

By Aaron and Demetrios

Intrusion Detection Systems (IDS)

IDS detect attacks against your network by generating alarms when they observe an intrusive activity. Although many different IDSs exist, they each support a triggering mechanism. The common triggering mechanisms are:

1. Anomaly detection.
2. Misuse detection.

Anomaly detection is more complex than misuse detection, but it provides the capability to detect previously unpublished attacks.

The down side is that alarms are not correlated with specific known attacks. An alarm represents a deviation from normal user activity, and must be investigated by the system administrator.

Misuse detection can detect only the attacks for which it has signatures. End users know exactly which attacks trigger a signature-based IDS because signatures are listed in the signature Database. Providing updates to the signature DB in response to new attacks however, is a major challenge.

Both anomaly detection and misuse detection only represent potential ways to trigger intrusion alarms. In addition to IDS triggering, each IDS must also monitor your network at defined locations to obtain the data necessary for triggering mechanisms to function. The two common monitoring locations are the host and the network.

A. Host based IDSs (HID)

Check for intrusive activity on the actual hosts on your network. This activity might be error logs, system calls, and so on. The main benefit of a host based IDS is that it can determine the success of the attack because the IDS is on the actual host being attacked. The Host based IDS (HIDS) look at what is happening on the computer it is installed on. This allows the IDS to look very specifically at what is happening on that machine via the log files and/or the internal auditing systems. There are two main types of HIDS: host wrappers/personal firewalls and agent-based software.

Host wrappers or personal firewalls are configured to look at all network packets, attempted connections, or attempted logins to the monitored machine. Host-based agents are designed to monitor accesses and changes to critical system files and changes in user privilege.

Pros:

- * Able to detect a large range of local attacks.
- * Encryption is generally not in the way if the data is decrypted at the server.
- * No problem with switched networks.

Cons:

- * Each host often must be installed and maintained separately.
- * Because the IDS is on the host, the IDS may be attacked and disabled first.
- * May not see a widely dispersed network scan.
- * May get swamped in a Denial of Service Attack (DoS).
- * Consumes processing power and network resources of the server it's protecting

Additionally HIDS, have limited view of the network in relation to attacks. Most HIDS do not detect port scan against the network, therefore almost impossible for HIDS to detect reconnaissance scans against your network. These scans represent a key indicator to more attacks against your network.

N Network based IDSs (NID)

NIDS work by capturing data from one or more points central to the network and reporting back to a management console. The capture systems must be placed in the network such that they can see all passing traffic. In a fully switched network, there may be difficulties in capturing data unless you can configure your switches to pass a copy of all the traffic to a specific port for the IDS.

One or more sensors watch the network and generate alarms whenever they observe intrusive activity. The benefit of NIDS is that it does not have to run on every host in the network. Because the IDS is examining network traffic only, the developer is free to choose the best sensor platforms.

Pros:

- * You can listen to a fairly large network with just a few machines.
- * The system is transparent as the unit collects traffic information.
- * All traffic between the console and the NIDS collector can be encrypted or on a separate network for complete security.

Cons:

- * There may be a lot of traffic passing the system, possibly more than the system can process. This will cause difficulties in detecting intruders when loads are high. Hence need to install more and more sensors, so as to handle the traffic volume.
- * The need to process packets quickly may mean that you have to turn off some of the features to keep up with traffic volumes.
- * Fully switched networks can be difficult to capture as traffic is not replicated across all ports like it is in a non-switched network.
- * Unable to analyse encrypted traffic.
- * Fragmentation assembly

Network packets have a maximum size, if a connection needs to send a data that exceeds this maximum bound, the data must be sent in multiple packets. This is known as fragmentation. Receiving host then reassembles the fragmented packet, in to data.

Different OSs, reassemble the packet in different order, e.g. last to first, or First to last, the assemble order does not matter if fragment do not overlap; if they do the result is different for each assembly process. To examine the packet the network sensor must reassemble the packet, the problem involves using the correct assembly order, as an attacker may send packets with overlapping fragments to try to circumvent NIDS.s.

C. Hybrid IDSs

Sometimes, a developer combines multiple triggering mechanisms and monitoring locations in to a single IDS. This is known as a hybrid. The main incentive behind developing hybrid system is to increase the functionality of the IDS. A hybrid IDS may perform host based and network based monitoring. Another combination might combine anomaly detection with misuse detection. The hardest part of creating a successful hybrid system is to make the different functions work together in a user-friendly manner.

Conclusion

Treats are both internal and external. Prevention, detection and reaction are needed in combination. IDS are a very useful second line of defence, in addition to firewalls and other safeguards. IDS deployment, customization and management is generally not straightforward.

There are many IDS products currently in the market for example:

- . Tripwire - HIDS, file integrity checker.
- . ISS Real secure -HIDS and NIDS combined.
- . Cisco IDS - NIDS
- . Sysmantec Netprowler – NIDS
- . Snort NIDS (Open source)

Selecting right product depends on many factors including: cost, performance, stability of product and vendor, security objectives, ease of management etc.

IDS systems don't fully guarantee security, but when used with security policy, vulnerability assessments, data encryption, user authentication, access control, and firewalls, they can greatly enhance network safety.