Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Intrusion Detection Systems: Definition, Need and Challenges

IDS are becoming the logical next step for many organizations after deploying firewall technology at the network perimeter. IDS can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all. However, the following points are very important to keep in mind. 1. Strong identification and authentication: An IDS uses very good signature analysis mechanisms but strong user identification and authentication mechanisms are still needed. 2. IDS are not a solution to all secur...

Copyright SANS Institute

Author Retains Full Rights

AD

INTRUSION DETECTION SYSTEMS; DEFINITION, NEED AND CHALLENGES

© SANS Institute 2001, Author retains full rights

A PAPER ON INTRUSION DETECTION SYSTEM

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Intrusion Detection system

Introduction:

Internet is a global public network. With the growth of the Internet and its potential, there has been subsequent change in business model of organizations across the world. More and more people are getting connected to the Internet every day to take advantage of the new business model popularly known as e-Business. Internetwork connectivity has therefore become very critical aspect of today's e_business.

There are two sides of business on the Internet. On one side, the Internet brings in tremendous potential to business in terms of reaching the end users. At the same time it also brings in lot of risk to the business. There are both harmless and harmful users on the Internet. While an organization makes its information system available to harmless Internet users, at the same time the information is available to the malicious users as well. Malicious users or hackers can get access to an organization's internal systems in various reasons. These are,

- Software bugs called vulnerabilities
- Lapse in administration
- Leaving systems to default configuration

The malicious users use different techniques like Password cracking, sniffing unencrypted or clear text traffic etc. to exploit the system vulnerabilities mentioned above and compromise critical systems. Therefore, there needs to be some kind of security to the organization's private resources from the Internet as well as from inside users as survey says that eighty percent of the attacks happen from inside users for the very fact that they know the systems much more than an outsider knows and access to information is easier for an insider.

Different organizations across the world deploy firewalls to protect their private network from the Public network. But, when it comes to securing a Private network from the Internet using firewalls, no network can be hundred percent secured. This is because; the business requires some kind of access to be granted on the Internal systems to Internet users. The firewall provides security by allowing only specific services through it. The firewall implements a policy for allowing or disallowing connections based on organizational security policy and business needs. The firewall also protects the organization from malicious attack from the Internet by dropping connections from unknown sources.

The definition of an Intrusion Detection System and its need:

The question is, where does the Intrusion detection system fit in the design. To put it in simpler terms, an Intrusion detection system can be compared with a burglar alarm. For example, the lock system in a car protects the car from theft. But if somebody breaks

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

the lock system and tries to steal the car, it is the burglar alarm that detects that the lock has been broken and alerts the owner by raising an alarm.

The Intrusion detection system in a similar way complements the firewall security. The firewall protects an organization from malicious attacks from the Internet and the Intrusion detection system detects if someone tries to break in through the firewall or manages to break in the firewall security and tries to have access on any system in the trusted side and alerts the system administrator in case there is a breach in security**.**

Moreover, Firewalls do a very good job of filtering incoming traffic from the Internet; however, there are ways to circumvent the firewall. For example, external users can connect to the Intranet by dialing in through a modem installed in the private network of the organization. This kind of access would not be seen by the firewall.

Therefore, an Intrusion detection system (IDS) is a security system that monitors computer systems and network traffic and analyzes that traffic for possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from inside the organization.

Components of Intrusion Detection System:

An Intrusion Detection system comprises of Management console and sensors. Management console is the management and reporting console. Sensors are agents that monitor hosts or networks on a real time basis. An Intrusion Detection System has a database of attack signatures. The attack signatures are patterns of different types of previously detected attacks.

If the sensors detect any malicious activity, it matches the malicious packet against the attack signature database. In case it finds a match, the sensor reports the malicious activity to the management console. The sensor can take different actions based on how they are configured. For example, the sensor can reset the TCP connection by sending a TCP FIN, modify the access control list on the gateway router or the firewall or send an email notification to the administrator for appropriate action.

