An Overview of Intrusion Detection System Strategies and Issues

[1]K.Rajasekhar, [2]B.Sekhar Babu , [3]P.Lakshmi Prasanna, [4]D.R.Lavanya, [5]T.Vamsi Krishna
[1,3,4]Dept. of CSE, KL University, Vijayawada, AP, India,
[2]Dept. of MCA, KL University, Vijayawada, AP, India,
[5]Dept. of ECM KL University, Vijayawada, AP, India,

Abstract

During the past five years, security of computer network has become main stream in most of everyone's lives. Today, most discussions on computer security is centered on the tools or techniques used in protecting and defending networks. Intrusion detection is the method of identifying unauthorized use, misuse, and abuse of computer systems by both system insiders and external attackers. Our aim is to discuss the feasibility of monitoring the traffic of different networks, to analyze it for providing better security. For this reason, we focus on all the components of intrusion sniffing and response system like host and network based IDS. Intrusion detection is the process used to identify intrusions; these techniques have been traditionally classified into two types: HIDS and NIDS. In this paper we discuss main functionalities of IDS, characteristics of IDS and discussing few detection techniques they are anomaly-based detection, signature based, target monitoring, Stealth Probes.

Keywords

IDS, Host-based, Network based anomaly, Signature, Attack, Active IDS, Passive IDS.

I. Introduction

There are different types of systems or the programs are designed for the monitoring of different types of work of the computer systems or many other devices related to the same pattern. So, another system whose name is intrusion detection system is used in the field of computer networking for the sake of the monitoring of different components of the networks and checks the possibilities of infection of the system and maintenance of the policy of management also. An Intrusion Detection System (IDS) monitors and analyzes traffic on a network or activity on a system in an attempt to detect malicious activity. The exact meaning of the word intrusion differs per IDS product and the systems and services it is monitoring [1]. It can be anything from a port scan to an attempt to gain unauthorized access. Other examples include RIP spoofing, ping sweeps, malicious SQL injections, DOS attacks, Trojans, and unauthorized changes to system files and settings. When an IDS detects an intrusion, it will log the event, store relevant data/traffic, notify an administrator, and in some cases it will try to intervene. Besides the obvious advantages of an ID, the stored data and the logs provide valuable forensic information and may be used as evidence in a legal case against the attacker [12]. An IDS is much like an alarm system, some being more advanced and intelligent than others. In a nutshell, intrusion detection systems do exactly as the name suggests: they detect possible intrusions. More specifically, IDS tools aim to detect computer attacks and/or computer misuse, and to alert the proper individuals upon detection. An IDS installed on a network provides much the same purpose as a burglar alarm system installed in a house. Through various methods, both detect when an intruder/attacker/burglar is present, and both subsequently issue some type of warning or alert. Intrusion detection systems serve three essential security functions: they monitor, detect, and respond to unauthorized activity by company insiders and outsider intrusion. Intrusion detection systems use policies to define certain events that, if detected will issue an alert. In other words, if a particular event is considered to constitute a security incident, an alert will be issued if that event is detected. Certain intrusion detection systems have the capability of sending out alerts, so that the administrator of the IDS will receive a notification of a possible security incident in the form of a page, email, or SNMP trap. Many intrusion detection systems not only recognize a particular incident and issue an appropriate alert, they also respond automatically to the event. Such a response might include logging off a user, disabling a user account, and launching of scripts. When AN IDS detects an intrusion, it will log the event, store relevant data/traffic, notify an administrator, and in some cases it will try to intervene. Besides the obvious advantages of an ID, the stored data and the logs provide valuable forensic information and may be used as evidence in a legal case against the attacker. An IDS is much like an alarm system, some being more advanced and intelligent than others.

