COMPARISON OFINTRUSION DETECTION AND PREVENTION SYSTEMS USING DATA MINING

Prof. Raghavendrarao B[1], Prof. Vinita Tapaskar[2]
[1]Assistant Professor, Sri Sairam College Of Engineering
[2]Assistant Professor,The Oxford College of Science

Abstract:The security of our computer systems and data is at tremendous risk. The high growth of the Internet led to the increasing availability of tools and tricks for intruding and attacking networks have provoked intrusion detection and prevention to become a critical component of networked systems. This paper aims to provide a detailed comparison between intrusion detection and prevention system latest tools in Data Mining.

Keywords:Network, Data Mining, IDS, IPS, Intruder, Types of Attacks.

I] Introduction:

An intrusion can be represented as any set of services that attack the integrity, confidentiality, or accessibility of a network resource for example user accounts, file systems, kernels, etc. In other way unauthorizedaccess by an intruder involves stealing valuable resources and misuses those resources, e.g. Worms and viruses. There are intrusion prevention tools and techniques for user authentication, and sharing encrypted information that is not enough to operate because the system is becoming more difficult day by day so, we need a layer of security controls.

The term 'Intruder' is an entity that is trying to gain unauthorized access over a system or a network. However, the data present in the system will be corrupted along with an inequality in the environment of that network.

Intruders are of majorly two types

1. (Outside Intruder) buiten Intruder
   – No authority to use the network or system
2. (Inside Intruder) binnen Intruder
   – Authorized access to limited applications

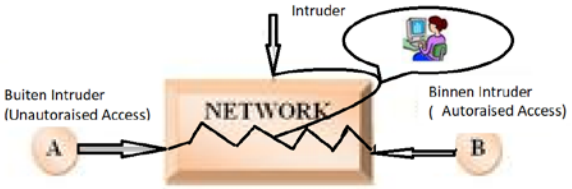

Figure 1: Intruders in a network

From Figure 1, an Intrusion Detection System (IDS) is a device or application that identifies anomalous behavior, monitors traffic, and reports its findings to an administrator, but it cannot prevent it. The system ensures the confidentiality, integrity, and availability of data and information systems in the face of online threats. We can see how the dangers and chances for hostile attacks increase as the network increases.

The following are the most common types of attacks identified by intrusion detection systems:

- Scanning attacks
- Denial of service (DOS) attacks
- Penetration attacks

The generic architecture[5] of IDS is given below:

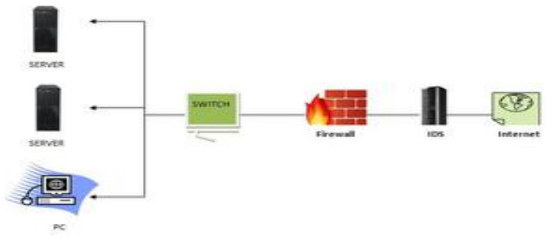

Figure2: Architecture of an IDS

In Figure 2 a single tire is the one in which components in an IDS collect and process data themselves, rather than passing the output they collect to another set of components. A host-based intrusion-detection tool that uses system logs as input is an example. On Unix systems,

for example, the utmp and wtmp files. Also, it compares it to known attack patterns..

A single tier has advantages, such as simplicity, low cost, and independence from other components. At the same time, however, a single tiered architecturehas components that are not aware of each other in reducing considerably the potential for efficiency and sophisticated functionality of the system.

II] Detection Methodsused by IDS & IPS

It is basically an extension of the Intrusion Detection System (IDS)[6] that can safeguard the system from suspicious activities, viruses, and threats. Once any undesirable behavior is detected, the IPS takes action against it, such as closing access points and disabling firewalls.

There are two ways majority of intrusion detection and prevention systems use either signature-based detection or anomaly-based detection.

1. Signature-Based: The signature-based system employs a library of known attack signatures, and if the signature matches the pattern, the system detects the intrusion and takes action to prevent it by banning the IP address or deactivating the user account's ability to access the application. This system is a pattern-based system that monitors network packets and compares them to a database of signatures from previous attacks or a list of attack patterns. If the signature matches the pattern, the system detects the intrusion and sends an alert to the administrator.E.g.Antiviruses.

