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.

IDS - Today and Tomorrow

During the course of my research on this topic, I found many disclaimers stating that the author is not predicting the future of Intrusion Detection Systems (IDS), but merely pointing out " ... the emerging tools and trends."1 This is a wise approach and this paper shall carry a similar disclaimer: This paper is not intended to predict the future, but bring to light emerging technologies and trends in the field of IDS that could make the life of the security specialist easier (if there is such a thing). For someone tha...

Copyright SANS Institute
Author Retains Full Rights

AD

IDS – Today and Tomorrow
Thomas Goeldenitz
January 22, 2002

Introduction

During the course of my research on this topic, I found many disclaimers stating that the author is not predicting the future of Intrusion Detection Systems (IDS), but merely pointing out " … the emerging tools and trends."[1] This is a wise approach and this paper shall carry a similar disclaimer:

> This paper is not intended to predict the future, but bring to light emerging technologies and trends in the field of IDS that could make the life of the security specialist easier (if there is such a thing).

For someone that is new to the field of intrusion detection, it should be of interest to know where this technology is heading and which IDS technologies to deploy, while keeping in mind future IDS developments. It will also help in formulating questions to ask an IDS vendor on what features their IDS has and where they plan on taking their product in the future.

The IDS Concept

An IDS (as we currently use the term) is one of many tools that an organization may use to help determine if their network or server environment has experienced an unauthorized intrusion. An IDS may be used as hardware installed on the network or as an agent on an existing piece of hardware that is connected to your network.

The IDS has often been compared to a house alarm system, which it does act like in the sense of providing an alert when a predefined event occurs. Unlike a house alarm, it will provide you with the type of event that occurred, when and where in your network/server environment the intrusion occurred and the source of the intrusion (if the IP address has not been spoofed). Some IDS's even allow a user to configure an automated response to an alert, such as shunning and dropping an IP session.

The concept of Intrusion Detection Systems has been around for a couple of decades and has evolved into a viable and highly recommended piece of security technology that a company should implement in its arsenal of security tools. An IDS is not a "silver bullet" when it comes to securing your infrastructure. Rather, it is an integral part of a multi-layered security architecture that consists of several security tools deployed throughout your network and server environment. Before exploring what the future may hold for IDS's, it is important to note the current state of IDS technology.

Current State of IDS

For the most part, IDS's currently come in two varieties:

- Network Intrusion Detection System (NIDS)
- Host Intrusion Detection System (HIDS)

The methods that either the NIDS or HIDS uses to determine if malicious activity is occurring can be based upon known signatures or anomalies against normal patterns of activity. Which method a particular IDS uses depends upon the vendor and product. The following is a brief explanation of the two main IDS categories.

Network Intrusion Detection Systems

Network Intrusion Detection Systems are usually deployed as a dedicated component on a network segment. There is some debate as to where to place a single NIDS (inside or outside of a firewall), but most agree that multiple NIDS are better. It will then compare captured network data to a file of known malicious signatures. If there is a match, the IDS will log and send an alert according to how it was configured by the network or security administrator.

Some of the advantages and disadvantages of NIDS are:

ADVANTAGE	*DISADVANTAGE*
Breadth of Coverage. An entire subnet may be covered by one NIDS.	False / Positive Alerts
Stealth	Cannot Analyze Encrypted Traffic

Minimal Install/Upgrade Impact to Network	NIDS only as strong as the latest signature update. New or variations in attack patterns will not register.
Avoid DoS that would otherwise affect a Host	Latency between time of attack and time of alert. By the time an alert is received the damage may have already occurred.
Ability to Identify Network Layer Errors	Difficulty in processing packets in a congested network.
Operating Environment Independent	Does not indicate whether the attack was successful.

Host Intrusion Detection Systems

Host Intrusion Detection Systems are usually deployed on a host computer. Instead of monitoring a network segment, a HIDS only monitors the host on which it is installed. A HIDS would typically be placed on business critical hosts and on servers in a DMZ that are most likely to be compromised. The HIDS operates by monitoring changes to a number of variables on the host system.

This may include:

- System Processes
- Registry Entries
- CPU Usage
- File Access and Integrity Checking
- and many other variables.[2]

Any exceeded thresholds or suspicious file changes will send an alert.

Some of the advantages and disadvantages of HIDS are:

ADVANTAGE	*DISADVANTAGE*
Ability to associate a user to an event	Information provided by the HIDS becomes unreliable as soon as an attack on that host has been successful.
May detect attacks that are not detectable by NIDS	When an OS is brought down by an attack, the HIDS goes down with the system.
Can analyze encrypted data that has been decrypted on the host.	In order to monitor several hosts, an HIDS would need to be placed on each host.
Ability to provide information about a host during an attack on that host.	HIDS are not able to detect network scans.
	HIDS may be ineffective during a DoS attack
	HIDS require resources of the host in order to operate.

Each type of IDS has its strengths and weaknesses. A best practice is to utilize a variety of solutions and place them into strategic areas throughout your infrastructure. Now that we have taken a look at the current IDS technologies, we will now begin to explore what tomorrow (which may be as soon as today) will bring in the field of IDS technology.

IDS – Future Possibilities

The name of this section was almost called "The Future of IDS", but as stated earlier there is no way to predict, with absolute certainty,

what the future will hold. Instead, this section will focus on possible changes in the IDS industry.

Hybrid IDS implementations seem to be a logical approach in establishing proper intrusion detection coverage. The key is coverage, to ensure that an IDS deployment will cover the weaknesses of other types of IDS's. The hybrid approach is achieved by using various types of IDS's and placing them at "… critical network aggregation and entry points …"[3], and on hosts that support business critical functions.

