ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

# Classification of Intrusion Detection System and its Methodologies

[1] Rahul Chandra Reddy Karne, [2] Pasham Akhil Kumar Reddy, [3] Ms. G. Pratibha
[1][2] B.E. Student, [3] Asst. Professor
[1][2][3]Department of Computer Science and Engineering, Matrusri Engineering College, Saidabad – 500059

***Abstract:*** **The process of monitoring the network traffic within a host or on a network and detecting any unwanted or malicious traffic that might have crept in, is known as Intrusion Detection. An IDS may either be a piece of software or hardware appliance that keeps an eye on real-time network traffic so as to ascertain unwanted activities and occurrences such as illegal and vicious traffic, traffic that breaches established security policy, and traffic that violates passable use policies. This paper aims at delivering i) a general concept of types of IDS, pros and cons of the various available IDS ii) a description of different features of the IDS and IPS iii)attacks on IDS and how to evade IDS exploiting various security loop-holes. An IPS is a type of IDS which usually logs activities and identifies malicious activity which is reported so as to enact necessary counter measures.**

***Index Terms*— HIDS, IDS, IPS, NBA, NIDS**

## I. INTRODUCTION

The responsibility of IDS is to gather and analyze various activities on a system or a network it is monitoring. IDS logs information about the activity and alert the administrator of any unusual, suspicious activity. The IDS detects the type of activity depending upon where the sensor is placed. IDS assist information systems to prepare and deal with attacks. Various organizations use IDS for different purposes such as determining problems with security policies, logging risks, avoiding individuals from breaching security policies. IDSs have become a need of every organization to enhance their security infrastructure.

This paper is structured is as follows; Section II discusses different techniques of IDS, Section III discusses various Intrusion Detection Methods, Section IV discusses different IDS components, Section V gives a brief idea about IDS architectures, Section VI discusses various IDS tools and Conclusion.

## II. TECHNIQUES

There are different types of IDS technologies due to the difference in their network configurations. Each technique has its own benefits and obstacles in configuration, detection, and cost. There are three different types of IDPS technologies which are basically differentiated by the events they monitor and the ways in which they are deployed.

### *2.1 Network-Based IDS*

A network based intrusion detection system (NIDS), may be deployed as its own network device or as software on a system. NIDS is a ordinary type of IDS that examines network traffic at all layers of Open Systems Interconnection (OSI) model that pass across the network, monitors and makes decisions about the traffic, suspicious activities, logs the details of activity and sends an alert to the administrator. It also performs analysis for whole traffic throughout the entire Subnet. Many NIDPSs can be deployed at a specific place in a network from where it is viable to monitor the traffic going into, out of a particular network segment. To determine whether an attack has happened or is underway, NIDPS equates measured activity to known patterns on lore database. They are commonly deployed at a boundary between networks such as firewall or routers, VPN servers, Remote access servers, when deployed next to a switch, hub or any other port also known as switched port analysis (SPAN), it is a configured connection on a network hardware which has the ability of monitoring all the traffic that moves through the entire device. They are easy to deploy on a network and can view logs in many systems at once. NIDs are passive IDS. The NIDPS are capable of detecting wide range of attacks than HIDS, but requires more configuration and maintenance.

### *2.2 Host-Based IDS*

HIDS are commonly implemented on sensitive hosts such as public accessible servers which contain sensitive information. HIDS can be used to defend attacks which are

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

cannot be detected by NIDS. Most HIDS mechanisms usually include inspection of events that occur on a specific host. These are not commonly used due to the overhead they incur. HIDS which runs on an individual host on a network keeps track of the inbound and outbound packets from the host and alerts the administrator in case of any suspicious activity detected in the network. In HIDS, the host is left to be in learning mode as it has to differentiate between good and bad behavior. When the erudition of good behavior is done, it is switched to detection mode and any activity or event that does not match the good behavior will trigger an alarm to report the administrator. HIDS inspects TCP/IP packets and helps us to know which traffic is assessing the network, the kind of activity that involves updating or modifying the server. NIDS cannot analyze traffic in an encrypted tunnel and we cannot detect malicious activity. HIDS is basically a host-based software solution. HIDS has better performance and reliability than any hardware solution and is also viable due to its low cost. It is a good layer of security defense.

