A Survey On Intrusion Detection System

[1]Jayesh Surana, [2]Jagrati Sharma, [3]Ishika Saraf, [4]Nishima Puri,[5]Bhavna Navin
[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student
[1]Information Technology,
[1]SVITS, Indore, India

Abstract— **Intrusion Detection System (IDS) is meant to be a software application that is a security system which act as a protection layer for the infrastructure it also monitors the network and finds if any malicious operations occur. Exponential usage of internet results in raising the concerns about how to protect the digital information in a protective manner. Throughout the years, the IDS technology has grown enormously to keep up with the advancement of computer crime. Nowadays, hackers use different types of attacks for entering our computer's personal secured information. Many intrusion detection techniques, methods and algorithms will act as a shield towards these attacks. This main goal of this paper is to provide a complete study about the definition of intrusion detection, history, life cycle, and intrusion detection methods, types of attacks, different tools and techniques, challenges with its applications.**

Index Terms— *Intrusion detection, IDS attacks, Functionality, Life cycle, Tools, Techniques*

I. INTRODUCTION

An Intrusion Detection System is used to detect all types of malicious network traffic and computer usage that can't be detected by a conventional firewall. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware. Security is needed for the users to secure their systems from external unwanted force. Firewall technique is one of the popular protection techniques which is been used to protect the network. IDS are used in network related activities, medical applications, credit card frauds, Insurance agency.
An IDS is composed of the following three components:

Sensors: - which sense the network traffic or system activity and generate events.
Console: - to monitor events and alerts and control the sensors,
Detection Engine: - that records events logged by the sensors in a database and uses a system of rules to generate alerts from the received security events.
There are several ways to categorize an IDS depending on the type and location of the sensors and the methodology used by the engine to generate alerts. In many simple IDS implementations all three components are combined in a single device or appliance.

II. HISTORY

The main aim of intrusion detection is monitoring the network assets to detect anomalous behavior and misuse in network. Intrusion detection was first introduced in early 1980's after the evolution of internet. Since then, several events in IDS technology have advanced intrusion detection to its current state. James P Anderson's, a pioneer in information security and member of the Defense Science Board Task Force on Computer Security at the U.S. Air Force, produced "Computer Security Threat Monitoring and Surveillance," a report that is often credited with introducing automated IDS.
During the late 1980's, with a growing number of shared networks, enterprise system administrators all over the world began adopting intrusion detection systems. In the 1990's, IDS technology improved to address the increasing number and sophistication of network attacks. Big data also plays an important role in the growth and importance of intrusion detection today. The world's data doubles every 20 months, and as cloud-hosted databases expand exponentially, it's no wonder IDS is more important than ever.At Threat Stack, we're honored to play an important role in this evolution and to support the IDS community
There are a variety of tools providing a certain level of comfort with acceptable risks used in the defence and surveillance of computer networks. Defence-in-Depth is a term encompassing comprehensive analyst training, hardware deployed in strategic positions and a strong security policy necessary for achieving this objective. Every day, we have tools at our disposal to reach this goal. The aggregation of data comes from routers, the host itself, firewalls, virus scanners and a tool strictly designed to catch known attacks; an Intrusion Detection System (IDS).

III. INTRUSION DETECTION

Intrusion detection is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses *vulnerability assessment* (sometimes referred to as *scanning*), which is a technology developed to assess the security of a computer system or network.

IV. INTRUSION DETECTION SYSTEM

An IDS is referred as burglar alarm. For example the lock system in the house protects the house from theft. But if somebody breaks the lock system and tries to enter into the house, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm. Moreover, Firewalls do a very good job of filtering the incoming traffic from the Internet to circumvent the firewall. For example, external users can connect to the Intranet by dialing through a modem installed in the private network of the organization; this kind of access cannot be detected by the firewall.

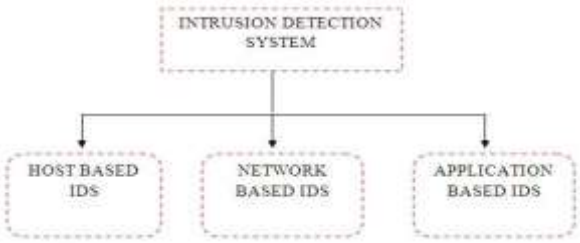

Figure.1. Types of Intrusion Detection System

Broad classification of intrusion detection system is:

A. Host based IDS

A Host Intrusion Detection Systems (HIDS) and software applications installed on host which are to be monitored. The agents monitor the operating system and write data to log files and/or trigger alarms. It can only monitor the individual workstations on which the agents are installed. Host based IDS systems are used to monitor any intrusion attempts on critical servers. Host based IDS views the sign of intrusion in the local system. Host based system trust strongly on audit trail. The information allows the intrusion detection system to spot subtle patterns of misuse that would not be visible at a higher level of abstraction.

