International Journal of Innovative Research and Advanced Studies (IJIRAS)
Volume 4 Issue 2, February 2017

ISSN: 2394-4404

# Complete Study Of Intrusion Detection System

**Miss Ankita B. Palekar**

**Dr. S. S. Dhande**

Department Of Computer Enginnering,
Sipna COET, Amravati University

***Abstract:*** *Intrusion detection is one of the popular techniques for preventing information in the systems. .Intrusion Detection System (IDS) is a software application which look over the network or system activities. It detects harmful activities that occur huge growth and usage of internet is responsible to protect and communicate with the digital information in a safe manner. Currently, for getting the valuable information, hackers make use of different types of attacks. There are many intrusion detection techniques, methods and algorithms help to detect such type of attacks. This thesis is about the definition of intrusion detection, history, types of intrusion detection system, types of attacks, different tools and techniques and need & challenges. The main goal of this paper is to provide a complete study of intrusion detection system.*

***Keywords:*** *Intrusion detection system, IDS attacks, Functionality, Tools, Techniques*

## I. INTRODUCTION

An Intrusion Detection System is a system used to watch over the network and protect it from the attacker with the fast growth of internet based technology new application areas for computer network have come forth. e.g, the fields like business, financial, industry, security and healthcare. All of these application areas were responsible for making the network as a target for the abuse and a big susceptibility for the entire community. The aim of intrusion detection is to look over the network assets to find abnormal behaviour and misuse of network. Intrusion detection system was discovered in early 1980's after the evolution of internet. Several events in IDS technology have advanced intrusion detection to its current state, Since then there was a quick rise in reputation and incorporation in security foundation. As a result audit data and its importance led to horrific improvements in the subsystems of every operating system. IDS and Host Based Intrusion Detection System (HIDS) were first defined in 1983. Around 1990s the turnovers are generated and intrusion detection market has been raised. Real secure is an intrusion detection network developed by ISS. After a year, Cisco acknowledge the importance for network intrusion detection and purchased the Wheel Group to accomplish the security solutions. To collect data, unauthorised users or hackers use the organization's internal systems which cause su-acceptability like Software bugs, temporary failure in administration. As the internet entering into the society, new dangerous items like viruses and worms are imported. Hence, security is important for the users to save their system from the attacker. Firewall technique is one of the popular protection techniques and it is used to save the private network from the public network. IDS are used in network related activities, medical applications, technical frauds etc.

## II. INTRUSION DETECTION SYSTEM

An IDS is referred as warning device such as burglar alarm. For example the lock system in the shop which protects the shop and goods in the shop from theft. But if somebody breaks the lock system and tries to enter into the shop, it is the burglar alarm that detects that the lock has been broken and alerts the owner by ringing an alarm. Moreover, Firewalls do a very good job of separating the incoming traffic from the Internet to avoid the firewall. e.g. external users can connect to the Intranet by dialling through a modem established in the private network of the organization this kind of unauthorised access cannot be detected by the firewall. Network traffic flows audits by an Intrusion Prevention System (IPS) to detect and prevent vulnerability exploits. There are two types of prevention system they are Network (NIPS) and Host (HIPS). These systems look over the network traffic and automatically take actions to save networks and systems. IPS issue have false positives and negatives. In False positive concept alarm is produced in IDS where there is no attack. In False negative concept alarm is not produced in IDS when there is an attacks takes place.

## III. TYPES OF IDS

There are three types of IDS:

- ✓ Host based IDS
- ✓ Network based IDS
- ✓ Application based IDS

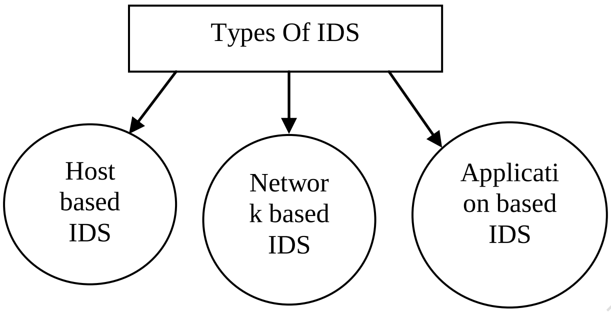

*Figure 1: Types of IDS*

### A. HOST BASED IDS

For doing analysis we can use host system's logging and other information. Host based handler is considered as sensor. Other sources, from which a host-based sensor can obtain data, include system logs and other logs generated by operating system processes. Host based system trust strongly on audit trail. The data grant the intrusion detection system to point out the complex patterns of misuse that would hidden at a higher level of abstraction. HIDS are used effectively for analyzing the network attacks, e.g. it can sometimes tell exactly what the intruder did, which commands he used, what files he opened, rather than attempt to execute a dangerous command.