### *2.3 Network Behaviour Analysis System*

NBAs catechize network traffic or statistics on traffic to distinguish uncommon traffic flows such as DDOS attacks, some types of malwares like backdoors and other privacy violations. This approach is used to sense attacks based on what the attacker intends to do, rather than whether their code equals patterns used in a distinct past event. NBAs' usually have sensors and consoles. NBA sensors are more commonly available as hardware appliances, some are similar to network based IDPS sensors. NBAs require multiple sensors to generate a good snapshot of a network and require benchmarking to judge the nominal quantity of segment traffic. NBA sensors do not watch networks directly but they depend on network flow data is delivered by routers and other networking devices.

## III. INTRUSION DETECTION METHODS

### *3.1 Signature Recognition*

Signature Recognition which is also known as misuse detection, identifies actions that indicate misuse of a system resource using a signature based IDS which has a signature file that lists what is considered as a supposed malicious activity. When the IDS detect any unusual activity it equates the activity with the database and if a match is found it alerts the administrator for an intrusion. Signature Recognition is not efficient against zero day attacks and the database should be updated frequently. This system generates few false positives, it means that few false alarms are generated which is considerably good for an IDS.

### *3.2 Anomaly-Based Detection*

In an anomaly-based system, the system initially understands what is a normal activity is and considers anything aberrant to be a malicious activity. The anomaly-based monitoring system is used to determine the baseline from the behavior of the user using the system. It is also known as behaviour -based anomaly monitoring system. Anomaly based detection is effective at spotting behaviour that is distinct from the usual activity of the user. The advantage of using the behavior-based anomaly system is that you do not need to configure a definition file of a known malicious activity; the system adapts users' activity and treats any other activity as malicious. The intrusion is detected based on the fixed behavioral traits of the users and components in a computer system. Anomaly-based IDPS frequently generates many false positives because of more diverse or dynamic environments. The major advantage of the anomaly based systems is that they have a good potential in detecting new kind of threats.

### *3.3 Stateful Protocol Analysis*

It is a procedure of equating predestines profiles of generally accepted definitions of protocol activity for protocol state against observed events to identify deviations. They rely on vendor developed profiles that specify how a protocol should be used. The main disadvantage of this method is that it is very resource intensive in nature and it cannot detect attacks that do not cause the violation.

## IV. IDS COMPONENTS

An IDS consists of management servers, sensors, large collection of consoles and database servers. All these components are commonly used in every IDS technology except for the sensors.

### *4.1 IDS sensor*

The sensor is generally placed on the network; it sniffs the network and listens to the network traffic. It is responsible for capturing packet and transmitting them to the console. A sensor acts similar to a sniffer.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

### *4.2 Management server*

The main objective of a management server is to process and analyze the data sent from the sensors. Some of the systems execute and carry out analysis on the event information that the sensors provide and identify events that an agent and individual sensors cannot. Management servers are available as appliance and software only products.

### *4.3 Database and Storage components*

It performs trend analysis, stores the IP address and other information about the attacker. This acts as a data warehouse for event information recorded by the sensors. Many IDSs support database servers.

### *4.4 Console*

The console plays the role of central administration for IDS system. With the help of a console, an administrant may view any current attack alerts. Console software is generally installed on to a desktop system. Some IDS consoles provides both administration and monitoring abilities

## V. IDS ARCHITECTURE

### *5.1 Host-Based IDS Architecture*

Most Host based IDPS systems have detection software installed in them, they are known as agents. An agent monitors activity on a host and transmits the data to management servers. Every agent is configured or designed to protect server, a client-host (personal computer) and an application service. Host based IDPS agents are commonly deployed to critical hosts such as publicly accessible servers which contain sensitive information. Different types of agents are available in the market that could protect laptop/desktops, organization servers and most agents support multiple operating systems. Certain organizations use host-based IDPS agents primarily to examine activity that cannot be monitored by any other security regulators.

