I J C T A, 9(20), 2016, pp. 391-397

Application Based Intrusion Detection System

Deepanshu Mangla* and Himanshu Gupta**

ABSTRACT

Today's world is mainly depending upon internet and internet now a day is becoming more and more vulnerable as new set of cyber-attacks are created and deployed every day. We need to understand the root where all these activities are done, that is devices used by end user.So we need to have some think in every host device that will monitor different malicious application.To generate intrusion one need some specific software with specific configuration and sometime need some additional hardware. We just to check if host is using these software, configuration and hardware, if yes then that host is put under suspect list, this list is provided to admin, which help to mainly focus on suspected host only. In this paper a new method or a new way to use Application based intrusion detection and prevention system is explained with their features.

Keywords: IDS, IPS, IDPS, NIDPS, Intrusion, Malicious Activity.

1. INTRODUCTION

Intrusion isblocking or interruption in normal network working created by any malicious activity performed by cracker. IDS (intrusion detection system), IPS (intrusion prevention system) and both collectively called IDPS (intrusion detection and prevention system) are mainly use for detecting and stopping /preventing those malicious activity or cyber-attack on network.

An IDS look in network or host or both for suspicious activity and events that might be the result of a virus, worm or hacker. This is done byscanning all incoming and outgoing packet to find known intrusion signatures or attack signatures that characterize different worms or viruses and take a close look on host activity and if there is variance in host activity which is difference from normal system activity [2][3][5]. The IDS is able to provide notification of only known attacks. the main function of an IDS product is to warn you of suspicious activity taking place – not prevent them [3][5].

IDSs consist of both software applications and hardware appliances and sensor devices which are installed at different points along your network.

IDS technique used are [2]:

Misuse detection–catch known attacks or system vulnerabilities, but can't detect unknown attacks.

Anomaly detection -Catch the intrusions in terms of the characteristics of known attacks or system vulnerabilities. There is a problem that it generates false alarm too frequently, which eat up administrator's time.

IDS are mainly of two types [2][3]: -

a) NIDS (network intrusion detection system)

b) HIDS (host intrusion detection system) [8].

* Amity Institute of Information technology Amity University Noida,Uttar Pradesh, India, *Email: dmangla85@gmail.com*

** Amity Institute of Information technology Amity University Noida,Uttar Pradesh, India, *Email: hgupta@amity.edu*

Network based IDS check the traffic coming from internet or other network forsenescing maliciousness. Host based IDS is check the host logs, study the host pattern, check outgoing and incoming packets to find any malicious activity done by host [8].

IPS is also known as IDPS. the main function of IDPS is to identify malicious activity, log information about this activity, attempt to block/stop it, and report it [4].

In this figure IDS scan incoming and outgoing packet, if IDS detect any intrusion, it will fire the alarm then IPS try to prevent and minimize the damage that can be done by intrusion. When IDS and IPS work together it's called IDPS. Router don't have capability to stop harmful traffic but IDPS system detect the malicious traffic and prevent the network form malicious traffic that can cause intrusion in network.

IDS is use to scan the data packet; it looks for some predefined parameters in the packet. If it finds, it fires the alarm. IPS is used to prevent or stop and minimize the intrusion effect. First IDS scan the packet and if packet contain malicious code by which intrusion can be generated, IDS fire the alarm, then IPS start its work by stopping intrusion to generate or by minimize the intrusion effects [5].

