IDS vs IPS

Suchita Patil
Computer Department
VJTI
Matunga, India

Pallavi Kulkarni
Computer Department
VJTI
Matunga, India

Pradnya Rane
Computer Department
VJTI
Matunga, India

Dr. B.B.Meshram
Computer Department
VJTI
Matunga, India

Abstract*—— Intrusion detection is an important component in network security. Many current Intrusion Detection Systems are designed on rule-based, which have a limitation of identifying the unknown attacks. Some IDS are designed on anomaly based detection technique which has advantage of identifying known and unknown attacks. It has a disadvantage of learning and training the data set to identify the good and bad data. Some IDS are designed on both signature based and anomaly based detection techniques. Those are also referred to as hybrid IDS systems. 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. This paper focuses oon the difference between IDS and IPS also limitations and advantages of IDS and IPS.

Keywords- signature based system, anomaly detection system, Intrusion Detection system

I. INTRODUCTION

Intrusion Detection System[1]: An Intrusion Detection System is a defense system, which detects hostile activities in a network. The key is then to detect and possibly prevent activities that may compromise system security, or a hacking attempt in progress including reconnaissance/data collection phases that involve for example, port scans. Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources".

One key feature of intrusion detection systems is their ability to provide a view of unusual activity and issue alerts notifying administrators and/or block a suspected connection. In addition, IDS tools are capable of distinguishing between insider attacks originating from inside the organization (coming from own employees or customers) and external ones (attacks and the thread posed by hackers).

Intrusion – a series of concatenated activities that pose threat to the safety of IT resources from unauthorized access to a specific computer or address domain;

Incident – violation of the system security policy rules that may be identified as a successful intrusion;

Attack – a failed attempt to enter the system (no violation committed).

Modeling of intrusions – a time-based modeling of activities that compose an intrusion.

The intruder starts his attack with an introductory action followed by auxiliary ones (or evasions) to proceed to successful access; in practice, any attempts undertaken during the attack by any person, for example by the IT resource manager can be identified as a threat.

An intrusion can be defined (Heady et al., 1990) as "any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource", for example, illegally gaining super user privileges, attacking and rendering a system out of service (i.e., denial-of-service), etc.

Intrusion prevention systems: 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.

Intrusion prevention techniques, such as user authentication (e.g. using passwords or biometrics), avoiding programming errors, and information protection (e.g., encryption) have been used to protect computer systems as a first line of defense.

Intrusion Prevention system[2]:"Intrusion prevention is the art of keeping your network free from attack. It is a holistic approach to security that includes hardening computer systems, deploying utility servers like email gateways and antivirus

servers, and, of course, deploying intrusion prevention systems (IPS)."

The key to differentiating an IDS from an IPS is that an IPS responds immediately and does not allow any malicious traffic to pass, whereas an IDS allows malicious traffic to pass before it can respond.

There are many flavors of IPS, but the basic function of each is to detect and stop attacks by either dropping sessions, resetting sessions, blocking packets, or proxying traffic. An IPS can be either hardware, software, or a combination hardware/software solution. The five main types of IPSes are in-line detection, layer seven switches, deceptive systems, application firewalls, and hybrid switches[3][4].

An in-line detection system is a direct barrier between your network and the rest of the world. It is commonly placed at the outer edge of the network perimeter in front of the firewall. An in-line IPS can also be installed on the interior network for finer tuned prevention. An in-line IPS works like a combination firewall and layer-two bridge. When good data comes across the line, the in-line IPS passes the packets through to the rest of the network. When the packets contain any known vulnerabilities, the firewall blocks the packet or drops the connection.

Layer seven switches are placed in front of the firewall, often acting as a load-balancer for web-based applications. The switch inspects HTTP, SMTP and DNS requests to identify where to direct the traffic. The switch is also able to read the intended URL of the HTTP request to route the traffic appropriately.

Deception systems and honeypots—Honeypots are systems that are online for the sole purpose of being attacked. They are good detectors for both virus attacks and hackers. Honeypots are used to deceive attackers into thinking that they are attacking a valid internal system. When an attacker finds a honeypot through port scanning and then tries to attack the system, the deception system returns a packet marked with misleading data. When the attacker attempts to use that data in his next attack, subsequent traffic is blocked.