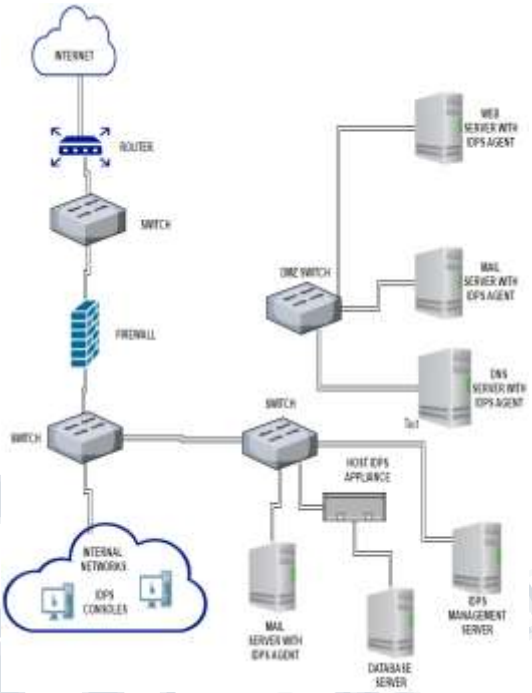


*Fig1: Host Based IDPS Agent Deployment Architecture*

### *5.2 Network Behavior Analysis (NBA) System Architecture*

NBA is basically a network-based IDPS solution. NBA solutions generally make use of various consoles and sensors in it. Some products also use analyzers also known as management servers. Usually these sensors are available as appliance. Most NBA sensors are deployed in passive mode. NBAs use the connection methods used in network based IDPSs such as a spanning port, network tap. Some sensors are very similar to network based IDS sensors which sniff packets to monitor network activity. Other sensors do not monitor the traffic directly but they can monitor by relying on network flow provided by the routers or any other networking devices such as switches. Conventional flow data particularly pertinent to IDS include

- IP address of source and destination
- TCP or UDP ports of source and destination
- Number of packets transmitted in a session
- Timestamps for start and end of a session

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

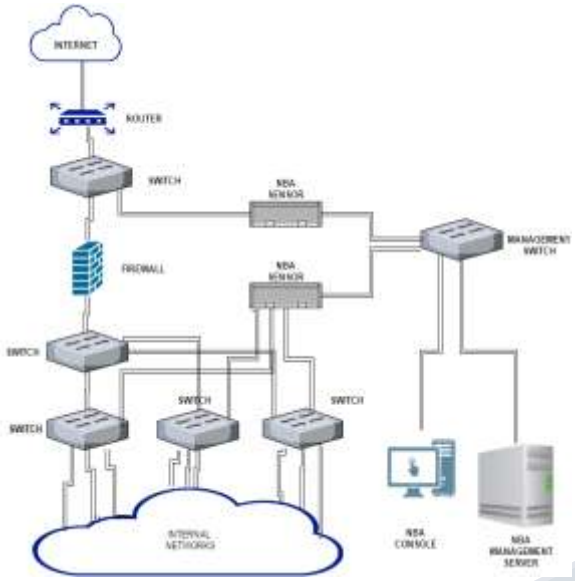


*Fig2: NBA Sensor Architecture*

Similar to a network based IDPS; a management network can be used for NBA component communications. Passive sensors that have the capability of performing direct network monitoring abilities should be used because they can monitor key network locations like demilitarized zone subnets and divisions between networks etc. Inline sensors are meant to be deployed in close range within the perimeter firewalls. They are generally placed between firewall and the internet border router. This action will limit all the incoming attacks that could devastate the firewall.

***5.3 Network based IDS Architecture***

A network based IDS consists of management servers, sensors, large collection of consoles and database servers. All these components are commonly used in every IDS technology except for the sensors.

***Sensor***

A network based IDS sensors records and monitors network activity on a network segment. An IDS sensors records and monitors network activity on a network segment. Most IDS deployments have multiple sensors placed in them. Sensors can be used in two formats

***Appliance***

An appliance based sensor consists of special software and a hardware piece for its sensor. It uses a customized and hardened operating system.

