Intrusion Detection System and Intrusion Prevention System – A Review Study

Kanika
Research scholar, Department of Electronics and Communication Engineering,
CT Institutes of Engineering and Management Technology, Jalandhar, Punjab, India
Email ID- kanika.31may@gmail.com

Abstract—Intrusion detection system (IDS) and intrusion prevention system (IPS) forms a security solutions to the robust network. A key requirement of a network is to maintain or provide a secure network services. So IDS and IPS both are network security devices that examine traffic looking for attacks. They are different by way of deployment of these devices in the network. IDS can only be deployed in promiscuous mode or out of band mode that is it cannot place within the network; it just receives the copy of the traffic whereas IPS can be deployed in the inline mode that means the traffic can pass through this device. If anomaly traffic pass through the network IDS would generate either a false positive or false positive which means it only detects the malicious traffic, takes no action and generates only alerts but IPS detects the malicious traffic or suspicious activity, takes the actions like terminate, block or drop the connections. An IPS combines the features of firewalls and IDS which can provide an intelligent tool that will change the network access point configurations according to the threats that are found in the network. The present paper tells the IDS/IPS security, its classifications, detection method used and the difference between them.

Index Terms— Alerts, firewall, IDS, IPS, malicious activity, SIEM and signatures.

1 Introduction

Intrusion is "Any set of actions that attempts to destroy the integrity, confidentiality, non-repudationality and availability of the resources" [3]. The intrusion detection is the act of monitoring the events that are occurred on end devices or network and detects the suspicious events such as illegal and malicious traffic by using signs of possible activities which are threat for computer or network security policies, acceptable use policies and security standards. Intrusion prevention is the act of performing intrusion detection and stops the detected events. Intrusion detection and prevention system (IDPS) used together provides identification of possible threats, logging information, attempts to block them and informs the security administrators. Organizations use IDPS for many other purposes like security procedure and policies. IDPS have become a necessary device to the security infrastructure of many organizations. IDPS is either of hardware or software type. Hardware is composed of components like sensors, database servers, management servers and administrator consoles. And the software is composed of all the IDS software and sometimes the operating system is also considered. But we have to keep all the operating system and applications up to date. IDPS integration can be performed by using SIEM software which stands for security information and event management. It is designed to bring information from various security logs, correlate events and help users by providing the accuracy of IDPS alerts [2].

There is a feature in IPS which is known as event action filter. If the filter stores the source IP address 10.2.0.1 then all the packets belonging to that address is forwarded. But if the packets belongs to other IP address tries to pass through it will block immediately as it does not match with the filter's IP address and considered as unauthorized individual.

2 IDS/IPS Security

Some organizations use firewalls as well as routers along with IPS/IDS. Basically the difference between both is that firewall only checks IP address and port no. By using port no. and IP address it blocks the traffic, for example for telnet we use port no. 29 if we want that no one can log in from outside the company we simply block that port whereas IPS/IDS will check each and every packet. It uses some signatures for detection; if packet meets the criteria or rules that are set in signatures it simply forward that packet otherwise block that packet.

Firewall is the first line which can protect our network against the intruders. As explained above it can detect only limited attacks. So we use IDS/IPS in between front end firewall and back end firewall which can detect and prevent the internal network traffic from the attacks called the DMZ, perimeter network and screened subnet. For example, in order to access the internet the web server use TCP port 80 and the hacker use this port to attack on the web server. So we can place IPS/IDS in between that port and web server by comparing the traffic with the internally set signatures [5]. So IDS/IPS provides an extra layer of protection for the traffic against internet accessible web servers etc.

3 Classifications

Intrusion prevention systems can be classified into four different types: [4]

3.1 Network Based Intrusion Prevention System (NIPS)

It monitors the entire network at all the layers of OSI model

and takes some decision about suspicious traffic. It will do this by analyzing protocol activity.

3.2 Wireless Intrusion Prevention System (WIPS)

It is similar to NIPS in that it analyzes or monitors a wireless network for suspicious traffic. This will be done by analyzing wireless networking protocols.

3.3 Network Behaviour Analysis (NBA)

It examines network packets or segments to identify threats that generate the anomalies and take decision according to anomalies exist or not such as denial of service (DOS) attacks, malware and policy violations.

