IPS** The performance of an IPS device doesn't cope up when the device is loaded with more number of signatures i.e. when applying all the signatures. All the network traffic is passing through the IPS

devices and are analyzed for signatures; hence the latency of the packets will increase when performance of IPS degrades. The performance of the device could be improved by removing unnecessary signatures dynamically based on the network dynamics.

2. **Increasing Incident Response Time** Each alert has to be analyzed by the network analyst to identify the real attacks based on the priority & severity of the alert generated. Increased number of false positives will result in delay of event analysis by the security analyst or by the analysis tool. The real attacks would be put in the queue if the false positives have higher severity than the real events.

Advanced Configuration of IPS

Security analyst can use Vulnerability Assessment (VA) tool to scan their network and identify the vulnerability in their network for configuring IPS. The issue with VA is, it's a resource consuming process and floods the network creating lots of noise; hence VA cannot be used frequently to learn the network topology. And also VA don't have direct mapping of the findings to the signatures in IPS.

Traditional way of fine-tuning IPS have always been dependent on Security Analysts researching the alarms and with the information gathered there after. What if we have a first hand tool, which does this analysis to some extent and then pass on the information to Security Analyst? Better still, if that first hand tool is integrated with the configuration module, automatic management based on network dynamics can be achieved!

The Event analysis tool can have the following information

Static Information

1. OS and Patch level Information about the hosts monitored by the IPS.
2. Information about applications running in the hosts and their versions.
3. Internal networks information
4. Key/Protected host information like web server, email server.

Dynamic Information

1. Downgraded alerts for a host
2. Upgraded alerts for a host
3. OS Information of a host
4. Application/OS/patch information of the hosts in the network

By making this information available to the management application for the devices, the management application could analyze the information, take the appropriate data to create configuration for individual devices, which will improve the performance of the device as well as reduce the incident response time.

Reducing Incident Response time and False Positives.

Every event is analyzed for incident confirmation by the event analysis tool or by the security analyst. The events are taken for analyses based on the severity or priority of the events.

When the network configuration is not reflecting the current topology, the IPS device will generate lot of false positives. The generated events might be having high severity hence resource is spent on analyzing these events even if they are not real events. Real attacks will not be addressed immediately due to large number of false positives events generated with high severity. By using the data from the analyzed events, the response time for the real attacks should be improved.

The Analyzed data from the Event Analysis Tool has the following information

1. OS information of the host.
2. Application versions running in the host.
3. Downgraded events and the reason for downgrade.
4. Upgraded events on confirmation on attack

If the signatures in an IPS are categorized by OS types, this categorization could be used in the management console for fine-tuning the IPS. When an attack is detected to a host, which belongs to different OS type, the event will be downgraded after analysis by the event analysis tool. Management Console can pick the OS information from the event data for all the available hosts. This information can be used to exclude the host from the signatures that belongs to different OS types.

If a Windows attack is seen in a range of hosts, which are running linux then these hosts, can be added to the excluded list for the windows related attacks. IPS will not trigger alert if it sees a windows attack for these hosts added in the excluded list.

The attack could be treated as false positive, when the attack to an application is patched. The downgraded events will be having the information of the application, which is patched for those signatures. Using this information, the host can be excluded from IPS analysis for that particular attack type.

A Signature could be considered harmless, if a particular alert is continuously getting downgraded. Those signatures can be downgraded on the severity. This will help the real attacks to get higher precedence and addressed sooner.

When events are continuously getting upgraded for a particular signature, it means the network is vulnerable. These types of events should be given higher priority for faster mitigation. Doing so will make sure to have faster response. The attack can be stopped by adding actions such as blocking or dropping the packets to the event if the host is identified to be vulnerable.

Excluding the hosts from the signatures reduces the false positives and also reduces load the event analysis tool or security analysts. This will improve the response time for events because reduced load by reducing the events.

Reducing or increasing the severity/priority of the events, will give the lower or higher precedence for the events for analysis. By making the vulnerable hosts to have higher precedence, the events will be addressed faster and giving lower precedence to the events to the hosts, which are less harm in nature, will give space for addressing real events faster.

These techniques improve the response time and increase the probability of the addressing the real attacks. All these information will have threshold time value, so the configuration will be regenerated based on the data available on the analyzed events in a regular fashion based on a time interval. The configuration are updated based on the events generated on the network, hence the system itself fine tunes the configuration.

Improving performance of IPS

The management application make use of the data available on the monitoring/Event Analysis tool to find out the signatures which are not occurring in the network and signatures which are not required to be monitored.

The Analyzed data has the information of

1. Events summary in the database over a period of time.
2. Internal networks information
3. Key host information

Management application can remove signatures that are not occurring in the sensor-monitored network. This would avoid the false positives being generated from the device and reduces the load on the device to reduce. The signatures, which are not required, can be found by analyzing the downgraded events.

Signatures are usually grouped by different categories such as OS, service, etc... If no events found in a category of signature

over a period of time say a month, Management application safely assume there is no immediate vulnerability in that category of the attacks. The signatures having low severity, which belongs to this category, can be safely ignored. i.e. can be removed from the device while creating configuration for the devices. Also the signatures having high severity and belongs to this category can be downgraded on the severity by the management application.

When the analysis tools downgrades a signature event continuously for all the victims over a period of time, Management application can assume this signature is not required and might generate false positives, hence the signatures, which are downgraded continuously for all the victims, can be removed from the configuration generated to the device.

However risk of removing signature is that, the device cannot find the attack directed to a host added to the network with this vulnerability. But the risk is very low because the dynamic configuration removes only the low severity signatures configured by the users, which are not serious and not seen for this network. Also the risk can be mitigated by adding the removed signatures, when ever an attack seen in the same category of the signature i.e. when any attack seen in the enabled signatures.

The management station can do removal of signatures automatically during regeneration of a configuration with the data it learned from event analysis tool. Or a manual procedure could be introduced so that it goes through Security Analyst's eyes before actually removing it.

Conclusion

The Configurations can be created dynamically based on the information available on the events and the analyzed events. This dynamic configuration will be fine-tuned itself during a period of time.

The dynamic configuration improves the performance of the IPS device by removing the signatures for which the hosts are not vulnerable.

The incident response time could be improved by reducing the event generation from the IPS device in the way of excluding events for the hosts for which the signatures are not applicable and by reducing the event severity for the signatures the hosts is not vulnerable.