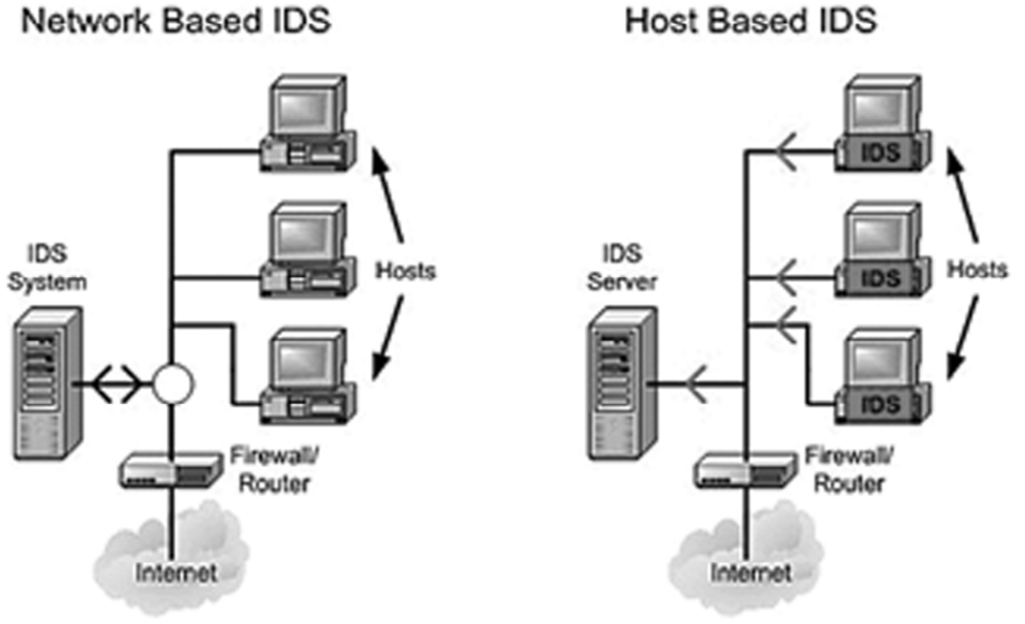

Figure 1: Working of NetworkBased IDS and Host Based IDS

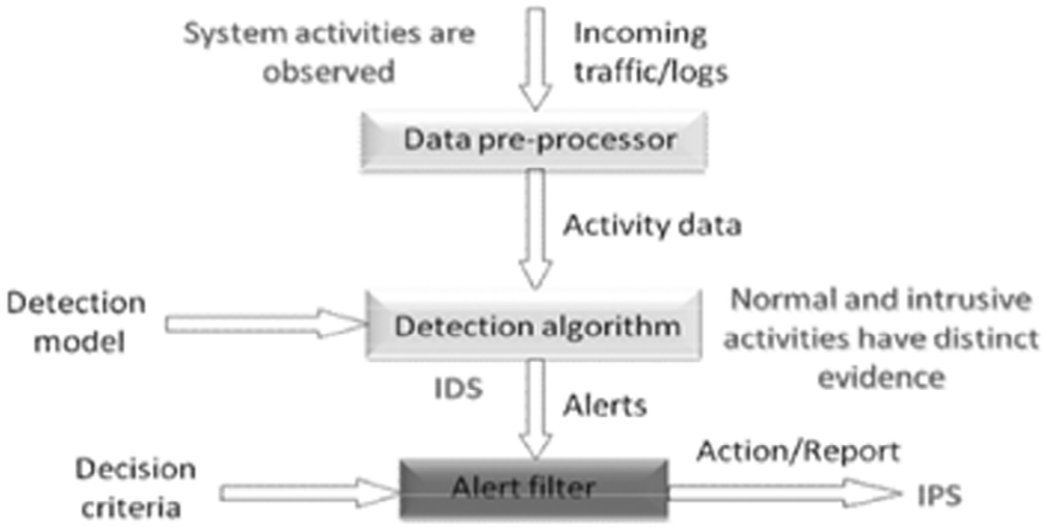

Figure 2: Working of IDPS

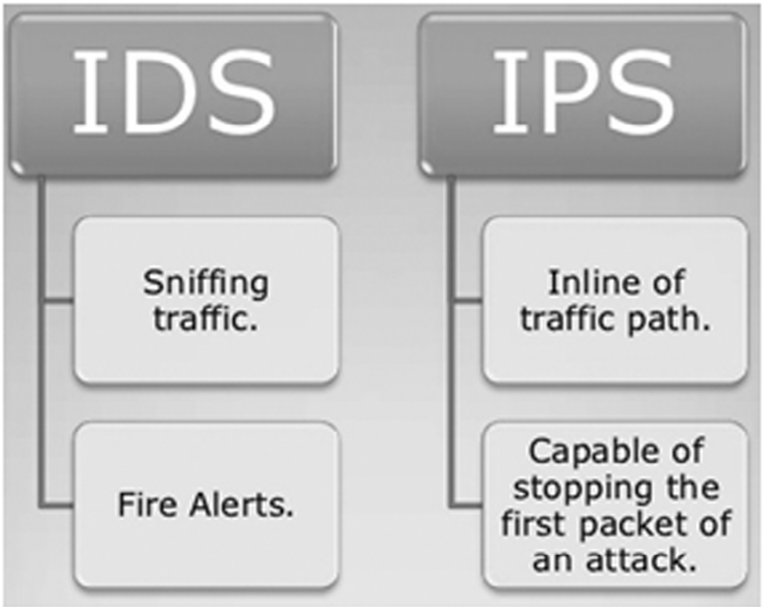

Figure 3: Difference Between IDS and IPS

III. PROPOSED METHOD

There must be some think every strong on host side that will scan and look each host activity for determining malicious code, activities and software. AIDPS on host devices should be used to monitor activities of different applications that are installed and used by host including those applications which attacker has installed remotely in host device and using them for its own purpose. We can use AIDPS as an antivirus software to be installed in host devices which will scan and inform host about the presence of malicious applications and configuration in its devices so that host can remove them, otherwise