An Inspection on Intrusion Detection and Prevention Mechanisms

Kanagadurga Natarajan[1], Aarthi Sadagopan[2]

[1, 2]Computer Science and Engineering, A.V.C.College of Engineering, Mannampandal, TamilNadu, India

Abstract

Securing a network environment is pivotal for any organization that uses network. Security Threats poses a major challenge for the core of a network and Communication channels in a networking environment. These security threats keeps on increasing every day every minute and every second in a networking organization that needs network connectivity 24/7. Firewalls acts as a check point even so security issues keep on arising like a phoenix bird. Intrusion Detection system(IDS) and Intrusion prevention system(IPS) acts as a fortress of a networking environment and also raving popularity in almost every networking organization. Intrusion Detection system monitors all the events of a network system or a computer system and analyses them and signals those which poses as a violations or threats of violations of computer security policies to the network management system. Intrusion prevention system is also an Intrusion detection system which attempts to stop the detected possible threats with all its might. This Critical analysis aims to study different types of Intrusion Detection and prevention system techniques for securing and encapsulating the networking environment from ever increasing security threats.

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

1. Introduction

Network security is vital for the survival of any organization that uses network technology. Most of the organizations are depending on the internet to communicate with the people and systems to extract necessary information (news, online shopping, email, credit card details and personal information). Due to sensational increase in technology and widespread use of internet a lot of security issues are faced everyday by the network environment. A huge number of attackers are attempting to steal the system's critical information within or across the networks each and every second. These attempts have been increasing over the years as the possibilities and the scopes of internet are limitless nowadays. As firewalls and anti viruses are not enough to provide complete protection to the system, organizations have to implement the Intrusion Detection and Prevention Systems (IDPS) to protect their critical information against various types of attackers lurking in the network environment. Intrusion Detection and Prevention Systems play an immense role against those attacks by protecting the system's critical information. Intrusion Detection and Prevention Systems acts as a fortress for any network environment which makes it impossible or a lot difficult for any attackers from stealing the vital information.

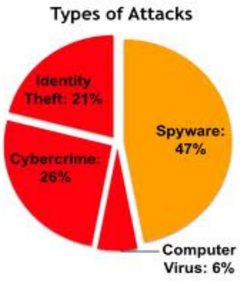


Fig. 1 Types of Attacks

2. Intrusion Detection System

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

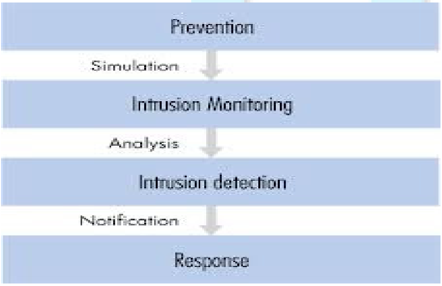


Fig. 2 Intrusion Detection System

3. Intrusion Prevention System

IPS is an ultra 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 the network environment, 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.(reflex) Similar to IDS, IPS can be divided into two types, i.e. Host-Based Intrusion Prevention Systems and Network-Based Intrusion Prevention Systems**.**

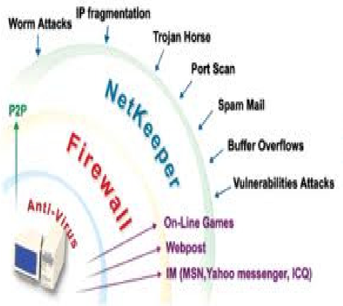


Fig. 3 Intrusion Prevention System

4. Types of Intrusion Detection System

There are two main types of Intrusion Detection Systems.

4.1 Anomaly Detection

Anomaly detection technique store the systems normal behavior such as kernel information, system logs event, network packet information, software running information, operating system information etc in the database. If any abnormal behavior or intrusive activity occurs in the computer system which deviate from system normal behavior 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. Intrusive activities no anomalous result in false negative.

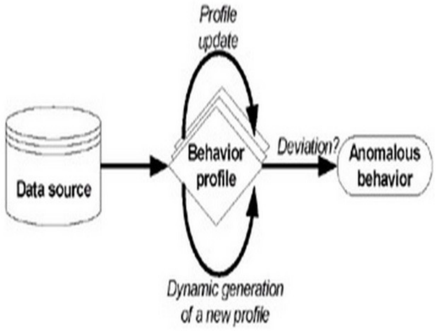


Figure 4 Anomaly Detection

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.

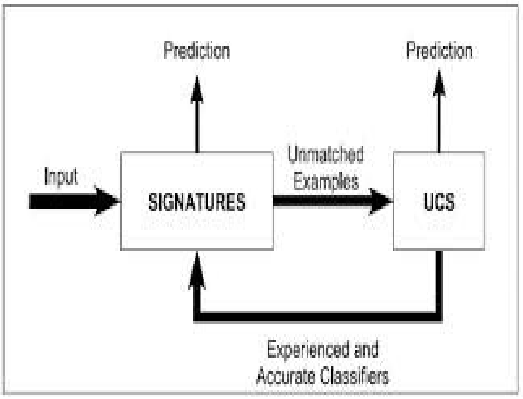


Fig. 5 Signature Detection

5. Intrusion Detection and Prevention System

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 behavior. The database contains important information about system files, behavior and objects such as attributes, modification time, size, etc. If any suspicious or anomaly behavior occurs then it generates an alarm and takes some appropriate response against detected threat or attack.