***Software only***

Software developers sell sensor softwares without an appliance. Administrators can install the software onto their hosts. Sensor software includes customized operating systems that can be installed on a user operating system sensors can be deployed in two ways

***Inline mode***

The main objective of deploying IDPS inline sensors is to stop attacks by blocking network traffic. An inline sensor is deployed so that the whole network traffic is passed through it just like a firewall. Some inline sensors may be hybrid IDPS devices or just simple IDS. These sensors are often placed in secure side of a network so that they can have less traffic to filter.

***Passive mode***

A passive sensor monitors a duplicate copy of the actual network traffic. Passive sensors are commonly deployed to monitor main network location such as activity on a demilitarized zone subnet (DMZ). Passive sensors use several methods to monitor traffic some of them are

***Spanning port***

Spanning port is a special port sees all the traffic passing through the switch. A sensor when connected to a spanning port allows it to watch incoming and outgoing traffic from many hosts. Spanning ports are resource intensive in nature. A switch must have several technologies like network forensic analysis tools, IDS sensors, monitoring tools to monitor traffic.

***IDS Load Balancer***

It is a device that collects and directs all the network traffic to monitoring systems. Some of the devices available in the commercial market can split the traffic across ten or more sensors. This device can admit copies of network traffic from one or more spanning ports or aggregate traffic in different networks. The load balancers then distribute copies of traffic to monitoring systems based on a set of rules configured by administrator. **[**1**][**3**]**

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

***Network tap***

It is a direct connection between a sensor and physical network media. The sensor is provided with a copy of all the traffic carried by the physical media by the tap. Network taps are generally purchased as an add-on to a network. The main drawback of a network tap is, configuring a network tap generally involves some network downtime.

The figure-3 below states the architecture of a passive network based IDPS sensor. Another way of improvising the IDPS security is to create a virtual management network using a VLAN within the network. VLAN provides protection for IDPS communication but not as better protection as a separate management network can provide. The main drawback of using a management network is it's expensive to deploy.

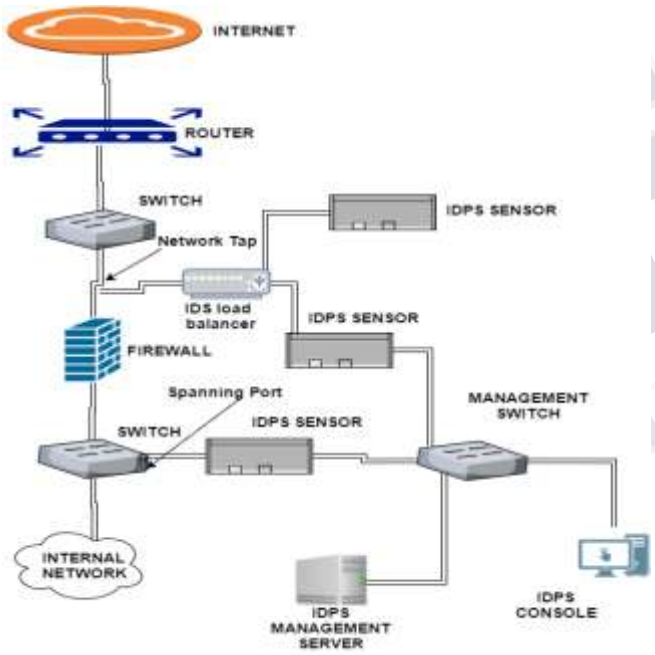


***Fig3: Passive Network-Based IDPS Sensor Architecture***

## VI. IDS TOOLS

***6.1 AIDE- Advanced Intrusion Detection Environment***

It is a file and directory integrity checker which creates a database from the regular expression rules it can find from the config file(s). Once the database is started it can be used to verify the integrity of the files. All of the usual file attributes can also be verified for any irregularities. It is highly multi threaded, scalable and has protocol identification. It supports plain text configuration files and database for simplicity. It supports various message digest algorithms like sha512, crc32, sha1, tiger, sha256, rmd160, md5.