Types of Intrusion Detection Systems:

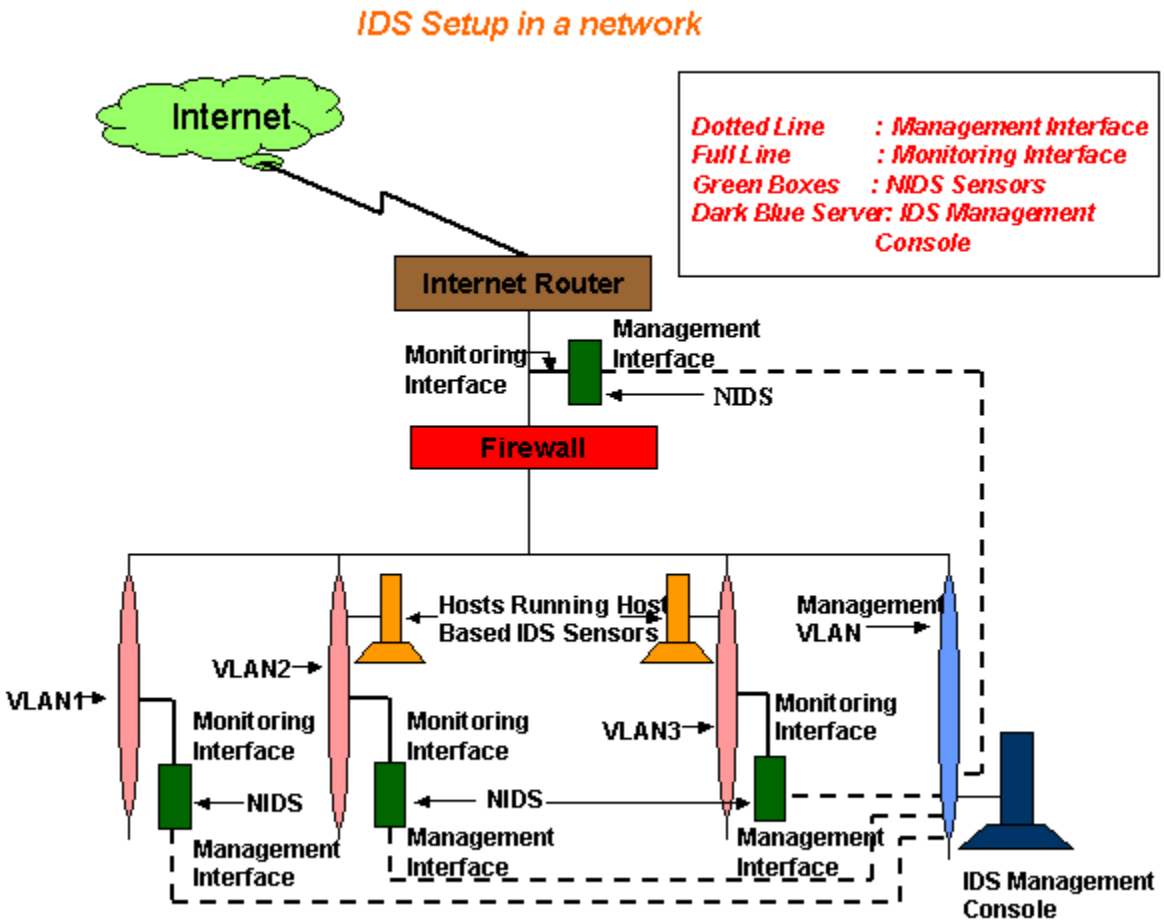
There are broadly two types of Intrusion Detection systems. These are host based Intrusion Detection System and network based Intrusion Detection System. A Host based Intrusion Detection system has only host based sensors and a network based Intrusion detection system has network-based sensor as explained in the Picture1 below.