II. Why We Need IDS

Of the security incidents that occur on a network, the vast majority (up to 85 percent by many estimates) come from inside the network. These attacks may consist of otherwise authorized users who are disgruntled employees. The remainders come from the outside, in the form of denial of service attacks or attempts to penetrate a network infrastructure. Intrusion detection systems remain the only proactive means of detecting and responding to threats that stem from both inside and outside a corporate network [2].Intrusion detection system are integral and necessary elements of a complete information security infrastructure performing as "the logical complement to network firewalls." [BAC99] Simply put, IDS tools allow for complete supervision of networks, regardless of the action being taken, such that information will always exist to determine the nature of the security incident and its source.

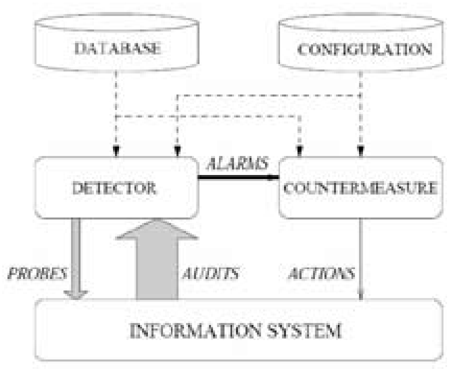
Clearly, corporate America understands this message. Studies show that nearly all large corporations and most medium-sized organizations have installed some form of intrusion detection tool [SANS01]. The February 2000 denial of service attacks against Amazon.com and E-Bay (amongst others) illustrated the need for effective intrusion detection, especially within on-line retail and e-commerce. However, it is clear that given the increasing frequency of security incidents, any entity with a presence on the Internet should have some form of IDS running as a line of defense. Network attacks and intrusions can be motivated by financial, political, military, or personal reasons, so no company should feel immune. Realistically, if you have a network, you are a potential target, and should have some form of IDS installed.

III .What is Intrusion Detection?

As stated previously, intrusion detection is the process of monitoring computers or networks for unauthorized entrance, activity, or file modification. IDS can also be used to monitor network traffic, thereby detecting if a system is being targeted by a network attack such as a denial of service attack. There are two basic types of intrusion detection: host-based and network-based. Each has a distinct approach to monitoring and securing data, and each has distinct advantages and disadvantages. In short, host-based IDSs examine data held on individual computers that serve as hosts, while network-based IDSs examine data exchanged between computers [3].

There are three steps in the process of intrusion detection which are:

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



NOTE: The arrow thickness represents the amount of information flowing from one component to another.

Fig. 1 : simple intrusion detection system

A. Characteristics of Intrusion Detection System

There are several characteristics of the intrusion detection system that governs the specification and the networking of the system in the protection of the computer networking. Some of the important characters are as follows.

1. A true intrusion detection system can be able to mange the security measures and can also mange all the events of the administration.
2. Many forms pf intrusion detection system can detect the problem and can stop them at the spot and restrict it from succeeding.
3. Intrusion detection system also has property to that they can change the settings of the windows firewall according to this work and prevent the system from dangerous attacks.

IV. How Intrusion Detection system Works?

The working of the intrusion detection system is quite similar as that of the other programs used to prevent the computer system from dangerous threats like malware, spyware, spam and many more. The job of the intrusion detection system starts from the recording the information about the problem and check the occurrence and the nature of the threat. When the system monitors the problem and collects the data about it, then it sends this information to the administration department of the intrusion detection system which makes several preventive measures to protect the system and keep the system in the safe hands[4]. Intrusion detection system can work in the specific manner by monitoring some important things. These important things are as follows.

Monitoring the activity of the network and activity of the threat in the network.

This system has ability to detect the viruses, malware, spyware and different form of viruses and the important thing about this it can also locate their restore point.

Intrusion detection system can work by observing the unauthenticated and unauthorized use of different programs of networking.

V. IDS FUNCTIONS

Functions of IDS:

- “Monitoring users and system activity.
- Auditing system configuration for vulnerabilitiesand misconfigurations.
- Assessing the integrity of critical system and data files.
- Recognizing known attack patterns in system activity.
- Identifying abnormal activity through statistical analysis.
- Managing audit trails and highlighting user violation of policy or normal activity.
- Correcting system configuration errors
- Installing and operating traps to record information about intruders.

