Taxonomy of Intrusion Detection System

Monika Sharma, Sumit Sharma

Abstract— **During the past years, security of computer networks has become main stream in most of everyone's lives. Nowadays as the use of computerized or online transactions is increased so there is very much need to secure the information from intruders. So today mainly discussions on computer security are centered on the tools or techniques that are used in protecting and defending networks. The researchers proposed a number of techniques like encryption and firewalls, to protect the computers and but with this techniques the intruders or attackers managed to penetrate the computers. IDS got much of the attention of researchers, Intrusion detection is the technique of identifying unauthorized use of any computer systems or network by both system insiders and outsiders. The aim of this paper is to discuss the feasibility of monitoring the traffic of different networks, to analyze it for providing better security. For this reason, this paper focuses on all the components of intrusion sniffing and response systems like host and network based IDS. This paper includes basic idea of intrusion detection system, technologies involved, detection types and IDS management.**

Index Terms—**Host IDS, Intrusion Detection System, Management, Network IDS, Wireless IDS.**

I. INTRODUCTION

A. Introduction of Intrusion Detection System

Intrusion detection systems are software or hardware systems whose main task is to monitor the events that are occurred in a computer system or in a network and if it detects any intrusion, it raises warning or alarm. An IDS is much like an alarm system, that is more advanced than other systems. An IDS is same as a burglar alarm that placed in a house same as IDS is placed in network and it checks all the traffic coming into network. Through various methods such as IDS and Burglar alarm both detect traffic when an attacker/ intruder/ burglar is there, and both successively issue various type of warning or alert. Intrusion detection systems serve three essential security functions: they monitor the network, detect any unusual activity and then respond to that unauthorized activity by insiders and outsider intrusion. To define assured events intrusion detection systems use some policies that, if any intrusion is detected, it will issue an alert. There are three steps in the process of intrusion detection which are:

- Monitoring and analyzing traffic.
- Identifying abnormal activities.
- Assessing severity and raising alarm.

***Monika Sharma**, M.E. Student, PEC University of Technology Chandigarh, India.*
***Sumit Sharma**, International Institute of Information Technology, Bangalore, India.*

B. Functions of Intrusion Detection System

Intrusion detection functions [1] include:

- Both user and system activities are monitored and analyzed
- System configurations and their vulnerabilities are analyzed.
- Assessing system and file integrity
- Distinguish different patterns of attacks
- Analysis of anomalous activity patterns
- Tracking user policy violations

C. Efficiency of Intrusion Detection System

The following parameters are used to evaluate the efficiency of an intrusion detection system [2]:

- Accuracy: Accuracy deals with the proper detection of attacks and the absence of false alarms. When an intrusion detection system detects a legitimate action in the environment as anomalous or intrusive then inaccuracy occurs.
- Performance: The performance of an intrusion detection system depends on the rate at which audit events are progressed. If the performance of the intrusion detection system is not good then real-time detection is not possible.
- Completeness: Completeness of an intrusion detection system is to detect all attacks. Incompleteness occurs when the intrusion detection system fails to detect an attack.
- Fault tolerance: An intrusion detection system should itself be challenging to attacks, mainly denial of service type attacks. This is particularly important because most of IDS run above commercially available operating systems or hardware which are known to be vulnerable to attacks.
- Timeliness: An intrusion detection system has to perform and propagate its investigation as quickly as possible to permit the security officer to react. This means more than the measure of performance because it not only includes the essential processing speed of the intrusion-detection system, but also

depends on the time required to spread the information and react to it.

D. False Positives and Negatives

It is impossible for IDS to be perfect every time, mostly because network traffic is so complicated. False positives and false negatives are two types of the erroneous results of IDS. False positives occur when the IDS erroneously detects a problem with benign traffic. When unwanted traffic is not detected by the IDS then false negatives are occurred. False positives and negatives both create problems for security administrators. Generally a bigger number of false positives are more acceptable but can burden a security administrator with large amounts of data. on the other hand, because it is not identified, false negatives do not afford a security administrator an opportunity to review the data.