As shown in the picture1, a network based IDS sensor has two interfaces. One of the interfaces is manageable. The IDS management console communicates with the sensor through the management interface. The other interface of the IDS is in promiscuous

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

(listening) mode. This interface cannot be accessed over the network and is not manageable.

The monitoring interface is connected to the network segment, which is being monitored. The sensor examines every packet that crosses the network segment. Network based sensors apply predefined attack signatures to each frame to identify hostile traffic. If it finds a match against any signature, it notifies the management console. Some vendors offer network based sensors running off a workstation. Some vendors offer sensor appliances with proprietary operating system and sensor software.



Picture1: Deployment of IDS Sensors and Management Console in a network

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

In the picture1, the dotted line interface on each network based IDS sensor (shown as NIDS) is the management interface and the thick line interface is the monitoring interface.

As shown, the management interface connects to the management VLAN (VLAN0). The management console is also installed in the management VLAN in this example. The management console could be connected to any other VLAN, but it should be able to communicate with the other VLANs to which the management interfaces of the network based IDS sensors are connected. It is recommended to connect the management interfaces of the NIDS and the management console to the same VLAN.

The host based Intrusion detection systems on the other hand works off the hosts. The host-based sensor is software running on the host being protected. It monitors system audit and event logs. When any of these files change, the IDS sensor compares the new log entry with attack signatures to see if there is a match. In case a match is found, the sensor notifies the management console.

The host-based sensors do not do any packet level analysis. Instead, they monitor system level activities. For example, an unauthorized user (other than administrator) changing registry files in a Windows NT system, or changing /etc/password or /etc/shadow file in a Unix system, a user trying to login at 7:00 pm, although he or she is allowed to login only between 9:00 am and 5:00 pm.

The host-based sensors monitor these kinds of activities and if it finds any anomaly, respond with administrator alerts. Host based IDS have grown over the years. Some hosts based IDS systems checks key system files and executables via checksums at regular intervals for unexpected changes. Some products listen to port based activity and alert administrators when specific ports are accessed.

Network based and Host based Intrusion detection systems have their own advantages and disadvantages. These are discussed separately below. For more detailed comparison, refer to http://secinf.net/info/ids/nvh_ids/

Advantages of Network based Intrusion Detection Systems:

1. Lower Cost of Ownership: Network based IDS can be deployed for each network segment. An IDS monitors network traffic destined for all the systems in a network segment. This nullifies the requirement of loading software at different hosts in the network segment. This reduces management overhead, as there is no need to maintain sensor software at the host level.

2. Easier to deploy: Network based IDS are easier to deploy as it does not affect existing systems or infrastructure. The network-based IDS systems are Operating system independent. A network based IDS sensor will listen for all the attacks on a network segment regardless of the type of the operating system the target host is running.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3. Detect network based attacks: Network based IDS sensors can detect attacks, which host-based sensors fail to detect. A network based IDS checks for all the packet headers for any malicious attack. Many IP-based denial of service attacks like TCP SYN attack, fragmented packet attack etc. can be identified only by looking at the packet headers as they travel across a network. A network based IDS sensor can quickly detect this type of attack by looking at the contents of the packets at the real time.

4. Retaining evidence: Network based IDS use live network traffic and does real time intrusion detection. Therefore, the attacker cannot remove evidence of attack. This data can be used for forensic analysis. On the other hand, a host-based sensor detects attacks by looking at the system log files. Lot of hackers are capable of making changes in the log files so as to remove any evidence of an attack.

5. Real Time detection and quick response: Network based IDS monitors traffic on a real time. So, network based IDS can detect malicious activity as they occur. Based on how the sensor is configured, such attack can be stopped even before they can get to a host and compromise the system. On the other hand, host based systems detect attacks by looking at changes made to system files. By this time critical systems may have already been compromised.

6. Detection of failed attacks: A network based IDS sensor deployed outside the firewall (as shown in picture1 above) can detect malicious attacks on resources behind the firewall, even though the firewall may be rejecting these attempts. This information can be very useful for forensic analysis. Host based sensors do not see rejected attacks that could never hit a host inside the firewall.