AIDPS will inform/ notifyadministrator that such malicious software is present in host devices and host is not removing them from the device.AIDPS is connected to a database which contain list of malicious software, their behavior and their configuration. All Application-Based IDPS communications shall be secure and use encrypted tunnels or other cryptographic measures.

In this figure all host device has AIDPS installed and is connected to database present with administrator. Database contain information about all existing intrusion. Database provide regular updates to AIDPS. It

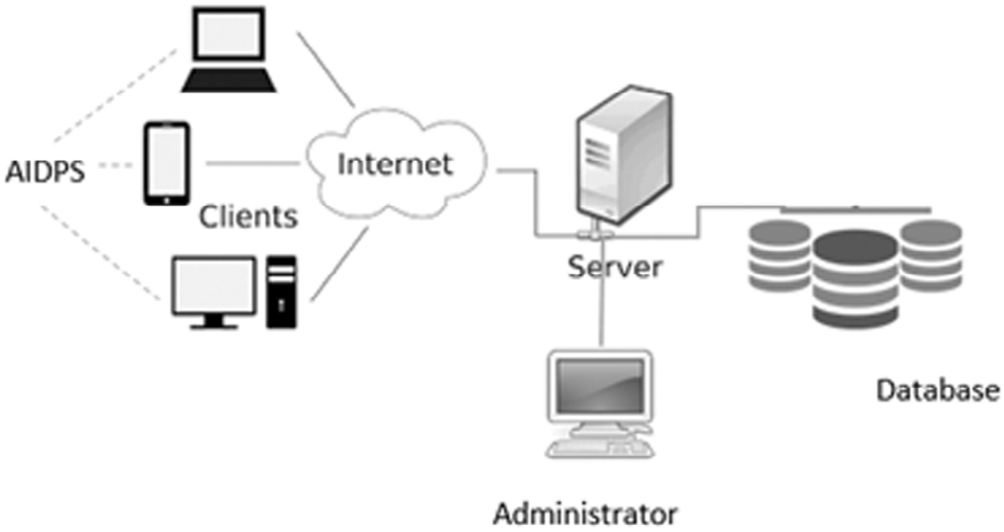

Figure 4: Application Based IDPS

uses these update in scanning and finding similar thinks (code, instruction, configuration and software) if it finds something it list them and send that list to administrator. And give a unclear tag to that host's device.

