INTRUSION DETECTION SYSTEMS (IDS) AND INTRUSION PREVENTION SYSTEMS (IPS) FOR NETWORK SECURITY: A CRITICAL ANALYSIS

Sandeep Singh*

ABSTRACT

This paper analyzes and criticizes the ways of functioning of IDS and IPS. Understanding the similarity of characteristics of IDS and IPS may be useful in making decisions regarding their use in Organizational Computer Network. To deploy IDS or IPS we need to understand the types of IDS and IPS and the way they operate when an attack is launched. Intrusion Prevention Systems can be Host based (HIPS) and Network Based (NIPS). Finally, knowledge of Signature and Signature alarms will make the administrative tasks easier.

Keywords: *Intrusion detection system, IDS, Intrusion prevention system, IPS, Signature, signature micro-engines, signature alarms, Host based IPS, HIPS, Network based IPS, NIPS, Network Security*

***Student, M. Tech. (I.T.),**

Intrusion detection system (IDS) and intrusion prevention system (IPS) solutions form an integral part of a robust network defense solution. Maintaining secure network services is a key requirement of a profitable IP-based business.

INTRODUCTION TO IDS AND IPS:-

IDS and IPS work together to provide a network security solution. An IDS captures packets in real time, processes them and can respond to threats, but works on copies of data traffic to detect suspicious activity by using signatures. This is called promiscuous mode. In the process of detecting malicious traffic, an IDS allows some malicious traffic to pass before the IDS can respond to protect the network. An IDS analyzes a copy of the monitored traffic rather than the actual forwarded packet. The advantage of operating on a copy of the traffic is that the IDS does not affect the packet flow of the forwarded traffic. The disadvantage of operating on a copy of the traffic is that the IDS cannot stop malicious traffic from single-packet attacks from reaching the target system before the IDS can apply a response to stop the attack. An IDS often requires assistance from other networking devices, such as routers and firewalls, to respond to an attack.

An IPS works inline in the data stream to provide protection from malicious attacks in real time. This is called inline mode. Unlike an IDS, an IPS does not allow packets to enter the trusted side of the network. An IPS monitors traffic at Layer 3 and Layer 4 to ensure that their headers, states and so on are those specified in the protocol suite. However, the IPS sensor analyzes at Layer 2 to Layer 7 the payload of the packets for more sophisticated embedded attacks that might include malicious data. This deeper analysis lets the IPS identify, stop and block attacks that would normally pass through a traditional firewall device. When a packet comes in through an interface on an IPS, that packet is not sent to the outbound or trusted interface until the packet has been determined to be clean.
An IPS builds upon previous IDS technology.

IDS AND IPS TECHNOLOGIES SHARE SEVERAL CHARACTERISTICS:-

❖ IDS and IPS technologies are deployed as sensors. An IDS or an IPS sensor can be any of the following devices:

- A router configured with IPS software
- An appliance specifically designed to provide dedicated IDS or IPS services
- A network module installed in an adaptive security appliance, switch or router

❖ IDS and IPS technologies typically monitor for malicious activities in two spots:

- Malicious activity is monitored at the network to detect attacks against a network, including attacks against hosts and devices, using network IDS and network IPS.
- Malicious activity is monitored on a host to detect attacks that are launched from or on target machines, using host intrusion prevention system (HIPS). Host based attacks are detected by reading security event logs, checking for changes to critical system files, and checking system registries for malicious entries.

❖ IDS and IPS technologies generally use signatures to detect patterns of misuse in network traffic. A signature is a set of rules that an IDS or IPS uses to detect typical intrusive activity. Signatures are usually chosen from a broad cross section of intrusion detection signatures and can detect severe breaches of security, common network attacks and information gathering.