Advantages of Host based Intrusion Detection Systems:

1. Verifies success or failure of an attack: Since a host based IDS uses system logs containing events that have actually occurred, they can determine whether an attack occurred or not with greater accuracy and fewer false positives than a network based system. Network based IDS sensors although quicker in response than host based IDS sensors, generate a lot of false positives because of the very fact that it detects malicious packets on the real time and some of these packets could be from a trusted host.

2. Monitors System Activities: A host based IDS sensor monitors user and file access activity including file accesses, changes to file permissions, attempts to install new executables etc. A host based IDS sensor can also monitor all user logon and logoff activity, user activities while connected to the network, file system changes, activities that are normally executed only by an administrator. Operating systems log any event where user accounts are added, deleted or modified. The host based IDS can detect an improper change as soon as it is executed. A network-based system cannot give so much detailed information about system activities.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

3. Detects attacks that a network based IDS fail to detect: Host based systems can detect attacks that network based IDS sensors fail to detect. For example, if an unauthorized user makes changes to system files from the system console, this kind of attack goes unnoticed by the network sensors. So, host based sensors can be very useful in protecting hosts from malicious internal users in addition to protecting systems from external users.

4. Near real time detection and response: Although host based IDS does not offer true real-time response, it can come extremely close if implemented correctly. Unlike older systems, which use a process to check the status and content of log files at predefined intervals, many current host-based systems receive an interrupt from the operating system when there is a new log file entry. This new entry can be processed immediately, significantly reducing the time between attack recognition and response.

5. Does not require additional hardware: Host based Intrusion detection sensors reside on the host systems. So they do not require any additional hardware for deployment, thus reducing cost of deployment.

6. Lower entry cost: Host based IDS sensors are far more cheaper than the network based IDS sensors.

Challenges of Intrusion Detection:

Intrusion detection systems in theory looks like a defense tool which every e-organization needs. However there are some challenges the organizations face while deploying an intrusion detection system. These are discussed below.

1. IDS technology itself is undergoing a lot of enhancements. It is therefore very important for organizations to clearly define their expectations from the IDS implementation. IDS technology has not reached a level where it does not require human intervention. Of course today's 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 etc.

But it is still very important to monitor the IDS logs regularly to stay on top of the occurrence of events. Monitoring the logs on a daily basis is required to analyze the kind of malicious activities detected by the IDS over a period of time. Today's IDS has not yet reached the level where it can give historical analysis of the intrusions detected over a period of time. This is still a manual activity.

It is therefore important for an organization to have a well-defined Incident handling and response plan if an intrusion is detected and reported by the IDS. Also, the organization should have skilled security personnel to handle this kind of scenario.

© SANS Institute 2001, Author retains full rights.

2. The success of an IDS implementation depends to a large extent on how it has been deployed. A lot of plan is required in the design as well as the implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS to benefit from both. In fact one technology complements the other. However, this decision can vary from one organization to another. 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 organizations implement a hybrid solution. Organizations deploying host based IDS solution needs to keep in mind that the host based IDS software is processor and memory intensive. So it is very important to have sufficient available resources on a system before installing a host based sensor on it.

3. It is important to take care of sensor to manager ratio. There is no thumb rule as such for calculating this ratio. To a large extent it depends upon how many different kinds of traffic is being monitored by each sensor and in what environment. Lot of organizations deploy a 10:1 ratio. Some organizations go for 20:1 and some others 15:1.

It is very important to design the baseline policy before starting the IDS implementation and avoid false positives. A badly configured IDS sensor may send a lot of false positives to the console and even a 10:1 or even better sensor to console ratio can be inadequate.

4. The IDS technology is still reactive rather than proactive. The IDS technology works on attack signatures. Attack signatures are attack patterns of previous attacks. The signature database needs to be updated whenever a different kind of attack is detected and the fix for the same is available. The frequency of signature update varies from vendor to vendor.