Advantages of Host based Intrusion Detection Systems:

- ✓ Conform success or failure of an attack
- ✓ Watch over System Activities
- ✓ Analyse attacks that a network based IDS fail to detect
- ✓ No need of additional hardware
- ✓ Low implementation cost

### B. NETWORK BASED IDS

These systems gather data from the network itself rather than from each separate host. While packets moving across the network, the NIDS audits the network attacks. The network sensors occupied with attack signatures that are based on what will include an attack. Most network-based systems permit advanced users to define their own signatures. Attack on the sensor is depends on signature and they are from the previous attacks. The operation of the monitors will be open to the users and this is also important as the transparency of the monitors decreases the probability to locate it and ignores its capabilities without the efforts. Network Node IDS (NNIDS) agents are install on every host within the network being protected.

Advantages of Network based Intrusion Detection Systems:

- ✓ Low ownership cost
- ✓ Easy to install
- ✓ Verify network based attacks
- ✓ Real Time detection and quick response.
- ✓ Detection of failed attacks

### C. APPLICATION BASED IDS

(APIDS) will check the efficient behaviour and event of the occurrence of rules. The system or agent is act as a mediator between a process and group of servers that monitors and verifies the application protocol between devices. Intentional attacks are the harmful attacks done by bad tempered employees to cause damage to the organization and Unintentional attacks causes financial harm to the organization by deleting the important information in file.

### D. TYPES OF ATTACKS

There are 6 types of attacks

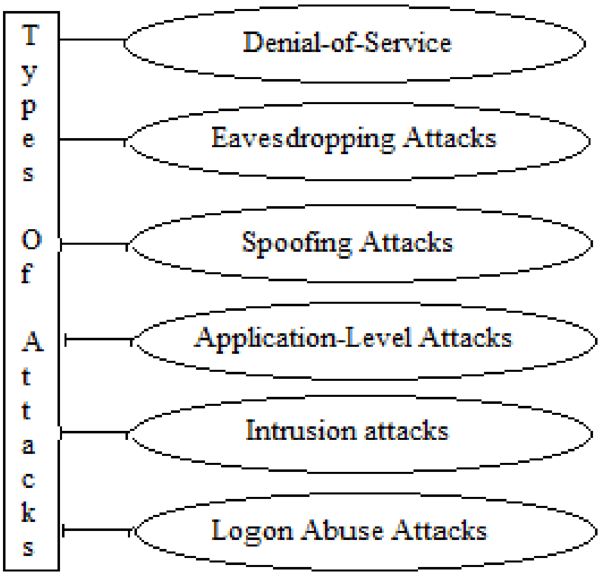

*Figure 2: Types of Attacks*

### A. DENIAL-OF-SERVICE (DOS) ATTACKS

It tries to not allow of the authorized users from attempting the requested service. An advanced Distributed Denial of Service occurs in a huge environment that the attacker sends or floods the server with so many connection that request to knock the target system.

### B. EAVESDROPPING ATTACKS

It is the scheme of illegal obstruction of opponent in communication by the attacker. This attack can be done over by telephone lines or through email.

### C. SPOOFING ATTACKS

This attacker describe as another user to get the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a authorised user and grant access to the attacker to attack.

### D. INTRUSION ATTACKS

An attacker tries to admit into the system or route through the network. Buffer overflow attack is a typical intrusion attack which happens when a web service got more data than it has been allowed to handle which is responsible to loss of data.

### E. LOGON ABUSE ATTACKS

A logon abuse attack would ignore the authentication and access control concept and permits a user with more advantages.

### F. APPLICATION-LEVEL ATTACKS

The attacker targets the disabilities of application layer. For example, security vulnerability in the web server or in faulty controls on the server side.

## IV. FUNCTIONS OF IDS

The IDS consist of four key functions namely, data collection, feature selection, analysis and action.

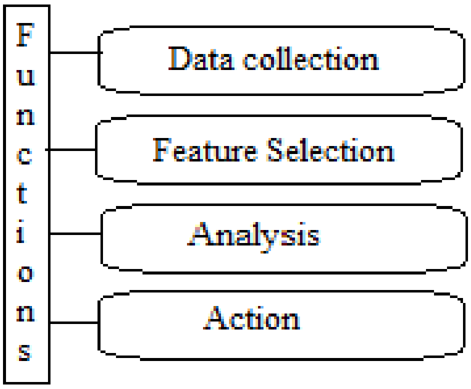

*Figure 3: Functions Of Ids*

### A. DATA COLLECTION

This module supplies the data as input to the IDS. The data is saves into a file and then it is verifies. Collection of the data packets were done by Network based IDS and collecting details like usage of the disk and processes of the system done by host based IDS.