VI. Active and passive IDS

An active Intrusion Detection Systems (IDS) is also known as Intrusion Detection and Prevention System (IDPS). Intrusion Detection and Prevention System (IDPS) is config.d to automatically block suspected attacks without any intervention required by an operator. Intrusion Detection and Prevention System (IDPS) has the advantage of providing real-time corrective action in response to an attack. Active-response IDSs automatically take action in response to a detected intrusion. The exact action differs per product and depends on the severity and type of attack. A common active response is increasing the sensitivity level of the IDS to collect additional information about the attack and the attacker. Another possible active response is making changes to the configuration of systems or network devices such as routers and firewalls to stop the intrusion and block the attacker. This could involve blocking the source address of the attacker, restarting a server or service, closing connections or ports, and resetting TCP sessions. Another less common active response that is not advisable from a legal perspective is retaliation – attacking the attacker

A passive IDS is a system that’s config.d to only monitor and analyze network traffic activity and alert an operator to potential vulnerabilities and attacks. A passive IDS is not capable of performing any protective or corrective functions on its own. Many intrusion detection systems merely log the intrusion and notify someone, by email or pager for example. This is known as passive-response intrusion detection, as it does not actively attempts to stop the intrusion. Instead, a system administrator or someone else will have to respond to the alarm, take appropriate action to halt the attack, and possibly identify the intruder. Modern IDSs offer a wide range of options to send notifications of intrusions, including pager, cell phone, email, SNMP trap messages, or simply a message box on the administrator’s PC. It is important to make sure that the notifications are send in a secure manner to prevent the attacker from intercepting or altering them.

VII. Types of Intrusion Detection System

Intrusion detection system can also categorized into different types if but the important one are given below

A. Host-Based IDS (HIDS)

Another important type of intrusion detection system that consist of a special agent on the host that observes the different activities such as calls of system, file logging and many other application of relevant field and can protect the from other host also is called as host based intrusion detection system. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity

Host-based systems were the first type of IDS to be developed and implemented. These systems collect and analyze data that originate on a computer that hosts a service, such as a Web server. Once this data is aggregated for a given computer, it can either be analyzed locally or sent to a separate/central analysis machine. One example of a host-based system is programs that operate on a system and receive application or operating system audit logs. These programs are highly effective for detecting insider abuses. Residing on the trusted network systems themselves, they are close to the network's authenticated users. If one of these users attempts unauthorized activity, host-based systems usually detect and collect the most pertinent information in the quickest possible manner. In addition to detecting unauthorized insider activity, host-based systems are also effective at detecting unauthorized file modification.

On the down side, host-based systems can get unwieldy. With several thousand possible endpoints on a large network, collecting and aggregating separate specific computer information for each individual machine may prove inefficient and ineffective.

Possible host-based IDS implementations include Windows NT/2000 Security Event Logs, RDMS audit sources, Enterprise Management systems audit data (such as Tivoli), and UNIX Syslog in their raw forms or in their secure forms such as Solaris' BSM; host-based commercial products include Real Secure, ITA, Squire, and Entercept.

A host-based IDS is usually a software application installed on a system and monitors activity only on that local system. It communicates directly with the operating system and has no knowledge of low-level network traffic. Most host-based IDSs rely on information from audit and system log files to detect intrusions. They can also monitor system files and system resources, and incoming application data. Because host-based IDS can produce a lot of data, hence an extra administrative load, they are often placed only on critical servers. To further reduce the load, the IDSs can report to a central console.