5. While deploying a network based IDS solution, it is important to keep in mind one very important aspect of the network based IDS in switched environment. Unlike a HUB based network, where a host on one port can see traffic in and out of every other port in the HUB, in a switched network however, traffic in and out of one port can not be seen by a host in another port, because they are in different collision domains.

A network based IDS sensor needs to see traffic in and out of a port to detect any malicious traffic. In a switched environment, port mirroring or spanning is required to achieve this. One entire VLAN can be spanned to one port on which the network based IDS sensor is installed.

Although this is a solution, there may be performance issues for a busy network. If all the 10/100 Mbps ports in a VLAN are mirrored to another 10/100 Mbps port in the VLAN, the IDS sensor may drop traffic, as the combined traffic of all the ports could be more than 100 Mbps. Now, Gigabit port speed being available, this becomes an even more difficult challenge. Cisco systems has an IDS module for Catalyst 6000 series

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

switch which can sit on the switch back plane and can monitor traffic right off the switch back plane. But this solution is yet to scale to Gigabit speed. This module supports traffic only up to 100 Mbps as of now. The portability of network based IDS in a switched environment is still a concern.

Conclusion:

IDS are becoming the logical next step for many organizations after deploying firewall technology at the network perimeter. IDS can offer protection from external users and internal attackers, where traffic doesn't go past the firewall at all

However, the following points are very important to always keep in mind. If all of these points are not adhered to, an IDS implementation along with a firewall alone can not make a highly secured infrastructure.

1. ***Strong identification and authentication:***

   An IDS uses very good signature analysis mechanisms to detect intrusions or potential misuse; however, organizations must still ensure that they have strong user identification and authentication mechanism in place.

2. ***Intrusion Detection Systems are not a solution to all security concerns:***

   IDS perform an excellent job of ensuring that intruder attempts are monitored and reported. In addition, companies must employ a process of employee education, system testing, and development of and adherence to a good security policy in order to minimize the risk of intrusions.

3. ***An IDS is not a substitute for a good security policy:***

   As with other security and monitoring products, an IDS functions as one element of a corporate security policy. Successful intrusion detection requires that a well-defined policy must be followed to ensure that intrusions and vulnerabilities, virus outbreaks, etc. are handled according to corporate security policy guidelines.

4. ***Human intervention is required:***

   The security administrator or network manager must investigate the attack once it is detected and reported, determine how it occurred, correct the problem and take necessary action to prevent the occurrence of the same attack in future.

Lastly, Tight integration between host and network based IDS is very much necessary. As shown in Picture1, it is advised to use network based IDS inside and outside the

© SANS Institute 2001, Author retains full rights.

firewall or between each firewall in a multi-layered environment and host based IDS on all critical or key hosts. Also, as shown in Picture1, it is important although not always necessary to have an integrated deployment of host based and network based Intrusion Detection Systems.

As security continues to move to the center stage, managers and network administrators alike are beginning to focus their attention on intrusion-detection technology. While modern-day IDSes are far from bulletproof, they can add significant value to established information-security programs. With vendors working on eliminating the shortcomings of Intrusion Detection Systems, the future looks brighter for this technology.

List of References:

1. Watching the Watchers: Intrusion Detection by Greg Shipley

   http://www.networkcomputing.com/1122/1122f3.html

2. Network vs Host-based Intrusion Detection; A guide to Intrusion Detection Technology

   http://secinf.net/info/ids/nvh_ids/

3. Intrusion Detection: Challenges and myths by Marcus J. Ranum

   http://secinf.net/info/ids/ids_mythe.html

4. State of the Practice of Intrusion Detection Technologies

   http://www.sei.cmu.edu/publications/documents/99.reports/99tr028/99tr028exsum.html

