BIOINFO Computer Engineering
Volume 1, Issue 1, 2011, pp-01-04
Available online at: http://www.bioinfo.in/contents.php?id=322

Comparative Study of IDS and IPS

[1]K.C. Nalavade and [2]B.B. Meshram
[1] Computer Department, VJTI, Matunga, Mumbai-1
[2]Professor, Computer Department, VJTI, Matunga, Mumbai-1
e-mail: knalavade@yahoo.com, bbmeshram@vjti.org.in

Abstract—Intrusion detection is an important component of a modern computer network system's protection from unauthorized and hostile use. The main purpose of a typical intrusion detection system is to detect outside intruders as well as inside intruders that may break into the system. Network intrusion detection systems, which are part of the organizations defence scheme, must be able to meet the security objectives in order to be effective. IDS have drawback of not being active in taking actions against intrusions. Also raising number of false alarms lead to design Intrusion Prevention Systems. IPS's are designed to protect information systems from unauthorized access, damage or disruption by detecting the intrusion and taking action against it. This paper gives the comparative study of Intrusion detection systems and Intrusion Prevention Systems giving the idea which meets security objectives.

Keywords: Intrusion, Security, Attacks, Vulnerability, Prevention

I. INTRODUCTION

With the global Internet connection, network security has gained significant attention in the research and industrial communities. An Intrusion detection system (IDS) is software designed to detect unwanted attempts at accessing, manipulating, or disabling of computer systems, especially through a network. It is a specialized tool that knows how to parse and interpret network traffic and host activities. The main target of IDS is to detect intrusions and intrusion attempts within our network, allowing a savvy admin to take appropriate mitigation and remediation steps. IDS will not prevent these attacks, but it will let you know when they occurred.

Furthermore, an IDS often stores a database of known attack signatures and can compare patterns of activity, traffic, or behavior it sees in the data it's monitoring against those signatures to recognize when a close match between a signature and current or recent behavior occurs. At that point, the IDS can issue alarms or alerts and collect evidence of the disreputable activities.

Intrusion detection provides a way to identify and thus allow responses to, attacks against these systems. Detecting an attack as it occurs is one thing, stopping it is another. The highest priority of any IT security activity in this area is to prevent an attack and possible related disaster; IDS often deliver little to meet this demand. So, the Intrusion detection System was extended and then comes Intrusion Prevention System. The inadequacies inherent in current defenses have driven the development of a new breed of security products known as *Intrusion Prevention Systems* (IPS).

An Intrusion Prevention System is a network security [4] device that monitors network and system activities for malicious or unwanted behavior and can react, in real-time, to block or prevent those activities. IPS make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. These systems are proactive defenses mechanisms designed to detect malicious packets within normal network traffic and stop intrusions dead, blocking the offending traffic automatically before it does any damage rather than simply raising an alert as, or after, the malicious payload has been delivered

II. INTRUSION DETECTION SYSTEMS

With the global Internet connection, network security has gained significant attention in the research and industrial communities. An Intrusion detection system (IDS) is software designed to detect unwanted attempts at accessing, manipulating, or disabling of computer systems, especially through a network. It is a specialized tool that knows how to parse and interpret network traffic and host activities.

The main target of IDS [1] is to detect intrusions and intrusion attempts within our network, allowing a savvy admin to take appropriate mitigation and remediation steps. IDS will not prevent these attacks, but it will let you know when they occur.

Intrusion Detection Systems, IDS, analyze network traffic and generate alerts when malicious activity is discovered. They are generally able to reset TCP connections by issuing specially crafted packets after an attack begins and some are even able to interface with firewall systems to re-write firewall rulesets on the fly.

Intrusion detection systems are classified into two general types known as signature based and heuristic based. IDSs that operate on a single workstation are known as host intrusion detection system (HIDS), while those that operate as stand-alone devices on a network are known as NIDS. HIDS monitor traffic on its host machine by utilizing the resources of its host to detect attacks. NIDS operate as a stand-alone device that monitors traffic on the network to detect attacks. NIDS come in two general forms; signature based NIDS and heuristic based NIDS. These two types of NIDS provide a varying degree. [1]

By today we have several kinds of IDSes in the field. It is possible to distinguish IDSes by the kinds of activities, traffic, transactions, or systems they monitor.

- IDSes that monitor network links and backbones looking for attack signatures are called *network-based IDSes*, whereas those that operate on hosts and defend and monitor the operating and file systems for signs of intrusion and are called *host based IDSes*
- Groups of IDSes functioning as remote sensors and reporting to a central management station are known as *distributed IDSes*.
- A *gateway IDS* is a network IDS deployed at the gateway between our network and another network, monitoring the traffic passing in and out of our network at the transit point.
- IDSes that focus on understanding and parsing application-specific traffic with regard to the flow of application logic as well as the underlying protocols are often called *application IDSes*.