Advantages of Host based Intrusion Detection Systems:

- Verifies success or failure of an attack
- Monitors System Activities
- Detects attacks that a network based IDS fail to detect
- Near real time detection and response
- Does not require additional hardware
- Lower entry cost

Drawbacks of Host based Intrusion Detection Systems:

- Difficult to analyze the intrusion attempts on multiple computers
- It can be very difficult to maintain in large networks with different operating systems and configurations
- It can be disabled by attackers after the system is compromised

B. Network based IDS

Network Intrusion Detection Systems (NIDS) usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode and a separate management interface. The IDS is placed along a network segment or boundary and monitors all traffic on that segment. These systems collect information from the network itself rather than from each separate host. The NIDS audits the network attacks while packets moving across the network. The transparency of the monitors decreases the likelihood that an adversary will be able to locate it and nullify its capabilities without the efforts. Network Node IDS (NNIDS) agents are deployed on every host within the network being protected.
Depending on how they function, network based IDS can be divided into two types:
Statistical anomaly IDS and Pattern matching IDS

Advantages of Network based Intrusion Detection Systems:

- Lower Cost of Ownership
- Easier to deploy
- Detect network based attacks
- Retaining evidence
- Real Time detection and quick response.

- Detection of failed attacks

Disadvantages of Network based Intrusion Detection Systems:

- Cannot analyze encrypted packet
- Requires access to all traffic to be monitored

C. Application based IDS

Application-Based IDS is a special subset of Host-Based IDS (HIDS) that analyzes the events transpiring within a software application. The most common information source for Application-Based IDS is the application's transaction log file.

Advantages of AIDS

- Aware of specific users
- Can observe interaction between application and user
- Able to operate when incoming data is encrypted

Disadvantages of AIDS

- More susceptible to attack
- Less capable of detecting software tampering

V. INTRUSION DETECTION ATTACKS

A. Denial-of-Service (DOS) Attacks

There are two main types of denial of service (DoS) attacks: flooding and flaw exploitations. Flooding attacks can often simply implement. For example, one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim. As another example, a SYN flood attack sends a flood of TCP/SYN packets with a forged source address to a victim. This will cause the victim to open half open TCP connections - the victim will send a TCPSYN/ACK packet and wait for an ACK in response. Since the ACK never comes, the victim eventually will exhaust available resources waiting for ACKs from a nonexistent host.

B. Eavesdropping Attacks

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

C. Spoofing Attacks

This attacker portrays as another user to forge the data and take advantages on illegal events in the network. IP spoofing is a common example where the system communicates with a trusted user and provides access to the attacker.

D. Intrusion attacks or User to Root Attack (U2R)

An intruder tries to access the system or route through the network. Buffer overflow attack is a typical intrusion attack which occurs when a web service receives more data than it has been programmed to handle which leads to loss of data.

E. Logon Abuse Attacks

A logon abuse attack would neglect the authentication and access control mechanisms and grant a user with more advantages.

F. Application-Level Attacks

The attacker targets the disabilities of application layer.

VI. FUNCTIONS OF IDS

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

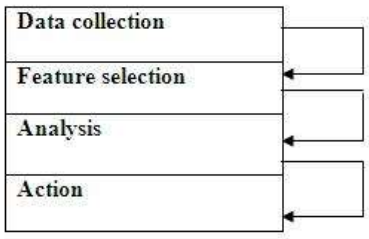

Figure 2. Functionality of IDS

A. Data collection

This module passes the data as input to the IDS. The data is recorded into a file and then it is analyzed. Network based IDS collects and alters the data packets and in host based IDS collects details like usage of the disk and processes of the system.

B. Feature Selection

To select the particular feature large data is available in the network and they are usually evaluated for intrusion. For example, 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 analyzed to find the correctness. Rule based IDS analyze the data where the incoming traffic is checked against predefined signature or pattern. Another method is anomaly based IDS where the system behavior is studied and mathematical models are employed to it.

D. Action

It defines about the attack and reaction of the system. It can either inform the system administrator with all the required data through email/alarm icons or it can play an active part in the system by dropping packets so that it does not enter the system or close the ports.

VII. IDS TECHNIQUES

A. ANOMALY BASED INTRUSION DETECTION

Also called behavior-based, these solutions track activity within the specific scope (see above) looking for instances of malicious behavior — at least, as they define it, which is a difficult job, and sometimes leads to false positives. For instance, outbound URLs of Web activity might be considered, and sites involving certain domains or URL length/contents might automatically be blocked, even though it's a human being trying to go there (not malware), and that user has a business-legitimate reason.