### B. FEATURE SELECTION

To choose the particular feature huge data is available in the network and they are usually computed for intrusion. e.g., the Internet Protocol (IP) address of the source and target system, protocol type, header length and size could be taken as a key for intrusion.

### C. ANALYSIS

The data is verifies to find the correctness. The incoming traffic is examined against predefined signature or pattern by Rule based IDS.

### D. ACTION

It says about the attack and reaction of the system. It can either inform the system administrator with all the needed data through email or it can play an active part in the system by dropping packets so that it restricts the entry into the system or close the ports.

## V. IDS TECHNIQUES

There are 3 techniques of IDS

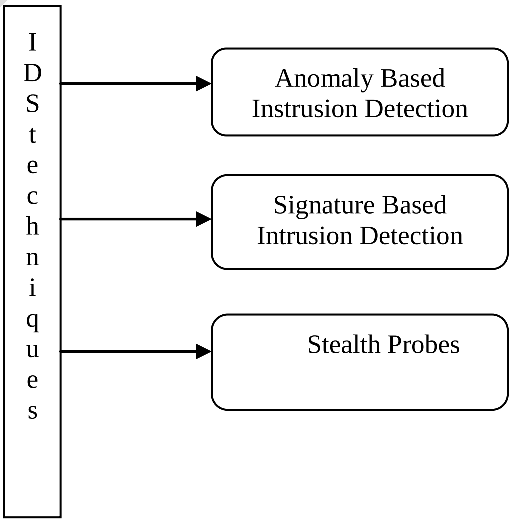
IDS techniques
Anomaly Based Instrusion Detection
Signature Based Intrusion Detection
Stealth Probes

*Figure 4: IDS Techniques*

### A. ANOMALY BASED INSTRUSION DETECTION

Anomaly is indicated as a thing which is away from main body. Anomaly detection technique is designed to reveal the patterns that are far away from the normal pattern. Anomaly detections are classified into static and dynamic detectors. Static anomaly detector is considered as a constant. The static part is classified into two parts that are system code and system data. Static portions of the system can be represented as a binary bit. If any changes from its original form is happened then the error has been indicated. or the burglar has reshaped the part of the system. In dynamic detector, the description of the system behaviour is included. The system behaviour is defined as an order of different actions. For example, IDS uses audit records that are generated by the operating system to define the actions of interest. In this case, the behaviour can be observed only when audit records are generated by OS and the actions are happened in strict series. Unexpected behaviour is considered as anomalous. If such type of behaviour happened then the system administrators may be alerted by false alarms. Anomaly detection is useful for detecting attacks like misuse of protocol and service ports, DoS based on functional virus, DoS based on volume (DDoS), buffer overflow etc.

*Techniques used in anomaly detection:*

There are number of actions and action counter are defined and have been implemented in anomaly detection.

### *a. COGNITION MODELS*

✓ *Finite State Machine:* A finite state machine (FSM) is a behavioural model which captures the states, transitions and actions. A state defines about the past information. An action is a description of an activity that is performed at a given time and the types of action are entry action, exit action and transition action.

✓ *Description Scripts:* Scripting languages determine the attacks on computer system and networks. All scripting languages are able to examine the series of specific actions.

### *b. STATISTICAL MODELS*

The statistical model gives the output as a statistical value. There are two types of statistical models, they are

✓ *Operational Model (or) Threshold Metric:* The actions that happened over a period of time regulate the alarm. For E.g. a user after n unsuccessful login attempts regulates the alarm. Here lower limit is 0 and upper limit is n.

✓ *Markov Process or Marker Model:* In this model the system is examine critically at fixed time interval.

## VI. SIGNATURE BASED INTRUSION DETECTION

Signature based intrusion detection is termed as misuse detection. Here consist of set of data. Each dataset has number of requests and every dataset must be tagged as normal or intrusive. The machine learning algorithms are used to teach the data set according to their tag. To detect the attacker, this technique automatically keep in use the signature. Misuse detection technique is created automatically. Depending on the quality of being robust and seriousness of a signature that is generated within the system, some alarm response or notification should be sent to the proper authorities.

Techniques used in signature based anomaly detection:

✓ *Expression matching:* It is the most easy & simple method in misuse detection. In this it searches for the series of actions like log entries for the occurrence of exact pattern.

✓ *State transition analysis:* This model attacks the state or the transitions in the network. Each action in the network is given as an input to finite state machine which gives output in transition.

### B. STEALTH PROBES

A stealth probe is a technique used to gather and binds the data. It tries to detect the attacks which takes a long time.