For informing administrator 5 types of notification or messages are used: -

Type 1: Show that there is malicious thing present in host device and the list of all the malicious thing that are harmful or malicious.

Type 2: Show that host is using that malicious software and also tell admin about frequency of using that software and what all activity host is performing while using them, but that activities are not harmful for network.

Type 3: Show that host is doing some malicious activities but that don't effect or intruding network working.

Type 4: Show that host is doing some malicious activities that can effect or intrude network working.

Type 5: Show that host malicious activities are causing intrusion in the network and administrator must have to act to stop/prevent from malicious activity.

By these notification administrator gets informed about what all is going inside his network. Admin gets information about host activities and if required admin can take action against the host to prevent network form any intrusion. Action can betaking the network down or a warning massage can be send to host to stop malicious activities. This way action can be taken instead of waiting for an attack to happen and put all resources to stop.A spy on host will do all the work, IDPS can inform administrator in advance that this all host are doing malicious activity and admin can take action in advance before any intrusion is generated to safe guard his network.

This application based IDPS can be used to scan the host devices to check for malicious hidden software placed by cracker to get host information.This hidden software can be detected by scanning the incoming and outgoing data packets by network based IDPS for checking their origin.Application based IDPS can recognize which application or software is generating that packet by checking port number of packets and that application can be taken down by AIDPS.

4. ARCHITECTURE / WORKING PRINCIPAL OF PROPOSED MODLE

AIDPS is installed in every host device. AIDPS is connected to a database that contain all information about malicious software, their configuration and specific hardware used in generating intrusion.