II. SYSTEM COMPONENTS

IDSs are made up of the following main types of components [3]

1. Sensors: Sensors are used to collect data from network and deployed in a network or on a device. Sensors take input from different sources, includes log files, network packets and system calls. They collect input from network, organized, and then forwarded that information to one or more analyzers.

2. The Analyzers: Analyzers in an IDS collect data forwarded by sensors and then determine if an intrusion has actually occurred. Output from the analyzers should include evidence supporting the intrusion report.

3. User interface: The user interface of the IDS provides the end user a view and way to interact with the system. Interface facilitates the user to control and configure the system. Many user interfaces can produce reports as well.

4. Honeypot: In fully deployed IDS, several administrators may prefer to install a 'honeypot'. It essentially a system component set up as decoy for intruders. Honeypots can be used as early warning systems of an attack. Many IDS vendors maintain honeypots for research purposes and to develop new intrusion signatures [4].

III. TECHNOLOGIES

Several types of IDS technologies [3]exist due to the variance of network configurations.

A. Network Based Intrusion Detection System

Network intrusion detection System (NIDS) is one most common type of IDS that examines network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for any suspicious activity.

Component Types

The NIDS [5] is usually made of components the sensor, management sever, database server, and console. Figure 1 shows NIDS placement.

1. Sensor: The sensor is the NIDS component that sees network traffic and can make decisions regarding whether the traffic is malicious or not. Multiple sensors are usually placed at specific points around a network, and the location of the sensors is important. Connections to the network could be at firewalls, switches, routers, or other places at which the net- work divides.

2. Management server: Management server is same as the analyzer; it is a central location for all sensors to send results. Management servers often connect to sensors via a management network and because of security reasons; they mostly separate from the rest of the network. The management server will make decisions based on reports of sensors. It can also compare information from several sensors and then make decisions based on specific traffic in different locations on the network.

3. Database server: Database servers are the storage components of the NIDS. From these servers, events from sensors and correlated data from management servers can be logged. As databases have large data spaces so databases are used.

4. Console: It is the part of the NIDS at which the administrator can log into and configure the NIDS or to monitor its status. The console can be installed as either a local program on the administrators computer or a secure Web application portal.

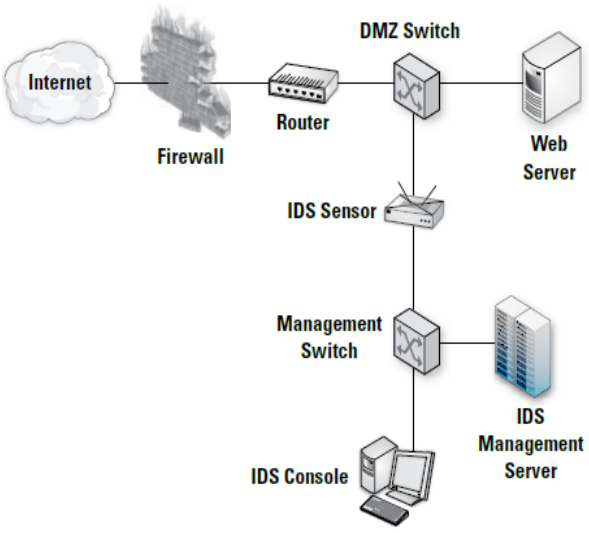

Fig. 1 above: NIDS Placement

Advantages of Network Based IDS [6]

- A network based IDSs can monitor a large network.

- Network based IDS are very secure against attack and even made invisible to many attackers.

- Easy to deploy network based IDS.

Disadvantages of Network Based IDS

- In case of a large or busy network, network Based IDSs may have difficulty in analyzing large data.

- Network Based IDSs cannot analyze data which is encrypted. And this problem is increasing as more organizations use virtual private networks.