An application firewall is software that gets installed on each server being monitored. The software monitors the application(s) on a server, watching the API calls the applications make, the memory utilization, and the way software interacts with the system. The application firewall has to have a behavioral profile built for each system it is installed on so that the firewall knows how to differentiate between proper use and malicious use. Application firewalls are distinct from application layer firewalls or web application firewalls, which are also known as layer seven firewalls. A variant of the application firewall is the personal application firewall, of which Windows Firewall and Zone Alarm are the most widely known. They block access into and out of a client system and block certain types of application behavior, such as instant messaging applications. There is no profiling done to configure the application, although the personal firewall may notify the user the first time it blocks a specific type of traffic so that the user can make the appropriate changes.

A hybrid switch is a combination of an application firewall and a layer seven switch. The switch is a hardware front-end for the protected server. Unlike a layer seven switch that is configured to generally protect the entire network, the hybrid switch is configured to protect one or more similarly configured servers. The switch is set up initially in learning mode so that a policy can be created.

II. RELATED WORK

To design any IDS/IPS three major techniques are used. As specified in [1],[2],[3],[5],[9].

There are three techniques used for detection

1. Misuse detection or Signature detection (knowledge based)
2. Anomaly detection (behavior based)
3. Stateful protocol analysis method

Misuse detection discovers attacks based on patterns extracted from known intrusions. Anomaly detection identifies attacks based on significant deviations from normal activities. Misuse detection has low false positive rate, but cannot detect novel attacks. Anomaly detection can detect unknown attacks, but usually has a high false positive rate. To combine the advantages of both misuse and anomaly detection, many hybrid approaches have been proposed. Data mining is the analysis of large data sets to discover understandable patterns or models. Data mining can efficiently extract patterns of intrusions for misuse detection, identify profiles of normal network activities for anomaly detection, and build classifiers to detect attacks. Data-mining-based systems are more flexible and deployable. The security experts only need to label audit data to indicate intrusions instead of hand coding rules for intrusions. There are many Data mining algorithms that can be used in the Intrusion Detection techniques. There are many papers based on the Probability based algorithm, Information theory based algorithms(based on entropy), Random forest based algorithm which can be used for prediction and probability estimation. The random forests algorithm is an ensemble classification and regression approach, which is one of the most effective data mining techniques.

Here there are some examples of Signatures given.

1) A telnet attempt with a username of "root", which is a violation of an organization's security policy.

2) An e-mail with a subject of "Free pictures!" and an attachment filename of "freepics.exe", which are characteristics of a known form of malware.

3) An operating system log entry with a status code value of 645, which indicates that the host's auditing has been disabled.

4) Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats.

For example, if an attacker modified the malware in the previous example to use a filename of "freepics2.exe", a signature looking for "freepics.exe" would not match it.

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations. Unlike anomaly-based detection, which uses host or network-specific profiles, stateful protocol analysis relies on vendor-developed universal profiles that specify how particular protocols should and should not be used. The "stateful" in stateful protocol analysis means that the IDPS is capable of understanding and tracking the state of network, transport, and application protocols that have a notion of state. For example, when a user starts a File Transfer Protocol (FTP) session, the session is initially in the unauthenticated state. Unauthenticated users should only perform a few commands in this state, such as viewing help information or providing usernames and passwords. An important part of understanding state is pairing requests with responses, so when an FTP authentication attempt occurs, the IDPS can determine if it was successful by finding the status code in the corresponding response. Once the user has authenticated successfully, the session is in the authenticated state, and users are expected to perform any of several dozen commands. Performing most of these commands while in the unauthenticated state would be considered suspicious, but in the authenticated state performing most of them is considered benign. This is helpful when investigating an incident. Some IDPSs can also use the authenticator information to define acceptable activity differently for multiple classes of users or specific users. Stateful protocol analysis can identify unexpected sequences of commands, such as issuing the same command repeatedly or issuing a command without first issuing a command upon which it is dependent. Another state tracking feature of stateful protocol analysis is that for protocols that perform authentication, the IDPS can keep track of the authenticator used for each session, and record the authenticator used for suspicious activity.

Problems with stateful Protocol Analysis is that they are very resource-intensive because of the complexity of the analysis and the overhead involved in performing state tracking for many simultaneous sessions. Another serious problem is that stateful protocol analysis methods cannot detect attacks that do not violate the characteristics of generally acceptable protocol behavior, such as performing many benign actions in a short period of time to cause a denial of service. Another problem is that the protocol model used by an IDPS might conflict with the way the protocol is implemented in particular versions of specific applications and operating systems, or how different client and server implementations of the protocol interact.