3.4 Host-based Intrusion Prevention System (HIPS)

HIPS is installed software package on a single host which monitors suspicious activity by analyzing network traffic, security policies and other events.

4 Working or Detection Methods

IDS normally use signature based detection and anomaly based detection method against suspected intrusions.

4.1 Signature-Based Detection

This method of detection is based on pattern matching which are used to detect the attacks by using signatures, also known as misuse detection. In this there are attack patterns which are predetermined and preconfigured. It monitors the network traffic and matching procedure is done with that signatures. If there is any match found it takes some appropriate action. It is very fast method and convenient to use. But has one disadvantage hackers can slightly modify the data so that it cannot be detected by this method. So we have to keep up to date. Example is Finger print analysis.

4.2 Anomaly-based detection

This method watches for deviations from normal usage pattern. It creates a baselines performance on the basis of average network traffic conditions. When a baseline is created, the system monitors the activity that is outside with those baseline parameters. If any activity is outside the baseline parameters then it takes the appropriate action. It monitors users and behaviour of the network. For example a police officer who will check or walks each and every beat around its area. When he sees something different from the ordinary, it creates suspicious in his mind about something may go wrong. At that time he investigates about the crime and even tries to identify who is responsible for that.

A problem is that there is a possibility of false positives.

5 How IDS and IPS are different from each other

The main differences between intrusion detection systems and intrusion prevention systems are that IPS is the extension of IDS. An IPS are placed in-line and if there is any intrusion detected in the line it prevent or block it. At that time IPS take actions like sending an alarm, drops the illegal or malicious packets, resetting or abort the connection and block the traffic. As compare to IPS, IDS sits off to the another side of line, only detects the intrusions but cannot prevent it.

An IPS can correct the errors using CRC method i.e. Cyclic Redundancy Check, provides sequencing and prevent TCP issues of sequencing [6]. IPS has a set of policies if certain packet meet with that policy or criteria then packet will be forward otherwise dropped. On the other hand IDS is a monitoring device if it detects anything it cannot act on it directly. It is connected through a port on a switch or router it has a copy of traffic but it does not interact with the server. It is just like security operation centre which monitors the alerts, do some investigation and take appropriate action.

IPS and IDS both have disadvantages. The problem in IPS is that if there are false positives, a lot of people can get disturbed and upset. Another one is if IPS fails then whole of the communication will be block. And the problem with IDS is that it generates so many alarms or alerts and the prioritization buckets are too large such that the SOC (Security Operation Centre) cannot investigate on all the alarms [6]. But still we overcome this problem by using the technology known as RISK rating. Risk rating is a technique which helps us to filter all the alerts on the basis of their priority by considering various other factors.

$$RR= [(ASR*TVR*SFR)/10,000] + ARR-PD+WLR \quad (1)$$

To calculate risk rating we can use equation (1) whereas ASR (attack severity rating) – It generates the value that tells about the how much damage is there when an attack occurs.

SFR (signature fidelity rating) - It indicates how accurate is the signature or the degree of attack certainity and generates the value.

TVR (target value rating) – It will generate the value and give the information about the IP address that is assigned to specific host.

ARR (attack relevancy rating) – It generates the value that indicates the vulnerability of the attack target.

PD (promiscuous delta) –The risk rating of IPS when deployed in promiscuous mode is lowered by promiscuous delta. It is configured on per-signature basis.

WLR (watch list rating) - It tells about the data found in watch list that contains IP address of the devices that are found in network contaminated with viruses. If an attack occurs and found in watch list then WLR is added to RR [7].

If the RR value is set to 80 by default and all the alerts which are triggered having the calculated RR value above 80 then IDS will generate an alert and it will assign the priority and SOC investigate on that alert.

The difference between IPS and IDS can be well understood by taking an example. This example tells what will happen when an attack occur and is monitored by IDS and IPS [1].

A management console is a separate computer or workstation having installed software which are used to configure, monitor and report on alarms, any activity or any other events. A sensor can be deployed in two ways either in promiscuous mode or in inline mode. In the promiscuous mode, the sensor only receives a copy of traffic or packets but the traffic makes its way to the target destination while in inline mode all the traffic have to be pass through sensor that is placed in inline mode, can monitor or actively block the data before they reach to their target destination as shown in fig 1.