- Most Network Based IDSs only understand that an attack was initiated, they cannot tell whether or not an attack was successful or not. So administrators must manually investigate each attacked host after a network-based IDS detects an attack.

B. Wireless Intrusion Detection System

A wireless IDS is similar to an NIDS because the same types of network-based attacks can occur on wireless networks. However, because WLANs have other functionality and vulnerabilities, a WLAN IDS must monitor for network based attacks as well as wireless specific attacks.

The location of a WLAN sensor is important because its physical location affects what a sensor can monitor. A sensor should be able to monitor traffic from devices that can connect to the wireless network (See Figure 2). WLAN devices run on one channel at a time, but can select from numerous channels. Several sensors may be used for listening to several channels at once.

Components

A wireless IDS contains several components such as sensors, management logging databases and consoles as does a NIDS. Wireless IDSs are unique in that they can be run centralized or decentralized. In centralized systems, the data is correlated at a central location and decisions and actions of intrusion is based on that collected data. Decisions are made at the sensor in decentralized systems.

Disadvantages of Wireless IDS

- Wireless networks are inherently open and viewable by all network scanners. There are no physical barriers between data sent through the air. As such it is relatively easy to intercept data packets in a wireless network.

- Wireless is the latest technology that comes with its own set of protocols for communication that break the traditional OSI layer model.

C. Network Behavior Anomaly Detection

Network behavior anomaly detection (NBAD) views traffic on network segments to determine if anomalies exist in the traffic. NBAD sensors are placed around a network in key places such as at switches, at demilitarized zones (DMZ), and at locations at which traffic splits to different segments. Sensors then report on what type and amount of traffic is passing through. NIDS and NBAD systems share some of the same components such as sensors and management consoles; however unlike NIDS, NBAD systems usually do not have database servers.

This is particularly useful for detecting DoS attacks and worms. As with other IDSs, NBADs can be used to prevent malicious traffic by stopping the traffic from passing through. NBADs have limitation that the network traffic causing the alert could also be the traffic that prevents a defensive mechanism.

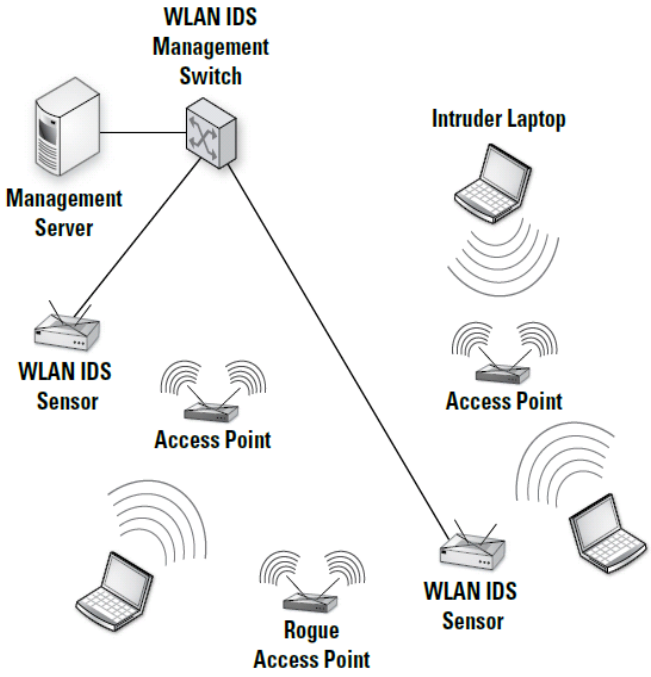

Fig. 2 above: Wireless IDS Placement

D. Host Based Intrusion Detection System

Host Based Intrusion Detection Systems (HIDS) [7] analyze network traffic and system specific settings such as local log audits, software calls, local security policy and more. HIDS must be fixed on each machine and requires configuration specific to that operating system and software. HIDS comprises sensors that are located on servers or workstations to prevent attacks on a specific machine.