One of the challenges in IPS/IDS is the feature selection. Feature selection is essential for improving detection rate. The raw data format of network traffic is not suitable for detection. IDSs must construct features from raw network traffic data, and it involves a lot of computation. Thus, feature selection can help reduce the computational cost for feature construction by reducing the number of features. Another challenge of intrusion detection is imbalanced intrusion. Some intrusions such as denial of service (DoS) have much more connections than others (e.g., user to root). Most of the data mining algorithms try to minimize the overall error rate, but this leads to increasing the error rate of minority intrusions. However, in real-world network environments, minority attacks are more dangerous than majority attacks.

As far as the data source is concerned, intrusion detection can be classified into host-based and network-based detections. [6], [8]

a) *Host-based approaches* detect intrusions utilizing audit data that are collected from the target host machine. As the information provided by the audit data can be extremely comprehensive and elaborate, host-based approaches can obtain high detection rates and low false-alarm rates. However, there are disadvantages for host-based approaches, which include the following.

1) Host-based approaches cannot easily prevent attacks: when an intrusion is detected, the attack has partially occurred.

2) Audit data may be altered by attackers, influencing the reliability of audit data.

b*) Network-based approaches* detect intrusions using the IP package information collected by the network hardware such as switches and routers. Such information is not so abundant as the audit data of the target host machine. Nevertheless, there are advantages for network-based approaches, which include the following.

1) Network-based approaches can detect the so-called "distributed" intrusions over the whole network and thus lighten the burden on each individual host machine for detecting intrusions.

2) Network-based approaches can defend the machine against attack, as detection occurs before the data arrive at the machine.

Any IDS and IPS work in two modes[10].

5) Promiscuous mode : A sensor can be deployed either in promiscuous mode or inline mode. In promiscuous mode, the sensor receives a copy of the data for analysis, while the original traffic still makes its way to its ultimate destination

6) Inline Mode: A sensor working inline analyzes the traffic live and therefore can actively block the packets before they reach their destination.

III. DISCUSSION

Some common characteristics of IDS and IPS technologies: 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: i) 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. ii) 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. iii) IDS and IPS technologies generally uses, 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.

In signature based pattern matching the IDS or IPS looks for the Atomic pattern and Composite patterns.

1) Atomic pattern: In an atomic pattern, an attempt is made to access a specific port on a specific host, and malicious content is 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.

2) Composite pattern: A composite pattern is a sequence of operations distributed across multiple hosts over an arbitrary period of time.

The IDS works differently than IPS when attack is launched on the network. The following are the steps of 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 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.

Whereas the IPS steps are different than IDS. The steps which IPS perform are :

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

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.

Depending on the detection capabilities are used in the IPS and IDS, there are different types of IDS and IPS sensors available. I) Signature based, II) Anomaly based, III) Policy based, III) Honeypot based sensors. Each one has its own advantages and disadvantages.

Signature based IDS/IPs sensors: In signature based sensors configuration settings are easy. Ones system is in use and signatures are updated the system generate very few false positive alarms.

Limitations of signature based Sensors: One major drawback of Signature based is a new attacks or unknown signatures cannot be detected unless signatures are updated, Continuous creating , updating and Tuning has to be done in signature based sensors.

Initially, The system may generate lots of false positive alarms.

Policy based sensors[4]: Policy based sensors are simple and reliable. Also It allows to write a customized policies. These sensors can detect the known and unknown attacks.

Limitations of Policy based sensors is it generate generic output and also it needs to create the policy.

Anomaly based approach: The anomaly based sensors are easy to configure and It detects all known and unknown attacks.

Limitation of Anomaly based sensors is difficult to generate the dynamic profile and static profile in the large network.

Honeypot based sensors provide the window to view attacks. The honeypots are used to distract and confuse attackers.

Table shows advantages of IDS and IPS working in Promiscuous and inline mode respectively.

Table 1: Advantages of IDS and IPS working in Promiscuous mode and Inline mode respectively

Advantages of IDS working in Promiscuous Mode	Advantages of IPS working in Inline Mode
Deploying the IDS sensor does not have any impact on the network (latency, jitter, and so on).	We can configure an IPS sensor to perform a packet drop that can stop the trigger packet, the packets in a connection, or packets from a source IP address.
The IDS sensor is not inline and, therefore, a sensor failure cannot affect network functionality	Being inline, an IPS sensor can use stream normalization techniques to reduce or eliminate many of the network evasion capabilities that exist.
Overrunning the IDS sensor with data does not affect network traffic; however, it does affect the capability of the IDS to analyze the data.	Working in inline mode gives more security to the users on which the IPS is running. It can be a HIPS (Host-based Intrusion prevention system) or NIPS(Network based Intrusion Prevention system).

Following table shows the Limitations of IDS working in Promiscuous mode and limitations of IPS working in Inline mode.

Table 2 : Limitations of IDS and IPS working in Promiscuous mode and Inline mode respectively

Limitations of IDS working in Promiscuous mode	Limitations of IPS working in Inline mode

IDS sensor response actions cannot stop the trigger packet and are not guaranteed to stop a connection. IDS response actions are typically better at stopping an attacker more than a specific attack itself.	An IPS sensor must be inline and, therefore, IPS sensor errors or failure can have a negative effect on network traffic.
IDS sensor response actions are less helpful in stopping email viruses and automated attackers such as worms.	Overrunning IPS sensor capabilities with too much traffic does negatively affect the performance of the network.
Users deploying IDS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IDS deployments. Users must spend time to correctly tune IDS sensors to achieve expected levels of intrusion detection.	Users deploying IPS sensor response actions must have a well thought-out security policy combined with a good operational understanding of their IPS deployments.
Being out of band (OOB), IDS sensors are more vulnerable to network evasion techniques, which are the process of totally concealing an attack.	An IPS sensor will affect network timing because of latency, jitter, and so on. An IPS sensor must be appropriately sized and implemented so that time-sensitive applications, such as VoIP, are not negatively affected.

IV. CONCLUSION

When the computer is connected to network, there has to be more security provided to it. There are many tools available now a day's using which many attacks can happen easily. So to detect the attacks it requires and counter measures of these attacks. There are Intrusion detection system designed to detect the attack and also to store the new attack signatures in to the log file. Snort is the De-facto standard for IDS. And It is open source software. So it is used for research work. The drop action is much more effective for atomic signatures because the sensor makes a single packet match. Implementing an IPS can be risky because it has the potential to slow down network traffic or to set up a self-imposed denial of service attack by blocking legitimate traffic. IPS system presents additional performance challenges because of its in-line nature. Both algorithms based on misuse detection and anomaly detection have advantages and drawbacks. Major drawback of any IPS or IDS is after installing the IDS and IPS computer speed becomes slow. Even if it protect the computer from internal and external threats and attacks It is required to train the IPS and IDS system and Continuous update of signatures or profiles. If the profiles/Signatures are not updated regularly then any IDS or IPS cannot protect the system from the new threats and attacks.

V. REFERENCES

[1] INTRUSION DEECTION SYSTEM using Sax 2.0 and wireshark 1.2.2

[2] Shaw n Conaway ,"Using an Intrusion Prevention System as Part of a Layered Security Approach", Network Support , Technical Enterprises ,October-2006.

[3] IDO GREEN, TZVI RAZ, MOSHE ZVIRAN, "ANALYSIS OF ACTIVE INTRUSION PREVENTION DATA FOR PREDICTING HOSTILE ACTIVITY IN COMPUTER NETWORKS", COMMUNICATIONS OF THE ACM April 2007/Vol. 50, No. 4

[4] SURESH N. CHARI and PAU-CHEN CHENG, "BlueBoX: A Policy-Driven, Host-Based Intrusion Detection System", ACM Transactions on Information and System Security, Vol. 6, No. 2, May 2003.

[5] Nong Ye, Senior Member, IEEE, Syed Masum Emran, Qiang Chen, and Sean Vilbert(2002), "Multivariate Statistical Analysis of Audit Trails for Host-Based Intrusion Detection", IEEE TRANSACTIONS ON COMPUTERS, VOL. 51, NO. 7, JULY 2002.

[6] Fang Yu, T. V. Lakshman, Randy H. Katz (2006), "Efficient Multimatch Packet Classification for Network Security Applications", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 10, OCTOBER 2006 .

[7] Jianchao Han, Mohsen Beheshti, Kazimierz Kowalski, Joel Ortiz, Johnly Tomelden, "Component-based Software Architecture Design for Network Intrusion Detection and Prevention System", IEEE Computer society Sixth International Conference on Information Technology: New Generations 2009.

[8] DAVID J., CHABOYA, RICHARD A. RAINES, RUSTY O. ALDWIN, AND BARRY E. MULLINS,"Network ntrusion etection Automated and Manual Methods Prone to Attack and Evasion", PUBLISHED BY THE IEEE COMPUTER SOCIETY, 2006.

[9] Jiong Zhang, Mohammad Zulkernine, and Anwar Haque(2008), "Random-Forests-Based Network Intrusion Detection Systems", IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS—PART C: APPLICATIONS AND REVIEWS, VOL. 38, NO. 5, SEPTEMBER 2008

[10] Catherine Paquet "Network security using Cisco IDS IPS", Pearson Education