❖ IDS and IPS technologies look for the following general patterns of misuse:

- **Atomic pattern:** In an atomic pattern, an attempt is made to access a specific port on a specific host, for any malicious content contained in a single packet. An IDS is particularly vulnerable to an atomic attack because until it finds the attack, malicious single packets are being allowed into the network. An IPS prevents these packets from entering at all.
- **Composite pattern:** A composite pattern is a sequence of operations distributed across multiple hosts over an arbitrary period of time.

Steps that occur when an attack is launched in an environment monitored by an IDS:

Step 1. An attack is launched on a network that has a sensor deployed in IDS mode.

Step 2. The switch sends copies of all packets to the IDS sensor (Configured in promiscuous mode) to analyze the packets. At the same time, the target machine experiences the malicious attack.

Step 3. The IDS sensor, using a signature, matches the malicious traffic to the signature.

Step 4. The IDS sensor, sends the switch a command to deny access to the malicious traffic.

Step 5. The IDS sends an alarm to a management console for logging and other management purposes.

Steps that occur when an attack is launched in an environment monitored by an IPS:

Step 1. An attack is launched on a network that has a sensor deployed in IPS mode (configured in inline mode)

Step 2. The IPS sensor analyzes the packets as soon as they come into the IPS sensor interface. The IPS sensor, using signatures, matches the malicious traffic to the signature and the attack is stopped immediately. Traffic in violation of policy can be dropped by an IPS sensor.

Step 3. The IPS sensor can send an alarm to a management console for logging and other management purposes.

TYPES OF IDS AND IPS SYSTEMS:-

1. Signature-Based IDS/IPS Systems:

A signature-based IDS or IPS sensor looks for specific, predefined patterns (signatures) in network traffic. It compares the network traffic to a database of known attacks, and triggers an alarm or prevents communication if a match is found. The signature can be based on a single packet or a sequence of packets. New attacks that do not match a signature do not result in detection. For this reason, the signature database needs to be constantly updated.

Signature-based pattern matching is an approach that is rigid but simple to employ. In most cases, the pattern is matched against only if the suspect packet is associated with a particular service or, more precisely, destined to and from a particular port. This matching technique helps to lessen the amount of inspection done on every packet. However, it makes it more difficult for systems to deal with protocols that do not reside on well-defined ports, such as Trojan horses and their associated traffic, which can move at will.

At the initial stage of incorporating signature-based IDS or IPS, before the signatures are tuned, there can be many false positives (traffic generating alert which is not threat for the network). After the system is tuned and adjusted to specific network parameters, there will be fewer false positives than with the policy-based approach.

2. Policy-Based IDS/IPS Systems:

In policy-based systems, the IDS or IPS sensor is preconfigured based on the network security policy. The policies used in a policy-based IDS or IPS must be created. Any traffic detected outside the policy will generate an alarm or will be dropped. Creating a security policy requires detailed knowledge of the network traffic and is a time-consuming task.

Policy-based signatures use an algorithm to determine whether an alarm should be fired. Often, policy-based signature algorithms are statistical evaluations of the traffic flow. For example, in a policy-based signature used to detect a port sweep, the algorithm issues an alarm when the threshold number of unique ports is scanned on a particular machine. Policy-based signature algorithms can be designed to analyze only specific types of packets (for example, SYN packets, where the SYN bit is turned on during the handshaking process at eh beginning of the session).

The policy itself may require tuning. For example, you might have to adjust the threshold level of certain types of traffic so that the policy conforms to the utilization patterns on the network that it is monitoring. Policies can be used to look for very complex relationships.

3. Anomaly-Based IDS/IPS Systems:

Anomaly-Based or profile-based signatures typically look for network traffic that deviates from what is seen “normally”. The biggest issue with this methodology is that you first must define what normal is. If during the learning phase your network is the victim of an attack and you fail to identify it, the anomaly-based IPS systems will interpret that malicious traffic as normal, and no alarm will be triggered next time this same attack takes place. Some systems have hard-coded definitions of normal traffic patterns and, in this case, could be considered heuristic-based systems.