Like other IDS configurations, HIDS have various device types. The sensor or agent is located on or near a host such as a server, application service or workstation. The event data is sent to logging services to record the events and possibly correlate them with other events. As figure 3 shows HIDS block diagram. HIDS sensors can monitor servers, client hosts, and application servers. A client host is the workstation, such as a desktop or laptop, in which a user can connect to other machines. An application service is software that runs on a server, such as a Web service or database application. Because each host operates a different OS or service, the types of attacks that will affect the machines are specific to these machines.

Advantages of Host Based IDS

- Host based IDS are fixed on each machine so they monitor events occurred to a host and they can detect intrusion that is not detected by a network based IDS.
- Host based IDSs are uninfluenced by switched networks.
- Host based IDSs can mainly run in an environment in which network traffic is encrypted, when the host based information sources are generated before data is encrypted after the data is decrypted at the destination host.

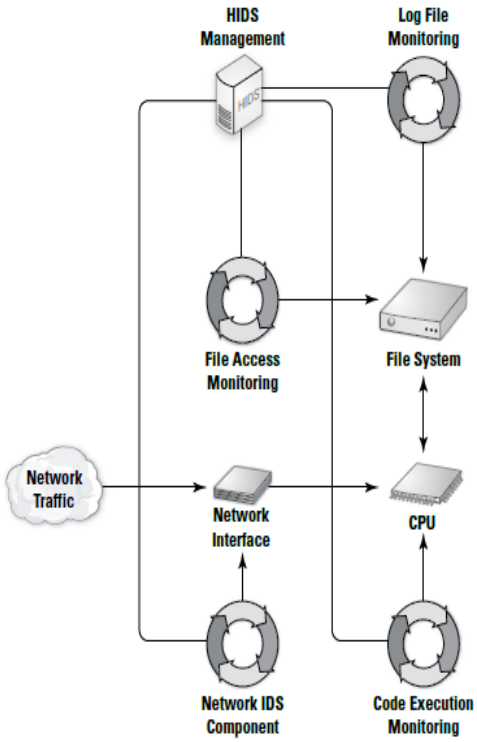

Fig. 3 above: HIDS Block diagram

Disadvantages of Host Based IDS

- Host based IDSs are difficult to manage because information must be configured and managed for every host monitored.
- Host based IDSs are not appropriate for detecting network scans or other such surveillance that targets an entire network, because the IDS only sees those network packets received by its host.
- Host based IDS can be disabled by certain type of denial of service attacks.

IV. Detection Types

A. Signature Based Detection

The process of comparing signatures against monitored events to recognize possible incidents is called signature based detection. Some examples of signatures are as follows:

- An e-mail with a subject of Free movies! and an attachment filename of freemovies.exe, which are form of a known form of malware.
- An operating system that have log entry with a code value of 645, which indicates that the hosts auditing has been disabled.

To detect known threats signature based detection is very effective but it is largely ineffective to detect previously unknown attacks. For example, if an attacker changed the malware to use a filename of freemovies2.exe, a signature looking for freemovies.exe would not match it.

Advantages of Signature Based Detection

- Signature based detectors are very useful at detecting attacks without generating an overwhelming number of false alarms
- The use of a specific attack tool or technique is quickly and reliably identify by signature based detectors.

Disadvantages of Signature Based Detection

- Signature based detection systems can only detect known attacks.
- Many Signature Based detectors are designed to use tightly defined signatures that prevent them from detecting variants of common attacks.

B. Anomaly Based Detection

An IDS that looks at network traffic and detects data that is incorrect, not valid, or generally abnormal is called anomaly-based detection. This method is useful for detecting un-wanted traffic that is not specifically known. The IDS compares the characteristic of current activity to thresholds related to the profile. Anomaly-based detection methods are very efficient to detect unknown threats.