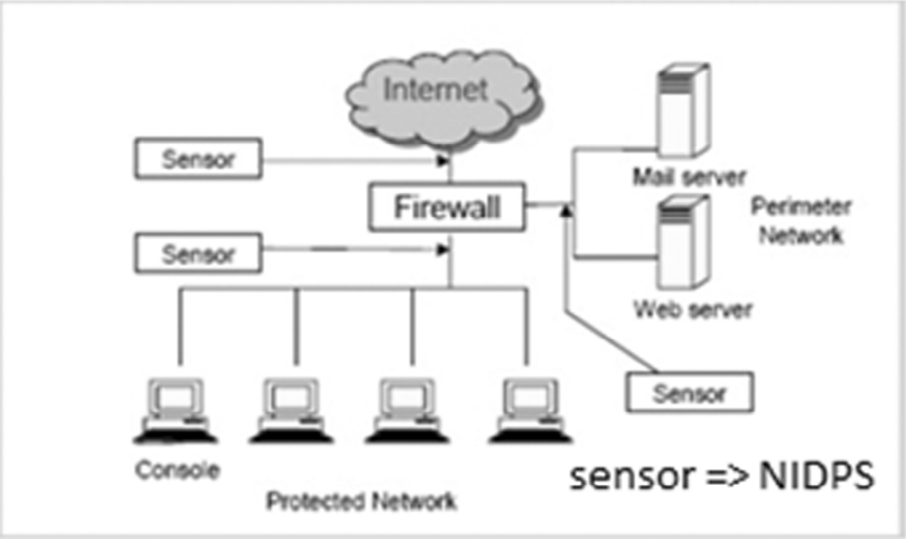

Figure 5: Network based IDPS

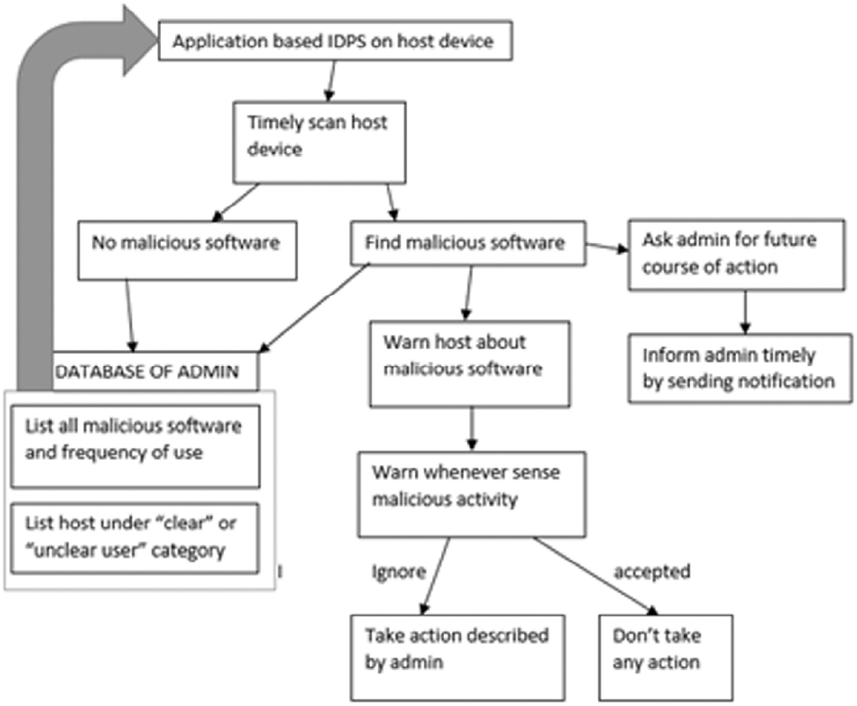
Application based IDPS on host device
Timely scan host device
No malicious software
Find malicious software
Ask admin for future course of action
DATABASE OF ADMIN
Warn host about malicious software
Inform admin timely by sending notification
List all malicious software and frequency of use
Warn whenever sense malicious activity
List host under "clear" or "unclear user" category
Ignore
accepted
Take action described by admin
Don't take any action

Figure 6: Flow Chart of AIDPS

Administrator has to keep this database updated.AIDPS will scan host device and list all the malicious software present in host by matching information in that databaseand will inform the host about that software and ask the host which all software he wants to remove. AIDPS put that host under "unclear list" in admin's user database. AIDPS ask admin about certain future course of action incase AIDPS sense that host activity can harm network then AIDPS is ready with some prescribed action to prevent from intrusion, as it take time to notify admin about detected intrusion and wait for admin action to prevent from intrusion.

This AIDPS will give complete freedom tothe host to do anything but AIDPS keep track of host malicious activities and timely warnthe host. Incasehost is doing any wrong activity, then Administrator is informed by different types of message. Administrator can set certain security parameter in AIDPS that if host is doing these activities very frequently then those parameterswill be used to stopthe host. AIDPSwill regularly check host devices for malicious software. If host deploys any intrusion, AIDPS will stop that intrusion and removethe software from host device which is involved in generating intrusion automatically without host permission. AIDPS sends host profile, location of host, software used by host, and log file of device to administrator confirming that host tried to intrude in network working. Then admin will take the necessary action against host activity.

5. SIGNIFICANT OF PROPOSED RESEARCH

Application based intrusion detection and prevention system will work as an antivirus with many additional features,when installed in every host device. It will warn host from doing any malicious activity, protect it from any malicious software or activity performed on his/her device without host knowledge and prevent network from malicious activity done by host. It will sense before intrusion is actually lunched on network and perform action which was imposed by admin in case any wrong think happens in that particular host device or in that network.