Techniques used in anomaly detection:

- Statistical Models
  a) *Operational Model (or) Threshold Metric:* The actions that occur over a period of time regulate the alarm. This can be visualized in Win2k lock; a user after n unsuccessful login attempts regulates the alarm. Here lower limit is 0 and upper limit is n.
  b) *Markov Process or Marker Model:* In this model the system is inspected at fixed time intermission. The behavior is detected as anomaly if the probability of the state is low.

- Cognition Models
  a) *Finite State Machine:* A finite state machine (FSM) or finite automation is a model of behavior captured in states, transitions and actions. A state defines about the past information. An action is a description of an activity that is to be performed at a given moment and the types of action are entry action, exit action and transition action.
  b) *Description Scripts*: Scripting languages characterize the attacks on computers and networks. All scripting languages are capable of examining the sequences of specific events.

B. SIGNATURE BASED INTRUSION DETECTION

Signature based intrusion detection is termed as misuse detection. This approach, also known as knowledge-based, involves looking for specific signatures that is byte combinations — that when they occur, almost invariably imply bad news. They generate fewer false positives than anomaly solutions because the search criteria is so specific, but they also only cover signatures that are already in the search database (which means truly novel attacks have good odds of success). Depending on the robustness and seriousness of a signature that is activated within the system, some alarm response or notification should be sent to the right authorities.

VIII. TOOLS IN INTRUSION DETECTION

An intrusion detection product available today addresses a range of organizational security goals. This section discusses about the security tools.

- SNORT

Snort is lightweight and open source software. Snort uses a flexible rule-based language to describe the traffic. From an IP address; it records the packet in human readable form. Through protocol analysis, content searching, and various pre-processors Snort detects thousands of worms, vulnerability exploit attempts, port scans, and other suspicious behavior.

- Suricata

Out of all the IDS/IPS systems that are currently available, Suricata competes most directly with Snort. This system has an architecture that is similar to Snort's, relies on signatures like Snort, and can even use the VRT Snort rules and the same Emerging Threat rule set that Snort itself uses. Being newer than Snort, Suricata has ways to catch up to in this area. If Snort isn't an option in your organization, this is the closest free tool available to run on an enterprise network.

- OSSEC-HIDS

OSSEC (open source security) is free open source software. It will run on major operating system and uses a Client/Server based architecture. OSSEC has the ability to send OS logs to the server for analysis and storage. It is used in powerful log analysis engine, ISPs, universities and data centres. Authentication logs, firewalls are monitored and analysed by HIDS.

- OpenWIPS-NG

OpenWIPS-NG is a free wireless IDS/IPS that relies on a server, sensors and interfaces. It runs on commodity hardware. Created by the author of Aircrack-NG, this system uses many of the functions and services already built into Aircrack-NG for scanning, detection and intrusion prevention. OpenWIPS-NG is modular and allows an administrator to download plug-ins for additional features. The documentation isn't as detailed as some systems', but it allows for companies to perform WIPS on a tight budget.

- FRAGROUTE

It is termed as fragmenting router. Here, from the attacker to the fragrouter the IP packet is sent and they are then fragmented and transformed to the party.

- KISMET

It is a guideline for WIDS (Wireless intrusion detection system).WIDS compromises with packet payload and happenings of WIDS. It will find the burglar access point.

- HONEYD

Honeyd is a tool that creates virtual hosts on the network. The services are used by the host Honeyd allows a single host to request multiple addresses on a LAN for networks simulation. It is possible to knock the virtual machines or to trace route them. Any type of service on the virtual machine can be simulated according to a simple configuration file.

- BRO Ids

Bro IDS is similar to Security Onion in that it uses more than IDS rules to determine where attacks are coming from. Bro IDS uses a combination of tools. At one point it used Snort-based signatures converted into Bro signatures. This is no longer the case, and it is now possible to write custom signatures for the Bro IDS. This system is highly documented and has been around for over 15 years.

IX. COMPARISION OF DIFFERENT TOOLS AND TECHNOLOGY

The research has been supported by grants from the Natural Sciences and Engineering Research Council of Canada and Dalhousie University Electronic Commerce Executive Committee showed that Dragon performed better than or scored as high as the three open source systems in four of the five categories for the insider traffic. With the exception of one category it caught at least 50% or more of the attacks in each. In addition many of these attacks were caught with a confidence level of two.

Denial of Service Category catching only one of the eight attacks present. 73% of the attack related information in the log entries was at level 2.

