Intrusion Prevention System (IPS)

Last Updated : 14 Mar, 2023

Intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. Major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it and attempt to block or stop it.

Intrusion prevention systems are contemplated as augmentation of Intrusion Detection Systems (IDS) because both IPS and IDS operate network traffic and system activities for malicious activity.

IPS typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IPS can also respond to a detected threat by attempting to prevent it from succeeding. They use various response techniques, which involve the IPS stopping the attack itself, changing the security environment or changing the attack's content.

How Does an IPS Work?

An IPS works by analyzing network traffic in real-time and comparing it against known attack patterns and signatures. When the system detects suspicious traffic, it blocks it from entering the network.

Types of IPS

There are two main types of IPS:

1. **Network-Based IPS:** A Network-Based IPS is installed at the network perimeter and monitors all traffic that enters and exits the network.

2. **Host-Based IPS:** A Host-Based IPS is installed on individual hosts and monitors the traffic that goes in and out of that host.

Why Do You Need an IPS?

An IPS is an essential tool for network security. Here are some reasons why:

- Protection Against Known and Unknown Threats: An IPS can block known threats and also detect and block unknown threats that haven't been seen before.
- Real-Time Protection: An IPS can detect and block malicious traffic in real-time, preventing attacks from doing any damage.
- Compliance Requirements: Many industries have regulations that require the use of an IPS to protect sensitive information and prevent data breaches.
- Cost-Effective: An IPS is a cost-effective way to protect your network compared to the cost of dealing with the aftermath of a security breach.
- Increased Network Visibility: An IPS provides increased network visibility, allowing you to see what's happening on your network and identify potential security risks.

  Classification of Intrusion Prevention System (IPS):
  Intrusion Prevention System (IPS) is classified into 4 types:

1. **Network-based intrusion prevention system (NIPS):**
   It monitors the entire network for suspicious traffic by analyzing protocol activity.

2. **Wireless intrusion prevention system (WIPS):**
   It monitors a wireless network for suspicious traffic by analyzing wireless networking protocols.

3. **Network behavior analysis (NBA):**
   It examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service attacks, specific forms of malware and policy violations.

4. **Host-based intrusion prevention system (HIPS):**
   It is an inbuilt software package which operates a single host for doubtful

activity by scanning events that occur within that host.

Comparison of Intrusion Prevention System (IPS) Technologies:
The Table below indicates various kinds of IPS Technologies:

IPS Technology Type	Types of Malicious Activity Detected	Scope per Sensor	Strengths
Network-Based	Network, transport, and application TCP/IP layer activity	Multiple network subnets and groups of hosts	Only IDPS which can analyze the widest range of application protocols;
Wireless	Wireless protocol activity; unauthorized wireless local area networks (WLAN) in use	Multiple WLANs and groups of wireless clients	Only IDPS able to predict wireless protocol activity
NBA	Network, transport, and application TCP/IP layer activity that causes anomalous network flows	Multiple network subnets and groups of hosts	Typically more effective than the others at identifying reconnaissance scanning and DoS attacks, and at reconstructing major malware infections
Host-Based	Host application and operating system	Individual host	Can analyze activity that was transferred in end-to-end

	(OS) activity; network, transport, and application TCP/IP layer activity		encrypted communications

Detection Method of Intrusion Prevention System (IPS):

1. **Signature-based detection:**
   Signature-based IDS operates packets in the network and compares with pre-built and preordained attack patterns known as signatures.

2. **Statistical anomaly-based detection:**
   Anomaly based IDS monitors network traffic and compares it against an established baseline. The baseline will identify what is normal for that network and what protocols are used. However, It may raise a false alarm if the baselines are not intelligently configured.

3. **Stateful protocol analysis detection:**
   This IDS method recognizes divergence of protocols stated by comparing observed events with pre-built profiles of generally accepted definitions of not harmful activity.

Comparison of IPS with IDS:

The main difference between Intrusion Prevention System (IPS) with Intrusion Detection Systems (IDS) are:

1. Intrusion prevention systems are placed in-line and are able to actively prevent or block intrusions that are detected.
2. IPS can take such actions as sending an alarm, dropping detected malicious packets, resetting a connection or blocking traffic from the offending IP address.
3. 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.

Conclusion:

An Intrusion Prevention System (IPS) is a crucial component of any network security strategy. It monitors network traffic in real-time, compares it against known attack patterns and signatures, and blocks any malicious activity or traffic that violates network policies. An IPS is an essential tool for protecting against known and unknown threats, complying with industry regulations, and increasing network visibility. Consider implementing an IPS to protect your network and prevent security breaches.

Comment More info

Next Article

Difference Between Symmetric and Asymmetric Key Encryption

Similar Reads

Approaches to Intrusion Detection and Prevention

Prerequisites - Intrusion Detection System (IDS)Intrusion Prevention System (IPS) IDS stands for Intrusion Detection System (IDS). It is device or software...

6 min read

Intrusion Detection System (IDS)

An Intrusion Detection System (IDS) is a security tool that monitors a computer network or systems for malicious activities or policy violations. It helps detect...

10 min read

Port Address Translation (PAT) mapping to Private IPs

In this article we will be learning how exactly a Home network works. In the beginning we should keep in mind that when we connect our Laptops, Smart...

4 min read

Pharming Attack Prevention and Examples

The term “Pharming” is a combinative word formed using farming and phishing. Pharming is a way of online fraud by cybercriminals that install some malicious...