***6.2 Bro network security monitor***

Bro is a powerful network analysis framework that very much differs from the typical IDS which targets high-performance networks and it is used functionally at various large sites. It comprehensively logs what it sees and provides a high-level archive of a network's activity. Bro does not rely on traditional signatures and is not restricted regarding detection approach. Bro keeps extended application-layer state about the network it monitors.

***6.3 Cisco IPS***

The Cisco Intrusion Prevention System (IPS) defends the entire network with a range of deployment options and delivers comprehensive network-wide security defense. This inline, IPS defines, classifies and stops known and unknown threats to a network, which includes directed attacks against servers, clients, applications and infrastructure components and malware. This refined protection can be easily deployed as a module in a switch or router or as a standalone appliance.

***6.4 IBM Security Network Intrusion Prevention System***

IBM Security Network Intrusion Prevention System appliances are primarily designed so as to constantly stop threats which are evolving before they impact your business. It provides both high levels of protection and performance lowering the overall cost and complexity. It protects business-critical assets such as servers, endpoints, applications from different malicious threats and networks.

***6.5 OSSEC***

OSSEC actively monitors all aspects of UNIX system activity with log monitoring, root check, file integrity monitoring, and process monitoring. When a system is attacked OSSEC alerts administrator through alert logs and email alerts. OSSEC also exports alert to any SIEM system via system log so the user can get insights into their system security events and also real-time analytics.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

### *6.6 Outpost Network Security*

Outpost Network Security is especially designed for small and medium business organizations for protection against modern security challenges and to address the problem of productivity waste. ONS safeguards office networks against internal sabotage and external attacks, spyware activity, blocking aggressive web content, stopping data transfer to non-authorized USB devices, keeps PCs clean of malware and. ONS brings manageability, transparency and security to your IT infrastructure, keeping administrators non-overloaded and workstations healthy.

### *6.7 SNORT*

SNORT is a very powerful open source signature based IDS. It is capable of performing real-time traffic analysis on IP networks. It can be used as a straight packet sniffer like TCP dump packet logger IPS. It can perform content matching and can also be used to detect various ranges of attacks such as buffer overflows, probes, port scans, OS finger printing attempts, CGI attacks. SNORT firstly sniffs packets using a library named libpcap. After packets have been captured they are passed to the packet decoder. It translates specific protocol elements into internal data structure. After the initial stage of packet capture and decoding is completed, the traffic is then handled by preprocessors. The preprocessors examine the packets carefully before handing them to the detection engine. This engine performs test on packets to detect any intrusions. The last module is the output; it generates alerts of any suspicious activity. Snort supports TCP, UDP and ICMP protocols. Basically SNORT can be used in four different modes

- Sniffer mode
- Packet logger mode
- IDS mode
- IPS mode

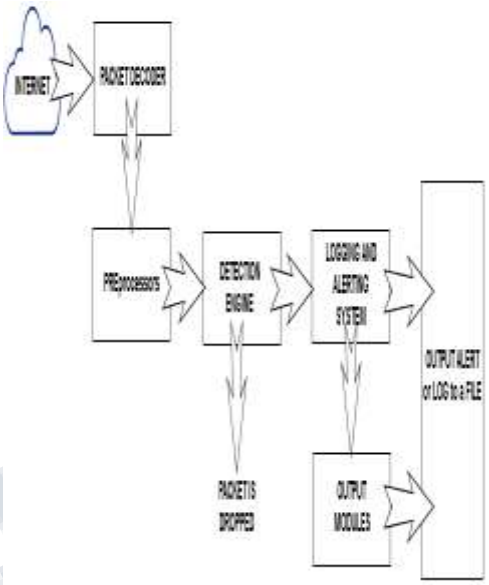


*Fig-4: SNORT Component Structure*

SNORT analysis the packets and also shows the statistics of the packets analyzed. It also shows the packet breakdown count by protocols. It shows the action statistics, alerts and logs.