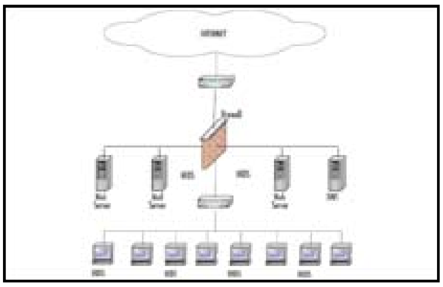


Fig. 2 : Host based IDS Architecture

B. Network-based IDS (NIDS)

Network-based intrusion detection analyzes data packets that travel over the actual network. These packets are examined and sometimes compared with empirical data to verify their nature: malicious or benign. Because they are responsible for monitoring a network, rather than a single host, Network-based intrusion detection systems (NIDS) tend to be more distributed than host-based IDS. Software, or appliance hardware in some cases, resides in one or more systems connected to a network, and is used to analyze data such as network packets. Network Intrusion Detection System is a independent systems that monitor the network traffic and different applications of networking such as sniffing and check them either they are free from threat or not with the help of sensors are called as network intrusion detection system. Common example is Snort. Network-based IDS can be a dedicated hardware appliance, or an application running on a computer, attached to the network. It monitors all traffic in a network or coming thru an entry-point such as an Internet connection [5]. The network card of a network-based IDS runs in promiscuous mode, which means it picks up all traffic from the media even if the destination address is not the IDS. It basically works like a sniffer. It is passive while it collects real-time raw network traffic; other hosts are usually not aware of the IDS and no extra load is put on the network [6].

In general, network-based systems are best at detecting the following activities:

1.Unauthorized outsider access

When an unauthorized user logs in successfully, or attempts to log in, they are best tracked with host-based IDS. However, detecting the unauthorized user before their log on attempt is best accomplished with network-based IDS [13].

2.Bandwidth theft/denial of service

These attacks from outside the network single out network resources for abuse or overload. The packets that initiate/carry these attacks can best be noticed with use of network-based IDS.

3. Limitations and drawbacks

Network-based IDS may not always be able to pick up and process all data in busy networks. Another challenge for a network-based IDS is encrypted data; most are able to inspect compressed data, but encrypted data remains an obstacle simply because the IDS does not have access to the keys of every devices in the network.

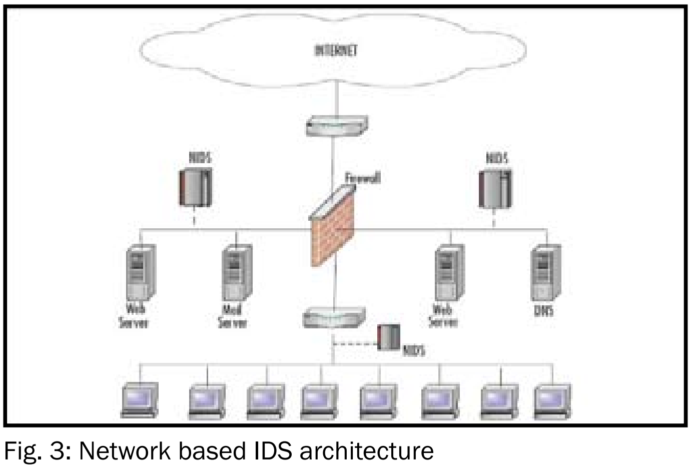


Fig. 3: Network based IDS architecture

C. Difference between HIDS & NIDS

Table1: Difference between HIDS and NIDS [7]

NIDS(Network IDS)	HIDS(Host IDS)
Watches all network activities(Broad in scope)	Watches only specific host activites(Narrow in scope)
Better for detecting attacks from outside	Better for detecting attacks from inside
Near real time response	Usually only response after a suspicious log entry has been made
Easier setup	More complex setup
Less expensive to implement	More expensive to implement
Detection is based on what can be recorded on the entire network	Detection is based on what any single host can record
Examines packet header	Does not see packet headers
OS independent	OS-specific
Detects network attacks as payload is analyzed	Detects local attacks before they hit the network
Detects unsuccessful attack attempts	Verifies success or failure of attacks

VIII. IDS Techniques

Now that we have examined the two basic types of IDS and why they should be used together, we can investigate how they go about doing their job. For each of the two types, there are four basic techniques used to detect intruders: anomaly detection, misuse detection (signature detection), target monitoring, and stealth probes.