IDSes can also be distinguished by their differing approaches to event analysis. Some IDSes primarily use a technique called *signature detection*. This resembles the way many antivirus programs use virus signatures to recognize and block infected files, programs, or active Web content from entering a computer. The IDS's which warn the intrusions depending upon the difference in current network traffic and normal activity are called as Anomaly Detection System (ADS). This type of IDS usually catches the data from the network and applies its rules to the data or detects differences in them.

A. False positive & Negative Alarms

The first security objective for consideration in any organization is the accuracy of the NIDS in detecting attacks and the frequency of its accuracy. In order to determine the accuracy rate of the heuristic based and signature based network intrusion systems, the false negatives and false positives of these systems are deduced. False negatives are associated with signature based NIDS. Signature based NIDS require the use of signatures incorporated into its database to match the signatures of packets of data entering into the network. Signatures of known viruses and other malicious codes are placed in the database for signature matching. As a result, any attack for which it has the signature can be accurately identified and detected. Unfortunately, newly created malicious code or known viruses with modified signatures are allowed to go undetected within the system and are classified as a false negative. Such a drawback is owed to the inability of signature based NIDS to detect new attacks as stated by McHugh et al. [4]. False positives are also generated by signature based NIDS as supported by Conorich, who indicates that outdated malicious signatures could be the signatures of a new benign application programs [3] and a subsequently flagged due to these amendments. Unlike signature based NIDS, the rate of false negatives are rare for heuristic systems as supported by Liston [5]. The non-dependence upon signatures and the use of statistical and behavioral patterns as the means to detect new types of malicious code allows for a low false negative rate. Heuristic based NIDS use behavioral patterns of users, applications and other program files to develop a pattern of normal and abnormal behavior, which is then used to detect the occurrence of an attack. Subsequently, any deviation from normal behavior by a user or program within the system would be detected and flagged, thereby generating an alarm. Unfortunately, most alarms are benign and false positives are derived as a result. For example, a programmer with authorization to all aspects of the system, but usually works with programs files, may access log files and would be flagged as a result, since it deviates from the normal behavior of the programmer. High false positives, as asserted by Pfleeger and Pfleeger can lead to administrators becoming disenchanted with heuristic systems by investigating less, alarms raised [6]. Although, the high rate of false positives are solvable. In accordance with the structure of a heuristic based NIDS, refinement of its detective analysis is based on continued sampling of statistical and behavioral patterns. The greater the volume of data available for sampling correlates to its ability to distinguish between deviating behavior of benign applications and the behavior of malicious applications. [1]

III. INTRUSION PREVENTION SYSTEMS

Intrusion Prevention Systems (IPSs) have become widely recognized as a powerful tool and an important element of IT security safeguards. An IPS is any device that has the ability to detect attacks, both known and unknown, and prevent the attack from being successful.

IPS technologies are differentiated from IDS technologies by one characteristic. IPS technologies can respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which can be divided into the following groups.

A. Response Techniques of IPS

IPS stops the attack itself. It can terminate the network connection or user session that is being used for the attack, and block access to the target from the offending user account, IP address, or other attacker's attribute. 2. *IPS can change the security environment.* The IPS could change the configuration of other security controls to disrupt an attack. 3. *The IPS changes the attack's content.* IPS technologies can remove or replace malicious portions of an attack to make it benign. [2]

B. Approaches to Intrusion Prevention Systems

There are different types of approaches is used in the IPS to secure the network.[2]

1. *Signature-Based IPS*

It is commonly used by many IPS solutions. Signatures are added to the devices that identify a pattern that the most common attacks present. That's why it is also known as pattern matching. These signatures can be added, tuned, and updated to deal with the new attacks.

2. *Anomaly-Based IPS*

It is also called as profile-based. It attempts to discover activity that deviates from what an engineer defines as normal activity. Anomaly-based approach can be statistical anomaly detection and non-statistical anomaly detection. *Policy-Based IPS*: - It is more concerned with enforcing the security policy of the organization. Alarms are triggered if activities are detected that violate the security policy coded by the organization. With this type approaches security policy is written into the IPS device.3

3. *Protocol-Analysis-Based IPS*

It is similar to signature based approach. Most signatures examine common settings, but the protocol-analysis -based approach can do much deeper packet inspection and is more flexible in finding some types of attacks.

C. *IPS technologies*

Basically IPS have two main technologies; host-based and network-based.

1. *Host-based IPS*

Host-based IPSs as shown in Figure 1 monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IPS might monitor are wired and wireless network traffic, system logs, running processes, file access and modification, and system and application configuration changes. Most host-based IPSs have detection software known as agents installed on the hosts of interest. Each agent monitors activity on a single host and also performs prevention actions. The agents transmit data to management servers. Each agent is typically designed to protect a server, a desktop or laptop, or an application service.

Host-based IPSs run sensors on the hosts being monitored, they can impact host performance because of the resources the sensors consume.