*Fig-5: SNORT Network Traffic Statistics*

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 8, August 2016

When SNORT detects any bad traffic it generates alert of any suspicious activity and then logs the IP address of the attacker.

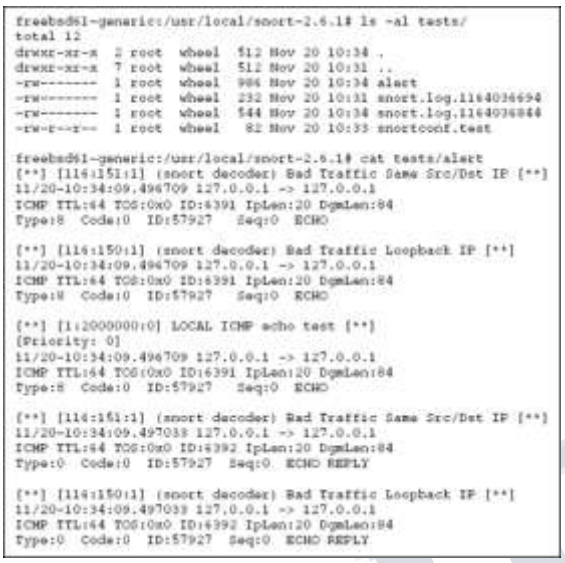


***Fig-6: SNORT Bad Traffic Detection Alert***

## VII. CONCLUSION

This paper gives a basic idea about different types of IDS, their life cycle, various domains, types of attacks and tools. IDS are essential for various network companies and corporate sector. IPS defines the prevention measures for the security. Different techniques use different approaches for intrusion detection. The IDSs mentioned above are still not efficient enough and hence cannot be relied upon completely and some of them are difficult to maintain. They still have to be enhanced in their functionality and efficiency guarantee a flawless security for a network. Since system security cannot be avoided, even with a little functionality it is strongly recommended to use a combination of various available IDSs. As technology is always in developing stage, this paper can be used as a guide to trigger more research in network security as there is an untapped potential for research in this area. Further much work should be done in this area.

## ACKNOWLEDGEMENT

We would like to extend our sincere thanks to the management of Matrusri Engineering College, Saidabad, Hyderabad, our guide Ms. G. Prathiba, M.Tech, (P.h.D)., Asst. Prof., Department of Computer Science & Engineering, Matrusri Engineering College.

## REFERENCES

[1] Susan Hansche, "Official (ISC)$^{2®}$," Guide to the CISSP® -ISSEP®.

[2] Michael E. Whitman, Herbert J. Mattord, "Principles of Information Security," Fifth Edition, pp 355-389, 2015.

[3] Karen Scarfone, Peter Mell, Guide to Intrusion detection and prevention systems (IDPS), NIST, 1 to 127, 2007.

[4] Sans institute infosec reading room, Understanding Intrusion Detection System, Internet, Sans Institute, 1 to 9, 2001.

[5] B. Rajul and B. Srinivas, Network Intrusion Detection System Using KMP Pattern Matching Algorithm, IJCST, 33-36, January 2012.

[6] David Geer, Behaviour-Based Network Security Goes Mainstream, IEEE, 14-17, 1-5.

[7] Michael Gregg and Billy Haines, CASP: CompTia Advanced Security Practitioner Study Guide, pp.135-137, 2013.

[8] Glen E. Clarke, CompTIA Security+ Certification Study Guide, Second Edition, pp 348-357, September 2014.

[9] Langin, C. L. A SOM+ Diagnostic System for Network Intrusion Detection. Ph.D. Dissertation, Southern Illinois University Carbondale, 2011.

[10] F. Cikala, R. Lataix, S. Marmeche", The IDS/IPS. Intrusion Detection/Prevention Systems ", Presentation, 2005.

[11] Tiwari Nitin, S. R. Singh and P. G. Singh, Intrusion Detection and Prevention System (IDPS) Technology-Network Behavior Analysis System (NBAS), International Science Congress Association , 51-56, July 2012.