A. Anomaly Detection

An anomaly detection system first creates a baseline profile of the normal system, network, or Program activity. Thereafter, any activity that deviates from the baseline is treated as a possible intrusion. Anomaly detection systems offer several benefits. First, they have the capability to detect insider attacks. For instance, if a user or someone using a stolen account starts performing actions that are outside the normal user-profile, an anomaly detection system generates an alarm.

Second, because the system is based on customized profiles, it is very difficult for an attacker to know with certainty what activity it can carry out without setting off an alarm. Third, an anomaly detection system has the ability to detect previously unknown attacks. An example of this would be if a user logs on and off of a machine 20 times a day instead of the normal 1 or 2. Also, if a computer is used at 2:00 AM when normally no one outside of business hours should have access, this should raise some suspicions [9]. At another level, anomaly detection can investigate user patterns, such as profiling the programs executed daily. If a user in the graphics department suddenly starts accessing accounting programs or compiling code, the system can properly alert its administrators. The major benefit of anomaly-based detection methods is that they can be very effective at detecting previously unknown threats.

1. Advantages

Because anomaly-based systems are capable of detecting misuse based on network and system behavior, the type of misuse does not need to be previously known. This allows for the detection of misuse a signature based system may not detect.

2. Disadvantages

- High false-alarm and limited by training data.

B. Signature-Based Detection

A signature is a pattern that corresponds to a known threat. Signature-based detection is the processes of comparing signatures against observed events to identify possible incidents. Examples of signatures are as follows:

1. A telnet attempt with a username of “root”, which is a violation of an organization’s security policy
2. An e-mail with a subject of “Free pictures!” and an attachment filename of “freepics.exe”, which are characteristics of a known form of malware
3. An operating system log entry with a status code value of 645, which indicates that the host’s auditing has been disabled.

Signature-based detection is very effective at detecting known threats but largely ineffective at detecting previously unknown threats, threats disguised by the use of evasion techniques, and many variants of known threats. Signature-based detection is the simplest detection method because it just compares the current unit of activity, such as a packet or a log entry, to a list of signatures using string comparison operations. Signature-based detection technologies have little understanding of many network or application protocols and cannot track and understand the state of complex communications [8].

1. Advantages

- Typicallysignature-based approaches Result in fewer false alarms because they can be very specific about what it is they are looking for.
- Because the IDS is looking for something Known, a lot of information regarding what the misuse is, the potential impact, And how to respond can be provided. This knowledge is extremely important in understanding what is occurring and effectively responding.

2. Disadvantages

Signature-based approaches can only detect misuse for which a signature exists. For a signature to exist, the form of misuse must be known about beforehand so it can be researched and programmatically identified. This means any new form of misuse will not be detected by a signature based system.

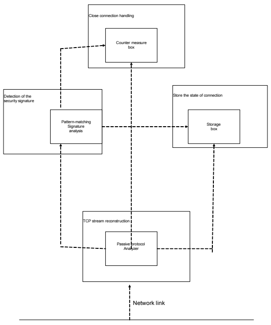

Close connection handling
Counter measure box
Detection of the security signature
Pattern-matching Signature analysis
Store the state of connection
Storage box
TCP stream reconstruction
Passive protocol Analyzer
Network link

Fig. 3 : Block schematic of the components in a signature based NIDS

C. Target Monitoring

The purpose of the target monitoring system is to monitor the changes made to some specific program instead of Detecting the misuse or anomaly. Wherever this system is deployed, the administrator does not need to monitor the System continuously. For monitoring the modifications, integrity checksum hashes can be computed either for all The files or for some specific file, based on the requirement. One way to check for the covert editing of files is by computing a cryptographic hash beforehand and comparing this to new hashes of the file at regular intervals. This type of system is the easiest to implement, because it does not require constant monitoring by the administrator. Integrity checksum hashes can be computed at whatever intervals you wish, and on either all files or just the mission/system critical files.