Other systems are built to learn normal traffic behavior; however, the challenge with these systems is eliminating the possibility of improperly classifying abnormal behavior as normal. Also, if the traffic pattern being learned is assumed normal, the system must contend with how to differentiate between allowable deviations, and those deviations that are not allowed or that represent attack-based traffic. Normal network traffic can be difficult to define.

The technique used by anomaly-based IDS/IPS systems is also referred as network behavior analysis or heuristics analysis.

4. Honeypot-Based IDS/IPS Systems:

Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns. You can use this analysis to tune your sensor signatures to detect new types of malicious network traffic.

Honeypot systems are used in production environments, typically by large organizations that come across as interesting targets for hackers, such as financial enterprises, governmental agencies, and so on. Also, antivirus and other security vendors tend to use them for research.

IPS ACTIONS:-

When an IPS sensor detects malicious activity, it can choose from any or all the following actions:

- **Deny traffic inline:** This action terminates the current packet and future packets from this attacker address for a specified period of time. The sensor maintains a list of the attackers currently being by the system. You can remove entries from the list or wait for the timer to expire. The timer is a sliding timer for each entry. Therefore, if attacker A is currently being denied, but issues another attack, the timer for attacker A is reset, and attacker A remains on the denied attacker list until the timer expires. If the denied attacker list is at capacity and cannot add a new entry, the packet is still denied.

- **Deny connection inline:** This action terminates the current packet and future packets on this TCP flow. This is also referred to as deny flow.
- **Deny packet inline:** This action terminates the packet.
- **Log 'attacker packets':** This action starts IP logging on packets that contain the attacker address and sends an alert. This action causes an alert to be written to the event store, which is local to the IOS router, even if the produce-alert action is not selected.
- **Log 'pair packets':** This action starts IP logging on packets that contain the attacker and victim address pair. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.
- **Produce alert:** This action writes the event to the event store as an alert.
- **Produce verbose alert:** This action includes an encoded dump of the offending packet in the alert. This action causes an alert to be written to the event store, even if the produce-alert action is not selected.
- **Request block connection:** This action sends a request to a blocking device to block this connection.
- **Request block host:** This action sends a request to the blocking device to block this attacker host.
- **Request SNMP trap:** This action sends a request to the notification application component of the sensor to perform Simple Network Management Protocol (SNMP) notification. This action causes an alert to be written to the event store, even if produce-alert action is not selected.
- **Reset TCP connection:** This action sends TCP resets to hijack and terminate the TCP flow.

EVENT MONITORING AND MANAGEMENT:-

Event monitoring and management can be divided into the following two needs:

- ✓ The need for real-time monitoring and management
- ✓ The need to perform analysis based on archived information (reporting)

These functions can be handled by a single server, or the functions can be placed on separate servers to scale the deployment. The number of sensors that should forward alarms to a single IPS management console is a function of the aggregate number of alarms per second that are generated by those sensors
(25 or fewer; where a mixture of default and tuned signatures are used).

Host and Network IPS:-

IPS technology can be network based and host based. There are advantages and limitations of both but in many cases, they are thought to be complementary.

Host-Based IPS (HIPS) :

HIPS audits host log files, host file systems and resources. A significant advantage of HIPS is that it can monitor operating system processes and protect critical system resources, including files that may exist only on that specific host. HIPS can combine the best features of antivirus, behavioral analysis, signature filters, network firewalls and application firewalls in one package.

HIPS operates by detecting attacks that occur on a host on which it is installed. It works by intercepting operating system and application calls, securing the operating system and application configurations, validating incoming service requests and analyzing local log files for after-the fact suspicious activity.

Precisely, HIPS functions according to the following steps:

Step 1. An application calls for system resources

Step 2. HIPS checks the call against the policy

Step 3. Requests are allowed or denied

HIPS uses rules that are based on a combination of known attack characteristics and a detailed knowledge of the operating system and specific applications running on the host. These rules enable it to determine abnormal or out-of-band activity.