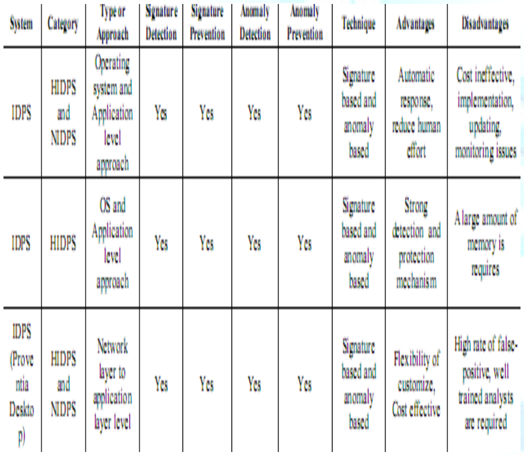
5.2 Network-Based Intrusion Detection and Prevention System (NIDPS)

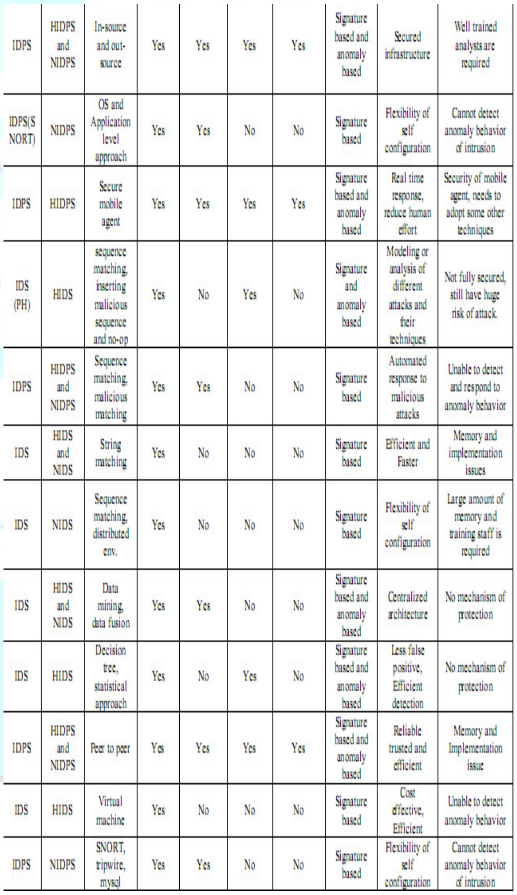
Intrusion detection is network-based when the system is used to analyze network packets. Network-based Intrusion Detection and Prevention System (NIDPS) capture the network traffic from the wire as it travels to a host. This can be analyzed for a particular signature or for unusual or abnormal behaviors 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 behavior 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 behavior. 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.

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.

6. Critical Analysis





System	Category	Type or Approach	Signature Detection	Signature Prevention	Anomaly Detection	Anomaly Prevention	Technique	Advantages	Disadvantages
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
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
IDPS (Proventia Desktop)	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
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
IDPS(SNORT)	NIDPS	OS and Application level approach	Yes	Yes	No	No	Signature based	Flexibility of self configuration	Cannot detect anomaly behavior of intrusion
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
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.
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
IDS	HIDS and NIDS	String matching	Yes	No	No	No	Signature based	Efficient and Faster	Memory and implementation issues
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
IDS	HIDS and NIDS	Data mining, data fusion	Yes	Yes	No	No	Signature based and anomaly based	Centralized architecture	No mechanism of protection
IDS	HIDS	Decision tree, statistical approach	Yes	No	Yes	No	Signature based and anomaly based	Less false positive, Efficient detection	No mechanism of protection
IDPS	HIDPS and NIDPS	Peer to peer	Yes	Yes	Yes	Yes	Signature based and anomaly based	Reliable trusted and efficient	Memory and Implementation issue
IDS	HIDS	Virtual machine	Yes	No	No	No	Signature based	Cost effective, Efficient	Unable to detect anomaly behavior
IDPS	NIDPS	SNORT, tripwire, mysql	Yes	Yes	No	No	Signature based	Flexibility of self configuration	Cannot detect anomaly behavior of intrusion

7. Conclusion

Different techniques are used against the security issues of an organization that uses network technologies in a network environment. Even so the attackers are trying to break the security policies. Firewall, antivirus and anti spyware only provides limited amount of security. So, security organizations will have to adopt such a strongest model or strongest mechanism which provides strongest protection against threats to ensure that the system remains secure no matter what attacks them. 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.

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).