Pros:

- Worth detecting only Known attacks.

Cons:

- Failed to identify new or unknown attacks.
- Frequent updates of new attacks.

2. Anomaly-based: This system views for unusual behavior. If any intrusion activity is identified, the system immediately disables access to the targeted host. This system follows a baseline pattern, in which we first train the system with a good baseline and then compare behavior to it. When someone goes above or below that threshold, it's regarded suspicious activity, and the administrator receives an alert.

Pros:

- Ability to detect unknown attacks.

Cons:

- Higher complexity, sometimes it is difficult to detect and chances of false alarms.

As we all know, data mining is the process of extracting patterns from large datasets using a combination of statistical artificial intelligence and database management approaches. We recall a few things in intrusion detection (ID) and intrusion prevention device (IPS) that could be useful in data mining for intrusion detection systems (IDS) and intrusion prevention devices (IPS).

III] How Data Mining helps in Intrusion detection and prevention system.

- Using data mining algorithms for developing a new model for IDS:

Data mining[4] algorithm for the IDS model having a higher efficiency rate and lower false alarms.

Both signature-based and anomaly-based detection techniques can be employed with data mining algorithms. Training data is classed as either "normal" or "intrusion" in signature-based detection. After that, a classifier can be created to find known invasions. Clarification algorithms, association rule mining, and cost-sensitive modelling have all been studied in this area. Anomaly-based total detection creates models of typical behaviour and discovers huge departures from it automatically. Clustering, outlier analysis, and class algorithms software, as well as statistical methodologies, are examples of methods. The solutions employed must be efficient and scalable, as well as capable of coping with large amounts of complex and heterogeneous community data.

- Analysis of Stream data:

This mean analyzing the data in a continuous manner nevertheless data mining is mainly used on static data fairly than Runningdata due to complex calculation and high processing time. Due to the dynamic nature of intrusions and malicious attacks, it is more critical to perform intrusion detection withinside the records stream environment. Moreover, this event can be regular on its own but taken into consideration malicious if regarded as a part of a series of activities must be considered. Thus, it’s very important to look at what sequences of activities are regularly encountered together, locate sequential patterns, and pick out outliers.

Other data mining schemes for detecting evolving clusters and constructing dynamic class models in records streams also are essential for real-time intrusion detection.

- Distributed data mining:

It is used to study the random data which is integrally distributed into various databases so, it becomes difficult to integrate processing of the data. Intrusions may be started from numerous distinctive places and focused on many different destinations. Distributed data mining methods can be used to find community data from numerous network places to detect those distributed attacks.

- Visualization tools:

These tools are used to display the data in the form of graphs which helps the user to get a visual effect of the data. These tools are also used for viewing any abnormal patterns detected. Such tools may include capabilities for viewing associations, discriminative patterns, clusters, and outliers. Intrusion detection systems must include a graphical user interface that allows security analysts to ask questions about network data or intrusion detection results.

IV] **Comparison of IPS with IDS:**

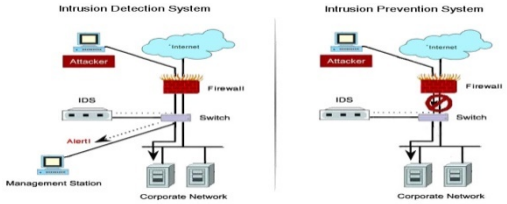

Figure3: Comparison of IDS and IPS

From the above Figure3 we have the main difference between [1]Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) are:

- Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
- IPS can take actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
- IPS also can correct cyclic redundancy check (CRC) errors, defragment packet streams, mitigate TCP sequencing issues and clean up unwanted transport and network layer options.

The basic function of IDS[2] is monitoring the traffic of a network to detect any intrusion attempts being made by unauthorized people.

- Observing the operation of files, routers, key management servers, and firewalls that are required by additional security control and these are the controls that help to identify, prevent, and recover from cyberattacks.
- We should allow non-technical staff to manage system security by providing aeasy interface.
- Allow administrators to bend, organize, and understand the key audit trails and other logs of operating systems that are generally hard to separate and keep track of.
- Stopping the intruders or the server to respond to an attempted intrusion.
- Informing the administrator that the network security has been breached.
- Noticing altered data files and reporting them.
- Givinganwide database of attack signature with which the information from the system can be matched.