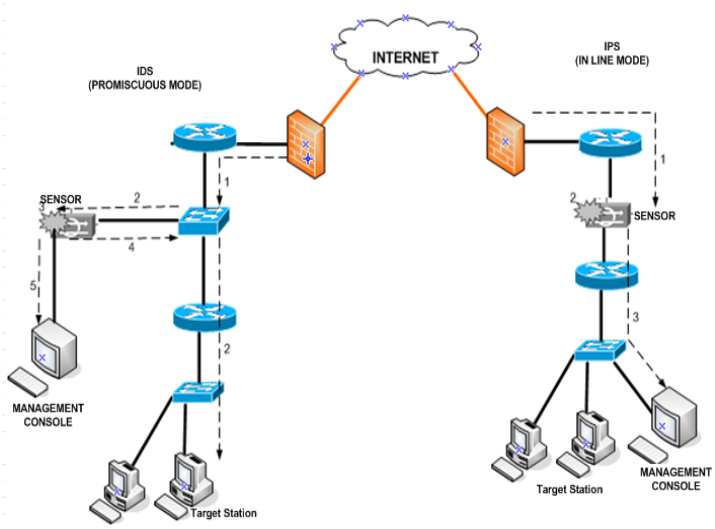

Fig.1 Traffic across IPS and IDS

5.1 IDS

When an attack is occurred on the network, a sensor is deployed in IDS mode.

The switch sends copies of all packets to the IDS sensor so that it analyzes the packets. But at the same time, the malicious attack enters into the target machine.

The IDS sensor which is using a signature detection method matches the malicious traffic or attacks to the signatures.

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

At the same time the IDS sends an alarm to a management console for management purposes etc.

5.2 IPS

When an attack is occurred on a network, a sensor is deployed in IPS mode.

When the packets come into the IPS sensor interface it checks the packets. The IDS sensor which is using a signature detection method matches the malicious traffic or attacks to the signatures and the attack is blocked immediately.

At the same time the IPS sensor can send an alarm to a management console for management purposes etc.

6 FUTURE SCOPE

The future scope of IDS/IPS is to extend its capabilities for other security purposes. The technology is known as Unified threat management (UTM). The goal of this technology is to provide a set of security features in a single product which can be deployed in a single location. The features of UTM are advanced firewalls having deep inspection of packets, gateway anti-spyware and antivirus, IDS/IPS features and capabilities, web content filtering in order to block the malicious websites and the VPN that is virtual private network which can provide the secure remote access for the users with in the organization [8].

7 CONCLUSION

IPS and IDS fulfills the basic needs of the business regarding security. It is a foundation of technology that tracks, monitors the traffic across the network, identifies the suspected traffic, blocks and takes the necessary actions by informing the administrator. If the organization wants to send the data confidentially then it's best to use IPS/IDS. In order to provide the extra network security and protective layer another way is to use firewall or router along with IPS/IDS. It is just like a check point for the traffic.

ACKNOWLEDGMENT

I would like to thank Dr. Amit Kohli, Professor in DAV institute of Engg & Technology, Jalandhar. I can fulfill this work under his guidance and moral support.

REFERENCES

[1] Catherine Paquest, "Implementing CISCO IOS network security", published by CISCO Press, April 2009, pages 437-440.

[2] Karen A. Scarfone; Peter M.Mell, "NIST - Guide to Intrusion Detection and Prevention Systems (IDPS)", Feb 2007, pages ES-1-2.

[3] C.N.S.S.L. Glossary - Texas State Library, http://www.tsl.state.tx.us/ld/pubs/compsecurity/glossary.html, accessed on 22-06-2013.

[4] John R. Vacca," Managing Information Security", Chapter 5, March 2010.

[5] Asmaa Shaker Ashoor, Prof. Sharad Gore, "International Journal of Scientific & Engineering Research", Volume 2, Issue 7, July 2011

[6] Harold F. Tipton; Micki Krause," Information Security Management Handbook", Auerbach Publications, 4 sub edition, Oct 1999.

[7] Risk Rating and Threat Rating: Simplify IPS Policy Management, http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html, accessed on 25-06-2013.

[8] Unified threat management: The next-generation network firewall StephenBlow http://searchsecuritychannel.techtarget.com/generic/0,295582,sid97_gci1322686_tax311688,00.html, accesesd on 27-06-2013.