Advantages of Anomaly Based Detection

- IDs based on anomaly detection detect unusual behavior and thus have the ability to detect signs of attacks without specific knowledge of details.
- Anomaly detectors can generate information that can in turn be used to define signatures for Signature based detectors.

Disadvantages of Anomaly Based Detection

- Anomaly based detection technique usually makes a large number of false alarms due to the unexpected behaviors of users and networks.
- Anomaly detection techniques mainly require widespread 'training sets' of system event records in order to characterize normal behavior patterns.

C. Stateful Protocol Inspection

Stateful protocol inspection [8] is similar to anomaly based detection, but it can also examine traffic at the transport and network layer and at the application layer, which is not analyzed by anomaly-based detection. Stateful protocol compares predetermined profiles of recognized definitions of benign protocol activity for each protocol state against observed events to identify deviations.

Disadvantages of Stateful Protocol Inspection

- In stateful inspection there is lot of complexity and the overhead in performing the state tracking for

various simultaneous sessions and they become very resource intensive.

- Stateful protocol analysis methods cannot detect attacks that do not defy the characteristics of generally acceptable protocol behavior, such as a denial of service attack.

V. IDS MANAGEMENT

- Maintenance: IDS maintenance is required for all IDS technologies. As intrusion detection and prevention techniques are always changing, signatures, patches, and configurations must be updated to ensure that the latest malicious traffic is being detected and prevented. Generally application, or secure web-based interface and graphical user interface, perform maintenance. Administrators from console can monitor IDS components to ensure they are operational, checks that they are working properly or not , and perform vulnerability assessments (VA) and updates [9].

- Tuning: To be effective, an IDS must be tuned perfectly. Tuning necessitates changing settings to be in compliance with the security policies and goals of the IDS administrator. Intrusion detection and prevention techniques, thresholds can be tuned to ensure that an IDS is identifying relevant data without overloading the administrator with warnings or too many false positives.

- Detection Accuracy: The accuracy of an IDS depends on the way in which it detects intrusion, by using the rule set. As signature-based detection detects only simple and well-known attacks, and anomaly-based detection can detect more different types of attacks, but anomaly detection has a large number of false positives. Tuning is necessitated to minimize the number of false positives and to make the data more useful.

VI. CONCLUSION

Intrusion detection systems are important parts of a well-rounded security infrastructure. Each of the IDS technologies Network IDS, Wireless IDS, NBAD, and Host IDS are used together, collecting data from each device and then making decisions based on what each type of IDS can monitor. Other techniques, policies and procedures should be used to protect the network. IDSs have many significant enhancements in the past decade, but some concerns still cause worry to our security administrators. These difficulties will continue to be addressed as IDS technologies improve.

REFERENCES

[1] http://searchmidmarketsecurity.techtarget.com/de_nition/intrusion- detection
[2] Herve Debar, "An Introduction to Intrusion-Detection Systems," IBM Research, pp. 1-18.
[3] Tzeyoung MaxWu, "Information Assurance Tools Report on Intrusion Detection system," sixth edition,2009.
[4] http://www.tracking-hackers.com last accessed on 17 June 2014.
[5] G.A. fink et. al, "a metric based approach to Intrusion Detection System evaluation for distributed real time system", WPDRTS, 15-17 april 2002.pp. 1-8.
[6] Rebecca Bace and Peter Mell, "Intrusion Detection Systems" Released by NIST on 16 August 2001.
[7] K. Rajasekhher, B. Sekharbaba, P. Lakshmi, "An overview of IDS strategies and issues", IJCST, oct-dec 2011, pp. 127-132.
[8] S. thakare, P.Ingle, BB. Meshram, " IDS: Intrusion Detection system the survey of information security", IJETAE, aug 2012,pp.86-91.
[9] Karen Scarfone Peter Mell, " Guide to Intrusion Detection and Prevention Systems (IDPS)" ,National Institute of Standards and Technology Special Publication 800-94,February 2007.