## V. TOOLS IN INTRUSION DETECTION

Today, the available intrusion detection tools points to the range of organizational security aims. These tools are as follows:

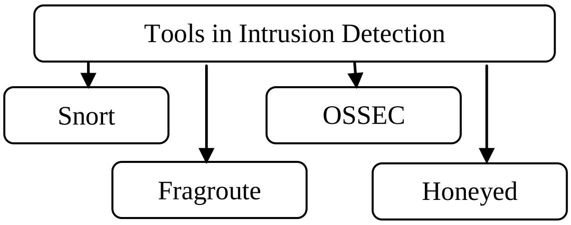

*Figure 5: Tools in Intrusion Detection*

### A. SNORT

Snort is open source & lightweight software. Snort uses a rule-based language to describe the traffic. From an IP address; it describes the packet in human readable form. Snort finds thousands of worms, susceptibility exploit attempts, port scans, and other harmful behaviour through protocol analysis, content searching, and various pre-processors.

### B. FRAGROUTE

It is termed as fragmenting router. Here, the IP packet is sent from the intruder to the fragrouter and they are then fragmented (broken into parts) and transformed to the party.

### C. HONEYED

Honeyed is a tool that produces hosts on the network. Honeyed permits a single host to send request to multiple addresses on a LAN for predicting actual network behaviour.

### D. OSSEC

OSSEC (open source security) is free open source software. It uses a Client/Server based architecture & can run on many operating system. OSSEC has the capability to send OS logs to the server for verification and storage. It is used in powerful log analysis engine, universities and data centres.

## VII. NEEDS AND CHALLENGES

✓ Each organization requires IDS which is treated as a defence tool.

- ✓ Currently, IDS technology itself is undergoing a lot of improvements. IDS technology does not require human participation. Today an IDS technology gives some advantages like notifying the administrator in case of detection of a harmful activity, avoid the harmful connection for a certain period of time. For each action that is going to be happened the IDS logs should be looked over.
- ✓ For IDS designing & implementation, planning is important. In most situations, it is better to implement a hybrid network of network based and host based IDS. The decision can vary between organizations.
- ✓ The ratio of sensor manager should be expressed at great approval. Before starting the IDS implementation, it is very significant to design and ignore false positives result.
- ✓ The IDS technology is still reactive rather than proactive.
- ✓ Signatures are described as a pattern of attacks. Whenever a different kind of attack is detected, the signature database needs to be updated and they must be stored in the database.

## VIII. CONCLUSION

The main motto of this paper is to provide an complete overview of the requirement and utility of intrusion detection system. This paper provide complete thesis about definition of IDS, history, types of IDS, types of attacks and tools & techniques, need & challenges. For day -to-day security in corporate world and for network users IDS is playing a very important role. IPS describes the preventive measures for the security. Still, there are many challenges to overcome. The techniques of anomaly detection and signature based anomaly detection are specially generated and more techniques can be used. Further Work can be done by comparing some popular data mining algorithms applied to IDS and improving a classification based IDS using selective feedback methods.

## REFERENCES

[1] "Gartner: Defining Intrusion Detection and Prevention Systems". Retrieved September 20, 2016.

[2] "Gartner report: Market Guide for User and Entity Behaviour Analytics". September 2015.

[3] Abdullah A. Mohamed, "Design Intrusion Detection System Based On Image Block Matching", International Journal of Computer and Communication Engineering, IACSIT Press, Vol. 2, No. 5, September 2013.

[4] Scarfone, Karen; Mell, Peter (February 2007). "Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Computer Security Resource Center. National Institute of Standards and Technology (800–94). Retrieved 1 January 2010.

[5] "NIST – Guide to Intrusion Detection and Prevention Systems (IDPS)" (PDF). Februar

[6] John R. Vacca (2010). Managing Information Security. Syngress. p. 137. ISBN 978-1-59749-533-2. Retrieved 29 June 2010.

[7] Tim Boyles (2010). CCNA Security Study Guide: Exam 640-553. John Wiley and Sons. p. 249. ISBN 978-0-470-52767-2. Retrieved 29 June 2010.

[8] Harold F. Tipton; Micki Krause (2007). Information Security Management Handbook. CRC Press. p. 1000. ISBN 978-1-4200-1358-0. Retrieved 29 June 2010.

[9] Mattord, verma (2008). Principles of Information Security. Course Technology. pp. 290–301. ISBN 978-1-4239-0177-8.

[10] Anderson, Ross (2001). Security Engineering: A Guide to Building Dependable Distributed Systems. New York: John Wiley & Sons. pp. 387–388. ISBN 978-0-471-38922-4.