This would include:

- NIDS
- HIDS
- Hybrid IDS, such as the Shim IDS

The Shim IDS acts like a NIDS, but is installed on a host as an agent. This particular type of IDS captures the network traffic that is sent to that host and would have to be installed on every host that a user would like to have covered.

As Information Technology advances, the "need for speed" seems to be a driving factor. In network environments, it is becoming more common to see gigabit speeds. The IDS hardware and software that vendors produce needs to keep pace with the increase in speed, and it is already evident that they are keeping pace. It is important to note that this is a factor to seriously consider when deploying IDS's, because an underpowered IDS will not be able to capture enough traffic to perform the function it was meant to perform.

The generation of False/Positives alerts is another area where IDS's could use improvement. This is an area where vendors have been making a lot of innovations. Many IDS's now allow the user to tune their IDS to platform specific alerts. More sophisticated methods employ statistics, algorithms and logic. The filtering of false/positives is an important feature to consider when purchasing an IDS. This can become a quagmire of wasted analytical time and potentially allow intruders undetected access. The successful filtering of false/positive alerts will continue to improve as advances in the logic and system intelligence increases.

One concept that that will have a significant impact on Intrusion Detection is Data Mining and Correlation. Data Mining is, as stated by Paul Reeder, "… essentially the creation of a complex database that records data related to specific activities or environment over long periods of time. A front-end application is developed using algorithms that process the accumulated data in a way that allows knowledge seekers to discover patterns or develop models."[4] This would provide a powerful tool in analyzing the reams of data that is collected by Intrusion Detection Systems. To add to the power of this concept, would be the implementation of a standardized Intrusion Detection protocol.

The implementation of a standardized Intrusion Detection exchange protocol is currently being developed by the Internet Engineering Task Force - Intrusion Detection Working Group (IETF-IDWG). This protocol would allow the various Intrusion Detection Systems to communicate in a standard format.[5] Combined with data mining and correlation, this would provide the security analyst a wealth of information that can be collected from any type of IDS that has been deployed in their infrastructure. It remains to be seen whether a standardized protocol would be adopted by the commercial IDS vendors. Presently, each vendor uses proprietary protocols to communicate.

Another change that may occur is how the term IDS is used in the future. Currently, when I hear about Intrusion Detection Systems, I think of the NIDS, HIDS and. In the future, I believe the term IDS will be used in the context of a combined arsenal of security tools that are integrated into a single management console.

This arsenal would consist of:

- Network Intrusion Detection Sensors and Agents
- Host Intrusion Detection Sensors and Agents
- Hybrid IDS
- Firewalls
- Routers
- Mail, Web, DNS Servers, etc.[6]
- Application / Database / Operating System / Audit Logs

These tools provide various logs, audit trails, policy violations and alerts. All of this data could be collected and aggregated into a single database. The database could then be analyzed using data mining concepts to determine and verify if an intrusion has occurred. To achieve this utopia of Intrusion Detection would be a monumental task. The protocols used by the various systems would need to be standardized and the data mining algorithms would need to be developed. Not to mention the actual design of the database and the intricate relationships that may or may not exist between collected data. Also, the amount of data collected in a busy network would place a great deal of stress upon the servers, applications, databases and networks established to perform this task.

Conclusion

The field of IDS has evolved from the days of manually " … discovering security incidents via recurring reviews of system audit logs and accounting files …"[7] to automated systems that analyze signatures and anomalies. Intrusion detection systems continue to evolve at a rapid pace as the demand for information technology security increases.

In light of the recent tragic events, it has taken on an even greater urgency to further enhance the efficiency and accuracy of intrusion detection systems. Many of the topics discussed in this paper are in various stages of research and implementation.

Performance issues are being addressed with systems that can effectively handle gigabit speed. Hybrid IDS's are here today with new variants being developed for tomorrow. And some vendors have already begun deploying management consoles, such as Cisco's CSPM, that centralize the management and analysis of their NIDS's and HIDS's. We are well on our way into the future of IDS.

References

1. Northcutt, Stephen and Novak, Judy Network Intrusion Detection An Analyst's Handbook Second Edition New Riders 2001. P203-213

2. Ranum, Marcus J. "Coverage in Intrusion Detection Systems" 6 June 2001
URL: http://philby.ucsd.edu/~cse291_IDVA/papers/orig_names/Coverage-in-IDS-White-Paper-final.pdf (16 Jan. 2002)

3. Yocom, Betsy and Brown, Kevin "Intrusion Battleground Evolves" 8 Oct.2001
URL: http://www.nwfusion.com/reviews/2001/1008bg.html (16 Jan. 2002)

4. Reeder, Paul "Intrusion Detection, The Next Generation: Making it Practical"
URL: http://8wire.com/articles/?aid=2168 (16 Jan. 2002)

5. IETF-IDWG "Implementing the Intrusion Detection Exchange Protocol" 2001
URL: http://www.acsac.org/2001/abstracts/wed-1030-a-pollock.html (16 Jan. 2002)

6. McAnderson, Brenda and Ramstedt, Paul "Intrusion Detection Technology: Today and Tomorrow" 18 Nov. 1999
URL: http://www.first.org/events/progconf/2000/D3-03.pdf (16 Jan. 2002)

7. Tanase, Matthew "The Future of IDS" 4 Dec. 2001
URL: http://www.securityfocus.com/infocus/1518 (16 Jan. 2002)

8. ITL Bulletin "Acquiring and Deploying Intrusion Detection Systems" Nov. 1999.
URL: http://www.itl.nist.gov/lab/bulletns/nov99.htm (16 Jan. 2002)

9. Messmer, Ellen "Intrusion Alert" 3 Dec. 2001
URL: http://nwfusion.com/news/2001/1203ids.html

to top of page | to Reading Room Home

Last Updated: May 22nd, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**