5. Protect your network with an Intrusion Detection system, Gartner Research

   http://www.techrepublic.com/article.jhtml?src=search&id=r00520010209ggr01.htm

6. FAQ: Network Intrusion Detection Systems by Robert Graham

   http://www.ticm.com/kb/faq/idsfaq.html

7. Limitations of Network Intrusion Detection by Steve Schupp

   http://www.sans.org/infosecFAQ/intrusion/net_id.htm

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: October 2nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Seattle 2013	Seattle, WAUS	Oct 07, 2013 - Oct 14, 2013	Live Event
SANS Baltimore 2013	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SEC760 Advanced Exploit Development for Penetration Testers	Baltimore, MDUS	Oct 14, 2013 - Oct 19, 2013	Live Event
SANS Bangalore 2013	Bangalore, IN	Oct 14, 2013 - Oct 26, 2013	Live Event
GridSecCon 2013	Jacksonville, FLUS	Oct 15, 2013 - Oct 17, 2013	Live Event
Healthcare Cyber Security Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 24, 2013	Live Event
Securing the Internet of Things Summit	San Francisco, CAUS	Oct 17, 2013 - Oct 22, 2013	Live Event
SANS Tokyo Autumn 2013	Tokyo, JP	Oct 21, 2013 - Oct 26, 2013	Live Event
ICS410	Sterling, VAUS	Oct 21, 2013 - Oct 25, 2013	Live Event
October Singapore 2013	Singapore, SG	Oct 21, 2013 - Nov 02, 2013	Live Event
SANS Dubai 2013	Dubai, AE	Oct 26, 2013 - Nov 07, 2013	Live Event
FOR572 Advanced Network Forensics and Analysis	Washington, DCUS	Oct 28, 2013 - Nov 02, 2013	Live Event
SANS Chicago 2013	Chicago, ILUS	Oct 28, 2013 - Nov 02, 2013	Live Event
MGT415 at (ISC)2 SecureSoCal 2013	Manhattan Beach, CAUS	Oct 31, 2013 - Oct 31, 2013	Live Event
SANS South Florida 2013	Fort Lauderdale, FLUS	Nov 04, 2013 - Nov 09, 2013	Live Event
SANS DHS Continuous Diagnostics & Mitigation Award (CDM) Workshop	Washington, DCUS	Nov 06, 2013 - Nov 06, 2013	Live Event
MGT415 at (ISC)2 SecureDallas 2013	Dallas, TXUS	Nov 06, 2013 - Nov 06, 2013	Live Event
SANS Pen Test Hackfest Training Event and Summit	Washington, DCUS	Nov 07, 2013 - Nov 14, 2013	Live Event
SANS Sydney 2013	Sydney, AU	Nov 11, 2013 - Nov 23, 2013	Live Event
SANS Korea 2013	Seoul, KR	Nov 11, 2013 - Nov 23, 2013	Live Event
Cloud Security @ CLOUD Expo Asia	Singapore, SG	Nov 13, 2013 - Nov 15, 2013	Live Event
SANS London 2013	London, GB	Nov 16, 2013 - Nov 25, 2013	Live Event
SANS San Diego 2013	San Diego, CAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
FOR585 Adv Mobile Device Forensics	Vienna, VAUS	Nov 18, 2013 - Nov 23, 2013	Live Event
Asia Pacific ICS Security Summit & Training	Singapore, SG	Dec 02, 2013 - Dec 08, 2013	Live Event
SANS San Antonio 2013	San Antonio, TXUS	Dec 03, 2013 - Dec 08, 2013	Live Event
SANS Cyber Defense Initiative 2013	Washington, DCUS	Dec 12, 2013 - Dec 19, 2013	Live Event
SANS Oman 2013	Muscat, OM	Dec 14, 2013 - Dec 19, 2013	Live Event
SANS Golden Gate 2013	San Francisco, CAUS	Dec 16, 2013 - Dec 21, 2013	Live Event
SANS Forensics Prague 2013	OnlineCZ	Oct 06, 2013 - Oct 13, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced