2011 International Conference on Information Communication and Management
IPCSIT vol.16 (2011) © (2011) IACSIT Press, Singapore

A Survey of Intrusion Detection & Prevention Techniques

Usman Asghar Sandhu [1+], Sajjad Haider [2], Salman Naseer [3], Obaid Ullah Ateeb [4]

[1,2] Shaheed Zulfiqar Ali Bhutto Institute of Science & Technology, Islamabad. (SZABIST)
[3,4] University of the Punjab Gujranwala Campus

Abstract. Network security is a large and growing area of concern for every network. Most of the network environments keep on facing an ever increasing number of security threats in the form of Trojan worm attacks and viruses that can damage the computer system and communication channels. Firewalls are used as a security check point in a network environment but still different types of security issues keep on arising. In order to further strengthen the network from illegal access the concept of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) is gaining popularity. IDS is a process of monitoring the events occurring in a computer system or network and analyzing them for sign of possible incident which are violations or imminent threats of violations of computer security policies or standard security policies. Intrusion Prevention System (IPS) is a process of performing intrusion detection and attempting to stop detected possible incidents. This study aims to identify different types of Intrusion Detection and Prevention techniques discussed in the literature.

Keywords: Intrusion, Detection, Prevention, Anomaly, Signature.

1. Introduction

As the network technology is increasing rapidly, the security of that technology is becoming a need for survival for an organization. Most of the organizations are depending on the internet to communicate with the people and systems to provide them news, online shopping, email, credit card details and personal information. Due to the rapid growth in the technology and widespread use of the Internet, a lot of problems have been faced to secure the system's critical information within or across the networks because there are millions of people attempting to attack on systems to extract critical information. A huge number of attacks have been observed in the last few years. Intrusion Detection and Prevention Systems (IDPS) play an immense role against those attacks by protecting the system's critical information. As firewalls and anti viruses are not enough to provide full protection to the system, organizations have to implement the IDPS to protect their critical information against various types of attacks.

2. Intrusion Detection System (IDS)

Intrusion means to interrupt someone without permission. Intrusion is an attempted act of using computer system resources without privileges, causing incidental damage. Intrusion Detection means any mechanism which detects the intrusive behaviour. Intrusion Detection System (IDS) monitors network traffic and its suspicious behaviour against security. If it detects any threat then alerts the system or network administrator. The objective of IDS is to detect and inform about intrusions. IDS is a set of techniques and methods that are used to detect suspicious activities both at the network and host level. There are two main types of Intrusion Detection System, Host Based Intrusion Detection Systems (HIDS) and Network Based Intrusion Detection Systems (NIDS).

+ Corresponding author. Tel.: +92-321-747-4001.
E-mail address: usmanasghar001@yahoo.com.

3. Intrusion Prevention System (IPS)

IPS is an advance combination of IDS, personal firewalls and anti-viruses etc. The purpose of an Intrusion Prevention System (IPS) is not only to detect an attack that is trying to interrupt, but also to stop it by responding automatically such as logging off the user, shutting down the system, stopping the process and disabling the connection etc. Similar to IDS, IPS can be divided into two types, i.e. Host-Based Intrusion Prevention Systems and Network-Based Intrusion Prevention Systems [15].

4. Types of Intrusion Detection Systems

There are two main types of Intrusion Detection Systems.

4.1. Anomaly Detection

Anomaly detection technique store the systems normal behaviour such as kernel information, system logs event, network packet information, software running information, operating system information etc into the database. If any abnormal behaviour or intrusive activity occurs in the computer system which deviates from system normal behaviour then an alarm is generated. Anomalous activities that are not intrusive are flagged as intrusive. This will result in false-positive, i.e. false alarm. (b) Intrusive activities that are not anomalous result in false negative [11].

4.2. Signature Detection

The concept behind signature detection or misuse detection scheme is that it stores the sequence of pattern, signature of attack or intrusion etc into the database. When an attacker tries to attack or when intrusion occurs then IDS matches the signatures of intrusion with the predefined signature that are already stored in database. On successful match the system generates alarm.

5. Intrusion Detection and Prevention Systems

IDPS is a process of monitoring the events occurring in a computer system or network and analyzing them for possible incidents, which are violations or imminent threats of violations of computer security policies, acceptable use of policies or standard security practices and process of performing ID and attempting to stop detected possible incidents.

5.1. Host Based Intrusion Detection and Prevention System (HIDPS)

If we merge both IDS and IPS on a single host then it is known as a Host-based Intrusion Detection and Prevention System (HIDPS). Host-based Intrusion Detection and Prevention System (HIDPS) relates to processing data that originates on computers themselves, such as event and kernel logs. HIDPS can also monitor that which program accesses which resources and might be flagged. HIDPS also monitors the state of the system and makes sure that everything makes sense, which is basically a concept of anomaly filters. HIDPS normally maintains a database of system objects and also stores the system's normal and abnormal behaviour. The database contains important information about system files, behaviour and objects such as attributes, modification time, size, etc. If any suspicious or anomaly behaviour occurs then it generates an alarm and takes some appropriate response against detected threat or attack.

5.2. Network-Based Intrusion Detection and Prevention System (NIDPS)

Intrusion detection is network-based when the system is used to analyze network packets. Network-based Intrusion Detection and Prevention System (NIDPS) capture the network traffic from the wire as it travels to a host. This can be analyzed for a particular signature or for unusual or abnormal behaviours. Several sensors are used to sniff the packets on network which are basically computer systems designed to monitor the network traffic. If any suspicious or anomaly behaviour occurs then they trigger an alarm and pass the message to the central computer system or administrator (which monitors the IDPS) then an automatic response is generated. There are further two types of NIDPS. Promiscuous-mode network intrusion detection is the standard technique that "sniffs" all the packets on a network segment to analyze the behaviour. In Promiscuous-mode Intrusion detection systems, only one sensor is placed on each segment in

the network. Network-node intrusion detection system sniffs the packets that are bound for a particular destination computer. Network-node systems are designed to work in a distributed environment [8].

6. Literature Review

The aim of [1] is to address the issues of information security and describes the security needs of an organization to protect their critical information from attacks. A well trained staff and analysts are required to continuously monitor the system. But still a huge effort is required to construct new security strategies in this system which are discussed in [2], [9] and [12].

[2] Provides a multilayer approach in IDPS to monitor a single host. Multilayer approach consists of three layers. File Analyzer, System Resource Analyzer and Connection Analyzer. The advantage of this technique [2] is that it provides both signatures based and anomaly based detection and prevention. The drawback in Multilayer approach is that the IDPS require a large amount of memory to store the data of the system and network traffic.

Proventia desktop is software based solution [3] which detects and protects the system from network layer up to application layer by known and unknown attacks. This software has great flexibility to set different type of filtering rules. The major drawback of HIPS is its high rate of false-positives. A lot of time and trained staff is required to monitor the IDPS [3].

The idea discussed in [4] helps an organization to take an informal decision in order to select the IDPS. The proposed model divides the IDPS into two types, in-source and out-source. Provide a security to an organization against attacks is a key business of Managed Security Services Provider (MSSP) [4]. MSSP spend most of the time to examine new technology to secure the information better than before. A risk is possible if MSSP do not exactly know the customer requirements of IDPS.

According to [5], Snort and source fire are best IPSs for a multinational company. Snort [5] product provides high flexibility that allow to the user to self configure and modify its source code by using source fire. The major drawback of Snort is that it uses only signature based technique to detect the intrusion but if anomaly behaviour occur then it will not be possible for SNORT to detect that anomaly attack [5].

This paper [6] provides a technique of secure mobile agent in IDPS for the security of system. Secure mobile agent monitors the system, processes the logs, detects the attacks, and protects the host by automated real time response. Major disadvantage is that if the target of the attackers is mobile agent then it will be difficult to protect the system from being hacked. So it needs to adopt some security infrastructures for the protection of mobile agent.

David and Paolo in [7] examined the technique which shows that how application interacts with the operating system and how (PH) IDS can be broken without detection, by using the technique of sequence matching, inserting malicious sequence and inserting no-op. This technique is unaware about that how much effort and knowledge is required to produce such an attack and also unaware about that how attackers can predict that how IDS actually works.

Harley [8] defines the difference between host based and network based intrusion detection and prevention system. This paper describes two types of network intrusion detection system: Promiscuous-mode and Network-node. The main disadvantage observed is that this IDS only responds to the signature based detected attacks but not to the anomaly based detected attacks. So still there is a need of human interaction who took real time action to resolve issue [8].

Novel string matching technique [9] is an optimization of other matching algorithms. Novel string matching algorithm breaks the string into small sets of state machines. Each state machine recognizes the subset of string. If any suspicious behaviour occurs then the system broadcasts the information about intruder to every module (state machine) which holds the database in order to define rules and compares the signatures of intruder with predefined detected signatures. This algorithm is most efficient and ten times faster than the other existing systems and it consumes less resources. The major issue is its practical implementation and it requires a large amount of memory. This algorithm is not capable to detect the anomaly behaviour of the intrusion as in [7] and [14].

According to S. Mrdović and E. Zajko [10], Distributed IDS is used to analyze the system in which multiple sensors are placed in selected network segments that observe the network traffic behaviour. SNORT is used as an analysis engine. Mysql is used to log the events with the help of SNORT. Distributed IDS is managed by management console which monitors and configures the IDS. This IDS provides a greater protection against attacks because multiple computers are continuously monitoring and preventing the network from malicious attacks [13]. Large memory and well trained security analysts are required to implement and continuous management of the system [13].

This paper [11] describes the security of IDS. It highlights the two different techniques of IDS. Misuse detection and anomaly detection. Three different approaches data mining, data fusion and immunological based approach used in IDS. This paper provides brief information about existing intrusion detection technology. It evaluates the challenges and future directions of intrusion detection technology. The approaches that are discussed in [4], [9] & [14] are much sufficient for IDPS to detect and respond to anomalies in real time.

This paper [12] proposed intrusion detection techniques by combining multiple hosts in order to detect multiple intrusions and to reduce false-positive rate. Hidden Markov Model (HMM) is a speech recognition technique that is used for modelling the system call events. Statistical technique gives the percentage of resource usages and system call events. Decision tree is used to model or classify the type intrusion to examine the future challenges. This technique [12] has advantage of less false-positive rate that increases performance of detection. If this IDS adopt the mechanism of protection that is discussed in [4] and [8] then the system can be secured in a better way.

INDRA (Intrusion Detection and Rapid Action) [13] provides IDPS that uses peer to peer approach for the security of network that works in a distributed environment by distributing the intruder's information on peer to peer network. If INDRA finds any interrupt then security agent cut off the effected packets. This IDPS is reliable and trusted and efficient. It requires a large amount of memory to store all the collected information about intruder as discussed in [2] and [3].

This paper [14] has proposed architecture to protect HIDS through virtual machine by observing the system behaviour or monitor the system inside a virtual machine. This technique is efficient, duplication of real operating system, invisibility and inaccessibility to intruders. Multiple virtual machines can run simultaneously on same hardware. The major benefit is cost effectiveness then other techniques discussed in [2] and [3].

Matt and Andrew in [15] investigate the IDPS and also IDS/IPS tools. SNORT is used to configure the log into the database directly. MySQL installed to create the schema and configure the setting of permissions. TRIPWIRE software is used to monitor the changes in specific files and enable the SNORT to continuously check logs. The major benefit of SNORT is that it can detect a large number of different attacks such as viruses, Denial of services, malware etc.

7. Critical Analysis

Lit. ref.	System	Category	Type or Approach	Signature Detection	Signature Prevention	Anomaly Detection	Anomaly Prevention	Technique	Advantages	Disadvantages
[1]	IDPS	HIDPS and NIDPS	Operating system and Application level approach	Yes	Yes	Yes	Yes	Signature based and anomaly based	Automatic response, reduce human effort	Cost ineffective, implementation, updating, monitoring issues
[2]	IDPS	HIDPS	OS and Application level approach	Yes	Yes	Yes	Yes	Signature based and anomaly based	Strong detection and protection mechanism	A large amount of memory is requires
[3]	IDPS (Prove ntia Deskto p)	HIDPS and NIDPS	Network layer to application layer level	Yes	Yes	Yes	Yes	Signature based and anomaly based	Flexibility of customize, Cost effective	High rate of false-positive, well trained analysts are required

[4]	IDPS	HIDPS and NIDPS	In-source and out-source	Yes	Yes	Yes	Yes	Signature based and anomaly based	Secured infrastructure	Well trained analysts are required
[5]	IDPS(SNORT)	NIDPS	OS and Application level approach	Yes	Yes	No	No	Signature based	Flexibility of self configuration	Cannot detect anomaly behavior of intrusion
[6]	IDPS	HIDPS	Secure mobile agent	Yes	Yes	Yes	Yes	Signature based and anomaly based	Real time response, reduce human effort	Security of mobile agent, needs to adopt some other techniques
[7]	IDS (PH)	HIDS	sequence matching, inserting malicious sequence and no-op	Yes	No	Yes	No	Signature and anomaly based	Modeling or analysis of different attacks and their techniques	Not fully secured, still have huge risk of attack.
[8]	IDPS	HIDPS and NIDPS	Sequence matching, malicious matching	Yes	Yes	No	No	Signature based	Automated response to malicious attacks	Unable to detect and respond to anomaly behavior
[9]	IDS	HIDS and NIDS	String matching	Yes	No	No	No	Signature based	Efficient and Faster	Memory and implementation issues
[10]	IDS	NIDS	Sequence matching, distributed env.	Yes	No	No	No	Signature based	Flexibility of self configuration	Large amount of memory and training staff is required
[11]	IDS	HIDS and NIDS	Data mining, data fusion	Yes	Yes	No	No	Signature based and anomaly based	Centralized architecture	No mechanism of protection
[12]	IDS	HIDS	Decision tree, statistical approach	Yes	No	Yes	No	Signature based and anomaly based	Less false positive, Efficient detection	No mechanism of protection
[13]	IDPS	HIDPS and NIDPS	Peer to peer	Yes	Yes	Yes	Yes	Signature based and anomaly based	Reliable trusted and efficient	Memory and Implementation issue
[14]	IDS	HIDS	Virtual machine	Yes	No	No	No	Signature based	Cost effective, Efficient	Unable to detect anomaly behavior
[15]	IDPS	NIDPS	SNORT, tripwire, mysql	Yes	Yes	No	No	Signature based	Flexibility of self configuration	Cannot detect anomaly behavior of intrusion

8. Conclusion and Future Work

Different techniques are discussed in this paper to support the security of an organization against threats or attacks. On the other side attackers are discovering new techniques and ways to break these security policies. Firewalls, antivirus and antispyware are limited to provide security to the system against threats. The only way to beat them is to know about their techniques that they use for attack. So, security organizations will have to adopt such a strongest model or mechanism which provides strongest protection against threats to ensure that the system will remain secure. IDPS provides the facility to detect and prevent from attacks by inheriting multiple approaches like secure mobile agent, virtual machine; high throughput string matching, multilayer and distributed approach provide greater and strongest security against multiple attacks. There are still many ways to improve the virtual machine based Intrusion Detection and Prevention System and in future we'll propose a solution to further secure virtual machine based implementation.

9. References

[1] Ahmed Patel, Qais Qassim, Christopher Wills. *A survey of intrusion detection and prevention systems*, Information Management & Computer Security Journal (2010).

[2] Oludele Awodele, Sunday Idowu, Omotola Anjorin, and Vincent J. Joshua, *A Multi-Layered Approach to the*

Design of Intelligent Intrusion Detection and Prevention System (IIDPS), Babcock University, (Volume 6, 2009).

[3] *Host Intrusion Prevention Systems and Beyond*, SANS Institute (2008).

[4] *Intrusion Detection and Prevention In-sourced or Out-sourced*, SANS Institute (2008).

[5] Mario Guimaraes, Meg Murray. *Overview of Intrusion Detection and Intrusion Prevention*, Information security curriculum development Conference by ACM (2008).

[6] Muhammad Awais Shibli, Sead Muftic. *Intrusion Detection and Prevention System using Secure Mobile Agents*, IEEE International Conference on Security & Cryptography (2008).

[7] David Wagner, Paolo Soto. *Mimicry Attacks on Host Based Intrusion Detection Systems*, 9th ACM Conference on Computer and Communications Security (2002).

[8] Harley Kozushko. *Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems*, (2003).

[9] Lin Tan, Timothy Sherwood. *A High Throughput String Matching Architecture for Intrusion Detection and Prevention*, Proceedings of the 32nd Annual International Symposium on Computer Architecture (ISCA 2005).

[10] S. Mrdovic, E. Zajko. *Secured Intrusion Detection System Infrastructure*, University of Sarajevo/Faculty of Electrical Engineering, Sarajevo, Bosnia and Herzegovina (ICAT 2005).

[11] Yeubin Bai, Hidetsune Kobayashi. *Intrusion Detection Systems: technology and Development*, 17th International Conference of Advanced Information Networking and Applications, (AINA 2003).

[12] Sang-Jun Han and Sung-Bae Cho. *Combining Multiple Host-Based Detectors Using Decision Tree*, Australian Joint Artificial Intelligence Conference, (AUSAI 2003).

[13] Ramaprabhu Janakiraman, Marcel Waldvogel, Qi Zhang. *Indra: A peer-to-peer approach to network intrusion detection and prevention*, Enabling Technologies: Infrastructure for Collaborative Enterprises, WET ICE 2003.

[14] M. Laureano, C. Maziero1, E. Jamhour. *Protecting Host-Based Intrusion Detectors through Virtual Machines*, The International Journal of Computer and Telecommunications Networking (2007).

[15] Matt Carlson and Andrew Scharlott. *Intrusion detection and prevention systems*, (2006).