2. *Network-based IPS*

A network-based IPS [13] as shown in Figure 2 monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity. Network-based IPS components are similar to HIPS technologies, except for the sensors. A network-based IPS sensor monitors and analyzes network activity on one or more network segments. Sensors are available in two formats: appliance-based sensors, which are comprised of specialized hardware and software optimized for IPS sensor use, and software-only sensors, which can be installed onto hosts that meet certain specifications.

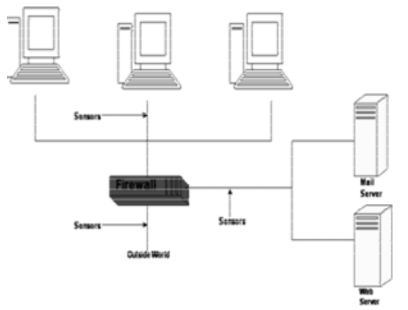

Fig. 1: Host based Intrusion Prevention Systems.

The agents are deployed to existing hosts on the networks, the components usually communicate over those networks instead of using a management network. Host-based IPS sensors are most commonly deployed to critical hosts such as publicly accessible servers and servers containing sensitive information but they are also available for various server and desktop/laptop operating systems, as well as specific server applications.

Host-based IPSs provide a variety of security capabilities. They typically perform extensive logging of data related to detected events and can detect several types of malicious activity. Detection techniques used include code analysis, network traffic analysis, network traffic filtering, filesystem monitoring, log analysis, and network configuration monitoring. Host-based IPSs that use combinations of several detection techniques should generally be capable of achieving more accurate detection than products that use one or a few techniques, because each technique can monitor different characteristics of hosts. Filesystem monitoring can prevent files from being accessed, modified, replaced, or deleted, which can stop malware installation and other attacks involving inappropriate file access.

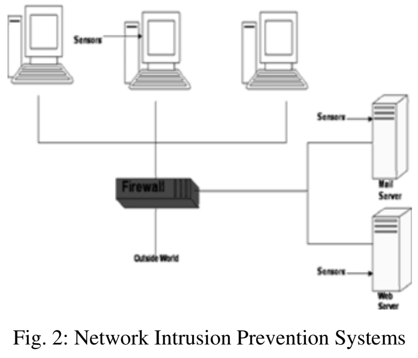

Fig. 2: Network Intrusion Prevention Systems

Organizations should consider using management networks for their network-based IPS deployments whenever feasible. In addition to choosing the appropriate network for the components, administrators also need to decide where the IPS sensors should be located. Sensors can be deployed in one of two modes: *inline sensors* are deployed so that the network traffic they monitor must pass through them, while *passive sensors* are deployed so that they monitor copies of the actual network traffic.

IV. CONCLUSION

Intrusion Detection Systems, IDS, analyze network traffic and generate alerts when malicious activity is discovered. They are generally able to reset TCP connections by issuing specially crafted packets after an attack begins and some are even able to interface with firewall systems to re-write firewall rulesets onthe-fly. The limitation of Intrusion Detection Systems is that they cannot preempt network attacks because IDS sensors are based on packet sniffing technologies that only watch network traffic as it passes by. Intrusion Prevention Systems, IPS, perform the same analysis as Intrusion Detection Systems but, because they are inserted in-line, between other network components, they can preempt malicious activity. In contrast to IDS sensors, network traffic flows through an IPS sensor not past it so the IPS sensor can pull or drop traffic from the wire.

This is the critical difference between IDS and IPS and it has implications for how both can be used. Because IPS sensors require traffic to flow through them, they can only be deployed at network choke points while IDS sensors can provide much broader network coverage.

REFERENCES

[1] Moses Garuba, Chunmei Liu, and Duane Fraites, “Intrusion Techniques : Comparative study of Intrusion Detection Systems”, 5th International Conference on Information Technolgy, IEEE 2008

[2] Teenam Bansode, B.B.Meshram, “Intrusion Prevention System: for End Users”, International Conference Ahmadnagar, March 2009.

[3] Conorich, D. G. (2004). Monitoring intrusion detection systems: From data to knowledge. Information Systems Security 13(2), 19-30. Retrieved October 02, 2006, from WilsonSelect Plus database.

[4] McHugh, J., Christie, A., & Allen, J. (2000). Defending yourself: The role of intrusion detection systems. IEEE Software 17(5), 42-51. Retrieved October 2, 2006, from IEEE Computer Society Digital Library database.

[5] Explain traffic analysis and anomaly detection. Retrieved October 30, 2006,from “http://www.sans.org/resources/idfaq/anomaly_detection.php ?portal=e cf89f730aa7b32ca4ffd0a7117c132f

[6] Pfleeger, C. F., & Pfleeger, S. L. (2003). Security in computing (3rd ed.). Upper Saddle River, NJ: Pearson Education.