6. COMPARISON & RESEARCH ANALYSIS

AIDPS will work more effectively as it will able to detect and prevent from more intrusion in the network, as it will not allow host to generate intrusion, if host get successful in creating intrusion but AIDPS will not allow host

Table 1
Difference between IDPS and AIDPS

IDPS	*Application based IDPS*
It can be network and host based	It is host based only
First detect then try to minimize the impact of intrusion .	It know about intrusion, at the time it is created but not yet deployed.
It can only try to prevent or stop intrusion, not 100% Shure to prevent from intrusion	It will stop intrusion as soon as intrusion is created as it keep a close check on host activity
Communication between IDPS and database is not encrypted	Communication between AIDPS, database, and admin is encrypted
It support static policies	It support dynamic policies
It send frequent false alarm	It sends notification with 5 different massage type.
It may miss intrusion	It can't as AIDPS know which all software with what all configuration is used to generate an intrusion
It scan incoming and outgoing packets.	It scans host devices for suspicious software, codes, configurations.
Admin set prevention step in general.	admin know what type of software host use for malicious activity so admin can set specific prevention steps.

Table 2
Research Analysis

Parameter	*IDS*	*IPS*	*Proposed AIDPS*
security solution type	Passive security solution	Active security solution	Active security solution
Scanning bases	Scan whole packet and based on policy	Scan whole packet and based on policy	Scan whole device (hardware and software) based on policy that are updated.
Job	Filtering, blocking, allowing of addresses, ports, services	It will filter, scan, start alarm and then take prevention action.	Scan host devices and then delete/ disable all malicious software present in host device by taking permission from host. Take prevention step when detect any intrusion .
Actions	Drop or allow packets and generate logs	Drop or allow packets, block certain traffic to access network and generate	Notify user as well as admin and take predetermined step defined by admin that is to block user or destination traffic or to drop whole traffic coming from particular location .
Hardware scanning	No	No	Yes
Network scanning	Yes	Yes	No
Alarm	Yes	Yes	Yes
Software scanning	No	No	Yes
Network packet scanning	Yes	Yes	Yes
problems	High false alarm ratio	It cannot detect a signature split over multiple TCP packets	Regular notification about host illegal activities to admin.

to deploy that intrusion AIDPS will follow prevention step set by admin for that particular host. As compared to IDS, IPS, IDPS, they will try to stop and take preventive step to minimize the effect/loss by intrusion.

Table 1 show AIDPS is more advanced and can detect and elements more intrusion than IDPS. The working of AIDPS is different and more suitable to catch more intrusion than on going IDPS technology.

Table -2 show difference between IDS , IPS , AIDPS.

6. CONCLUSION

AIDPS will not prevent host from using malicious software, it will only warn host that software used by host is malicious and user must stop using this type of software otherwise strict action can be taken by admin against host. Host is free to do whatever he/she want to do but by keep this in mind that his/her activity will not affect network or create any intrusion in the network. Application based intrusion detection and prevention system's warning may make the host to close that software but if host don't stop doing that malicious work then AIDPS use those prevention methods which are predefined by the administrator to safe guard the network.

AIDPS run inside every host device and keep a close look on host activities. It scans host devices looking for malicious software, abnormal configuration and software that are installed by remote attacker, it also tries to analysis the change in behavior of host.

REFERENCES

[1] Lap T. Huynh, and Linwood H. Overby, Jr, Application based intrusion detection system, patent No.: US 8,925,081 B2, Date of Patent: Dec.30,2014

[2] Michael Scheidell, Intrusion detection system, Patent No.: US 7,603,711 B2, Date of Patent: oct,13,2009

[3] IDS [online], available: https://en.wikipedia.org/wiki/Intrusion_detection_system

[4] IPS [online], available: https://en.wikipedia.org/wiki/Intrusion_prevention_system

[5] IDS [online], available: http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp

[6] Application based IDS [online], available: http://archive.oa.mo.gov/itsd/cio/architecture/domains/security/CC-ApplicationBasedIDS040303.pdf

[7] Application based IDS [online], available: http://searchnetworking.techtarget.com/tip/Application-specific-network-intrusion-detection-systems-emerge

[8] Host based IDS [online], available: https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system