Network-Based IPS (NIPS) :

Network IPS involves the deployment of monitoring devices, or sensors, throughout the network to capture and analyze the traffic. Sensors detect malicious and unauthorized activity in real time and can take action when required. Sensors are deployed at designated network points that enable security managers to monitor network activity while it is occurring, regardless of the location of the attack target.

Network IPS sensors are usually tuned for intrusion prevention analysis. The underlying operating system of the platform on which the IPS software is mounted is stripped of unnecessary network services, and essential services are secured (i.e. hardened). The hardware includes the following components:

- **Network Interface Card (NIC):** Network IPS must be able to connect to any network (Ethernet, Fast Ethernet, Gigabit Ethernet)
- **Processor:** Intrusion prevention requires CPU power to perform intrusion detection analysis and pattern matching
- **Memory:** Intrusion detection analysis is memory intensive. Memory directly affects the capability of a network IPS to efficiently and accurately detect an attack.

Network IPS gives security managers real-time security insight into their networks regardless of network growth. Additional hosts can be added to protected networks without needing more sensors. When new networks are added, additional sensors are easy to deploy. Additional sensors are required only when their rated traffic capacity is exceeded, when their performance does not meet current needs, or when a revision in security policy or network design requires additional sensors to help enforce security boundaries.

Signatures and Signature Engines :-

A signature is a set of rules that an IDS and an IPS use to detect typical intrusive activity, such as DoS attacks.

As sensors scan network packets, they use signatures to detect known attacks and respond with predefined actions. A malicious packet flow has a specific type of activity and signature, and an IDS or IPS sensor examines the data flow using many different signatures.

Signature-based intrusion detection can produce false positives because certain normal network activity can be misinterpreted as malicious activity. False positives can be minimized by tuning the sensors. Signatures can be tuned by adjusting many signature parameters.

Examining Signature Micro-Engines:

A signature micro-engine is a component of an IDS and IPS sensor that supports a group of signatures that are in a common category. Each engine is customized for the protocol and fields that it is designed to inspect and defines a set of legal parameters that have allowable ranges or sets of values. The signature micro-engines look for malicious activity in a specific protocol. Signatures can be defined for any of the supported signature micro-engines using the parameters offered by the supporting micro-engine. Packets are scanned by the micro-engines that understand the protocols contained in the packet.

When IDS (promiscuous mode) or IPS (inline mode) is enabled, a signature micro-engine is loaded (or built) on to the router. When a signature micro-engine, the router may need to compile the regular expression found in a signature. Compiling a regular expression requires more memory that the final storage of the regular expression.

A regular expression is a systematic way to specify a search for a pattern in a series of bytes. For example, a regular expression used to prevent data containing .exe or .com or .bat from crossing the firewall could look like this:

“.*\.([Ee][Xx][Ee]|[Cc][Oo][Mm]|[Bb][Aa][Tt])”

Signature Alarms :

The capability of IDS and IPS sensors to accurately detect an attack or a policy violation and generate an alarm is critical to the functionality of the sensors. Attacks can generate the following types of alarms:

- **False positive:** A false positive is an alarm triggered by normal traffic or a benign action. For example a wrong password entered mistakenly by a genuine user may result in false positive. The sensor cannot differentiate between a rogue user and a mistaken user.
- **False negative:** A false negative occurs when a signature is not fired when offending traffic is detected. A false negative should be considered a software bug only if the IDS and IPS have a signature that has been designed to detect the offending traffic.
- **True positive:** A true positive occurs when an IDS and IPS signature is correctly fired, and an alarm is generated, when offending traffic is detected.
- **True negative:** A true negative occurs when a signature is not fired when non-offending traffic is captured and analyzed. In other words, the sensor does not fire an alarm when it captures and analyzes “normal” network traffic.