Benefits of IDS:

1. IDS software provides you with the ability to detect unusual or potentially malicious activity in the network.
2. IDS at any organization are equipping the relevant people with the ability to analyze not only the number of attempted cyber-attacks occurring in your network but also their types. This will provide any organization with the required information to implement better controls or change existing security systems.
3. Detecting problems or bugs within any network device configurations. This will help in better assessing future risks.
4. Attaining regulatory compliance. It is easier to meet security regulations with IDS as it provides any organization with greater visibility across networks.
5. Improving security response. IDS sensors allow you to assess data within the network packets as they are designed to identify network hosts and devices. Additionally, they can detect the operating systems of the services being used.

Intrusion prevention systems (IPS) are extensions to intrusion detection systems. IPSs

act once suspicious activity has been identified. So, there may already have been some damage done to the integrity of your system by the time the intrusion has been spotted.

The IPS is able to perform actions to shut down the threat. These actions include:

- Restoring log files from storage
- Suspending user accounts
- Blocking IP addresses
- Killing processes
- Shutting down systems
- Starting up processes
- Updating firewall settings
- Alerting, recording, and reporting suspicious activities

The responsibility of admin tasks that make many of these actions possible is not always clear. For example, the security of log files with encryption and the backing up of log files so that they can be restored after tampering are two threat protection activities that are usually defined as intrusion detection system tasks.

V] Comparison of tools used for IDS and IPS[3]:

Table1: Comparison of tools

Slno	Tool used	Controls access to	IPS /IDS functions	Platform
1	Solar Winds Security Event Manager	log files, live data.	Event Manager	Windows server, Unix, Linux
2	Datadog's	Network and device monitoring, applications monitoring, and web performance monitoring.	Real-time Threat Monitoring	cloud-based service
3	Splunk &Splunk Cloud	network traffic and on log files	Enterprise and Cloud editions	Windows, Linux& SaaS
4	Sagan	log files	event messages	Unix, Linux, and Mac OS
5	OSSEC (Open Source HIDS Security)	log files	policies	Unix, Linux, Mac OS, and Windows
6	Open WIPS-NG	wireless systems	a wireless packet sniffer	Linux
7	Fail2Ban	log files	an IP address ban	Unix, Linux, and Mac OS.
8	Zeek (Bro)	signatures across network packets	network-based intrusion detection methods	Unix, Linux, and Mac OS.

Conclusion:

The Comparative study says that there are lot of tools available for intrusion detection and prevention system with respect to network and some tools are used in specific platform and uses different control structures. With increase in use of Cloud infrastructure the more effective IPS and IDS systems are required.

REFERENCES

[1] Korcak, Michal & Lamer, Jaroslav &Jakab, Frantisek. (2014). "Intrusion Prevention/Intrusion Detection System (IPS/IDS) for Wi-Fi Networks". International journal of Computer Networks & Communications. 6. 77-89. 10.5121/ijcnc.2014.6407.

[2] Abdelkarim, Amjad & H. O. Nasereddin, Hebah.(2011).Intrusion Prevention System. International Journal Of Academic Research. 3. 432-434.

[3] Biswas, Saroj. (2018). Intrusion Detection Using Machine Learning: A Comparison Study. International Journal of Pure and Applied Mathematics. 118. 101-114.

[4] Zibusiso Dewa and Leandros A. Maglaras , Data Mining and Intrusion Detection Systems (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 1, 2016

[5] Tiwari, Mohit& Kumar, Raj & Bharti, Akash &Kishan, Jai. (2017). INTRUSION DETECTION SYSTEM. International Journal of Technical Research and Applications. 5. 2320-8163.

[6] Mudzingwa, David & Agrawal, Rajeev. (2012). A study of methodologies used in intrusion detection and prevention system (IDPS). Proceedings of IEEE Southeastcon. 1 - 6. 10.1109/SECon.2012.6197080.