D. Stealth Probes

This technique attempts to detect any attackers that choose to carry out their mission over prolonged periods of time. Attackers, for example, will check for system vulnerabilities and open ports over a two-month period, and wait another two months to actually launch the attacks. Stealth probes collect a wide-variety of data throughout the system, checking for any methodical attacks over a long period of time [10]. They take a wide-area sampling and attempt to discover any correlating attacks. In effect, this method combines anomaly detection and misuse detection in an attempt to uncover suspicious activity.

IX. Conclusion

An Intrusion Detection System (IDS) monitors and analyzes traffic on a network or activity on a system in an attempt to detect malicious activity. In this paper we analyzed two intrusion detection types. They are Host Based and Network Based IDS. And also analysed various detection techniques like Anomaly Based, Signature based, Target Monitoring, and Stealth Probes.

References

[1] Stephanie Forrest, Steven A. Hofmeyr, Anil Somayaji, Thomas A. Longstaff,"A sense of self for UNIX processes." In Proceedings of the 1996 IEEE Symposium on Security and Privacy, 6–8 May 1996, Oakland, California, pp. 120–128, IEEEComputer Society Press, Los Alamitos, California, 1996.

[2] Endorf, Carl et al,"Intrusion Detection and Prevention", McGraw-Hill Osborne Media, 2003

[3] Vera Marinova-Boncheva, “A Short Survey of Intrusion Detection Systems”, Problems of Engineering Cybernetics and Robotics, 58, [Online] Available: http://www.iit.bas.bg/PECR/58/23-30.pdf 2007

[4] [Online] Available: www.techexams.net/technotes/securityplus/ids.shtml.

[5] [Online] Available: Searchmidmarketsecurity.techtarget.com /definition/intrusion-detection.

[6] [Online] Available: netsecurity.about.com/cs/hackertools/a/aa030504.html.

[7] [Online] Available: ebutler.webs.com/ids%20power%20point.ebutler.ppt.

[8] herve debar,"an introduction to intrusion detection system,” in IBM research.

[9] Guide to intrusion detection and prevention system.

[10] Saira beg, umair naru, mahamood ashruf, sajjad moshsin,”fesabuility of intrusion detection system with high performance computing:A survey,”in international journal for advances in computer science December 2010,volume1,issue1.

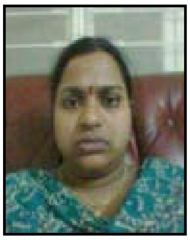
[11] [Online] Available: www.insecure.in/ids.asp

[12] [Online] Available: www.logrhythm.com/Portals/0/resources/IntroductionToIDS.pdf

[13] Northcutt, S," Network Intrusion Detection: An Analyst’s Handbook." New Riders, Indianapolis 199

This is B.Sekhar Babu received M.C.A degree in the year 2006 at Koneru Lakshmaiah college of Engineering,Andhra Pradesh,India. He received M.Tech degree at Nagarjuna university.presently he is working as Ass.Prof in K L University.

This is P. Prasanna received B.Tech degree in the year 2009 at Koneru Lakshmaiah college of Engineering,Andhra Pradesh,India.Presently pursuing M.Tech at K L University.



This is D.R.Lavanya received B.Tech degree in the year 2005 at Bonam Venkata Chalamaiah Engineering college ,Andhra Pradesh,India.had worked as Database Administrator for 3 years for Sreeven Infocomm, Hyderabad.Presently pursuing M.Tech at K L University.

This is T.Vamsi Krishna studying B.Tech(ECM) in KLCE in the year 2008-20012.