ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 9, Issue 4, pp: (1-3), Month: October - December 2021, Available at: www.researchpublish.com

# INTRUSION PREVENTION SYSTEM

Hanan A Aldossary[1]

[1,2]Affiliation None

[1,2]Saudi Aramco, Dhahran, Saudi Arabia

***Abstract:*** **The Internet has opened the door to virtually unlimited opportunities for individuals to do business, share ideas, and connect with others. However, these same technologies have also led to the rise of cybercriminals who are rapidly gaining power. A common cybercrime is identity theft which can take many forms. These crimes are becoming more prevalent because they offer easy to use tools that can steal data without much risk or effort for the criminal .This research paper defines the needs of intrusion prevention system (IPS) in order to prevent internet crime. Also, it represents the ways to enhance the network security by using intrusion prevention systems. The paper also discussed how to protect the network from attacks and threats by using intrusion prevention system (IPS).**

***Keywords:*** **Cybercriminals, Intrusion Prevention Systems, antivirus, Hackers, Signatures and Behavior-based signatures.**

## I. INTRODUCTION

Scientific evidence has shown that intrusion prevention systems (IPS) can function as a valuable element of a strong network defense. It will help prevent IP spoofing, denial-of-service attacks, port scanning for vulnerabilities, or unauthorized access to sensitive data stored on network servers, caused by intruders who detect security loopholes in networks.

Today's, IPSs are used by all sizes of organization to protect their sensitive data. The goal of any IPS is to allow legitimate traffic through while blocking all unauthorized traffic.

IPS can also analyze the data stream inline, before it is sent to the destination, which is an attractive feature for organizations that do not want to slow down their networks or otherwise impact their users' experience. However, everything that comes into a network will need to pass through an IPS for inspection before it reaches its intended destination.

There are many different types of intrusion prevention systems (IPSs) and they range from those that can be used with a large-scale corporate network to ones that can be installed and used within the enterprise itself.

## II. LITERATURE REVIEW

### *A. Intrusion Prevention System*

You've just finished a long day of work and you're finally able to relax for the first time all week. But as soon as you boot up your computer, it starts beeping. You realize your computer is trying to warn you that it has been hacked by an Intrusion Prevention System (IPS). Before we get into what happens after this intrusion, let's first learn about IPS itself.

An IPS is a system that uses a combination of signatures and signatures based on behavior to detect an intrusion before it can be executed or if it has been executed, to slow it down. It's a security device, typically installed at the edge of a network, that monitors network activity and prevents unauthorized users from entering it. IPSs are similar to firewalls but they operate on or before the application layer of networks, rather than the network layer. They are primarily designed to prevent attacks against endpoints by filtering traffic so only authorized traffic can pass through.

Hackers often try to break into a system in the same way they use in a business environment. By making sure they follow a certain pattern or by using known vulnerabilities, security systems can detect when hackers are trying to gain access.

Intrusion Prevention Systems are designed to prevent the hacker from being successful in his attempt. It is this method of detection that has become one of the most widely used in business environments today.

***B. The Intrusion Prevention Systems are important***

An IPS is an important security measure because it can detect when a user or a hacker is trying to break into a system. Because of this, IPSs can be used in conjunction with antivirus software to keep your system safe at all times.

In many organizations, an Intrusion Prevention System is designed to detect known breaches before they can occur. During a breach, hackers typically try to get a certain way into a system. If an IPS detects a suspicious pattern or behavior it can prevent the breach from occurring.

***C. What do Intrusion Prevention Systems do and how it works?***

An Intrusion Prevention System monitors all the traffic coming in and out of a system. It intercepts any traffic that does not follow the correct pattern and filters out anything that does not fit within standard network patterns.

Through this filtering, an Intrusion Prevention System can stop a hacker from gaining access to your system. An Intrusion Prevention System uses a combination of predefined network patterns and behavioral analysis to detect known intrusions before they occur.

IPSs primarily function through the use of signatures and behavior-based signatures. After creating a signature, the IPS creates a set of rules for future events based on those signatures. These rules are constantly compared to actual events in an attempt to detect when something is wrong with the patterns.

The IPS compares the signatures against traffic that is actually coming into your system or an event that happens after your system is already compromised. This gives the IPS enough information to determine if the intrusion has occurred and what has happened. Once an intrusion is detected, the IPS can prevent further access by using a combination of filters and rules to block out unwanted traffic.

***D. Intrusion Prevention System prevent breaches***

An Intrusion Prevention System can be used for many security purposes. Because of the nature of the IPS, they are most commonly designed to detect and prevent an intrusion from occurring in the first place. Many IPSs are designed with a predefined set of rules or signatures that identify any known security issue and will automatically block out any actions associated with them. Because of this, an IPS can often detect and prevent cyberattacks before they occur.

IPSs are designed to act as a line of defense for your system. Without an IPS, an antivirus wouldn't be able to detect intrusions before they occurred. This is because the antivirus relies on signatures and behavior-based signatures created by an IPS to detect malware.

An Intrusion Prevention System can modify the normal event log on a system and notify security personnel if certain events occur. IPSs can also provide advanced network analysis for advanced system performance monitoring and real-time threat detection.

Many organizations use an Intrusion Prevention System to monitor network traffic and analyze all the information coming into a computer or computer system. IPSs are commonly used in conjunction with antivirus software because antivirus software cannot function without them. The reason IPSs are needed in conjunction with an antivirus is because each of their methods of detection are designed to work together to prevent security breaches.

***E. Types of Intrusion Prevention Systems***

There are four different types of IPSs available today. They include signature-based, behavioral-based, anomaly-based, and combined.

Signature-based systems are the most commonly used because of their ability to detect all types of malware already created. Signature-based IPSs are designed with a signature that is constantly updated as new malware is discovered.

Behavioral-based systems are used by many different security companies because they are designed to detect events on your system before the actual intrusion occurs. Behavior-based IPSs are designed to detect when an application is interacting with the system in a way that is not normal for that application.

Anomaly-based systems are much like behavioral-based IPSs because they take into account the data collected to identify unusual behavior. Anomaly-based IPSs do not rely on signature data, they instead use unique event logs created by the IPS to identify anything out of the ordinary.

Combined systems are powered by two separate Intrusion Prevention Systems. The combined system uses the same type of IPS, but monitors two separate networks. The reason for monitoring two networks is to determine if an intruder has breached one network and attempting to gain access to another.

## III. CONCLUSION

If you are looking for the best Intrusion Prevention Systems, you will want to stick with vendors that develop their own security software. This is because each vendor will customize their own computer program in order to match your needs better.

You will also want to make sure that you find a vendor that can provide security software for both your business and home networks. Most vendors will provide three different programs such as Antivirus, Anti-spyware, and Internet Security. If they do not, you should look elsewhere.

Look for a company that has been in business for at least ten years and offers 24/7 security monitoring. You want to make sure the company is reachable if their software does not work as expected. Many companies offer a free trial in order to see if their program is suitable for your needs.

You may also want to look for a company that offers Custom IPS Service because it will make the installation process much easier. The custom IPS service allows you to select all of the features and functions that you want included in their product. This is very important because you know the software is exactly what you need and nothing more.

## REFERENCES

[1] Desai, Neil. Intrusion Prevention Systems: The Next Step in the Evolution of IDS. Accessed on January 1, 2010. Available at http://www.securityfocus.com/infocus/1670