Snort once again performed well in the DOS and Probe categories catching over 50% of the attacks in each but fell down in the other 3 categories. 99% of the information within its attack related information was at confidence level 2. This work has shown that even when some old attacks are used none of the systems detected them. It also showed that Intrusion Detection Systems could not be at fault when attacks are based on the abuse of perfectly legitimate features. Faults still exist in the way Operating Systems are designed and built. Further research will investigate the performance of these tools under attacks, which are specifically designed to bring down the intrusion detection systems themselves.

School of Future Studies & Planning showed that there are many technologies in the market today to help companies fight the inevitable network and system attack. Having IPS and IDS technologies are only two of many resources that can be deployed to increase visibility and control within a corporate computing environment. IDS and IPS are to provide a foundation of technology that meets the requirement of tracking, identifying network attacks to which detect through logs of IDS systems and prevent an action through IPS systems. If the host is with critical systems, confidential data and strict compliance regulations, then it's a great to use IDS, IPS or both in network environments.

International Journal of Computer Science and Information Technologies proved that both the firewall and intrusion detection systems still need to be improved to ensure an unfailing security for a network. They are not reliable enough (especially in regard to false positives and false negatives) and they are difficult to administer. To assure an effective computerized security, it is strongly recommended to have a combination of several types of Intrusion detection system. However, these technologies require to be developed in the coming years due to the increasing security needs of businesses and changes in technology that allows more efficient operation detection systems. This paper provided a new way of looking at network research including types of firewalls, types of intrusion detection that are necessary, complete, and mutually exclusive to aid in the fair comparison of firewall, intrusion detection system and to aid in focusing research in this area of new trends like Intrusion Prevention System.

X. NEEDS AND CHALLENGES:

IDS technology itself is undergoing a lot of enhancements. From the IDS implementation it is understood that it is important for an organization. IDS technology does not need human interventions. Today an IDS technology offers some automation like notifying the administrator in case of detection of a malicious activity, shunning the malicious connection for a configurable period of time, dynamically modifying a router's access control list in order to stop a malicious connection. For every event occurrence the IDS logs should be monitored. Monitoring the logs on a daily basis is required to analyze the activities which are detected by the IDS over a period of time.

The ratio of sensor manager should be acclaimed. It is very important to design the baseline policy before starting the IDS implementation and avoid false positives result. IDS sensor may send a lot of false positives result to the sensor and the ratio can be inadequate.

XI. FUTURE SCOPE

IDS implementation depends on the deployment success. Planning is important for the design and implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS. The decision can vary between organizations. A network based IDS is an immediate choice for many organizations because of its ability to monitor multiple systems and also the fact that it does not require a software to be loaded on a production system unlike host based IDS. Some of the organizations provide hybrid solution. So, the available resources are needed for a system before installing a host based sensor.

The IDS technology is still reactive rather than proactive and this technology works on attack signatures. Signatures are defined as a pattern of attacks which is defined earlier. The signature database needs to be updated whenever a different kind of attack is

detected and they are fixed in the database and the frequency of signature update varies from vendor to vendor.

XII. CONCLUSION

The main objective of this paper is to provide an overview of the necessity and utility of intrusion detection system. This paper gives complete study about types of IDS, life cycle, various domains, types of attacks and tools. IDS are becoming essential for day today security in corporate world and for network users**.** IPS defines about the preventing measures for the security. In the lifecycle the phases developed and the stages are illustrated. Still, there are more challenges to overcome. The techniques of anomaly detection and misuse detection are specifically illustrated and more techniques can be used. Further Work will be done on comparative analysis of some popular data mining algorithms applied to IDS and enhancing a classification based IDS using selective feedback methods.

XIII. REFERENCES:

1. Corinne Lawrence- "IPS – The Future of Intrusion Detection"- University of Auckland - 26th October 2004.
2. Palen Schwab blog for history of IDS
3. Karthikeyan .K.R and A. Indra- "Intrusion Detection Tools and Techniques a Survey"
4. "Intrusion Detection and Intrusion Prevention"-Ed Sale VP of Security Pivot Group, LLC.
5. Proctor, Paul E. The Practical Intrusion Detection Handbook.
6. Bace, Rebecca. "An Introduction to Intrusion Detection and Assessment: for System and Network Security Management."
7. Research paper by Engineering Research Council of Canada and Dalhousie University Electronic Commerce Executive Committee.
8. Research paper by School of Future Studies & Planning, Devi Ahilya University, Indore.
9. Research paper by International Journal of Computer Science and Information Technologies
10. Research paper by Bharathiar University, Coimbatore.