Global Information Assurance Certification Paper

How to Choose Intrusion Detection Solution

Baiju Shah
July 24, 2001
Version 1.2e

Introduction

Network security has been an issue since computers have been networked together. The evolution of the Internet has increased the need for security systems. An important security product that has emerged is Intrusion Detection Systems (IDS).

In order to understand IDS properly, one must first have an understanding of *intrusions*. Intrusion is difficult to define because not everyone agrees on what is consider of an intrusion. Intrusions are defined as attempts to compromise confidentiality, integrity, or availability of data, or to bypass the security mechanisms of an IT system. An intrusion may be generally described as a sequence of related actions by a malicious adversary that results in the occurrence of unauthorized breaches to a target system or network.

What is Intrusion Detection?

The National Institute of Standards and Technology (NIST) defines intrusion detection as the process of monitoring the events occurring in an IT system and analyzing them for signs of intrusions. These intrusions are the results of attackers accessing systems from the Internet, authorized users of the systems who attempt to gain additional unauthorized privileges, and authorized users who misuse the privileges given to them.

The ideal Intrusion Detection System notifies appropriate person of an attack in progress with 100% accuracy, promptly, with complete diagnosis of the attack, and recommendations on how to block it. But such ideal systems do not exist.

Why do we need Intrusion Detection System?

It is a common misunderstanding that firewalls can recognize and block intruders. A firewall is simply a fence around a network, with a couple of well-chosen gates. A fence has no capability of detecting somebody trying to break in (such as digging a hole underneath it), nor can a fence differentiate somebody coming through the gate is allowed in. A firewall simply restricts access to the designated points on the network. Having Security cameras, motion detectors, and burger alarms can provide information about who is coming through allowed gates or if someone is digging a hole underneath, etc. These security devices can be configured to set off an alarm and notify housekeepers of any specious activity going around. Intrusion detection systems are the security cameras, motion detectors and burglar alarms. IDS can be configured to respond to predefined suspicious activities.

The underlying reasons for using intrusion detection systems are relatively straightforward: protect data and maintain systems integrity. Intrusion detection takes

one step further of basic measures of security mechanism such as firewalls and other access control. An Intrusion Detection System does not replace firewalls; firewalls are must in any corporate security foundation. Intrusion Detection Systems identify attacks against networks or a host that firewalls are unable to see. Having IDS to complement a firewall can provide an extra layer of protection to a system such as:

- Identifying attacks that firewall legitimately allow through (such as http attacks against web servers).
- Identifying attempts such as port scan or ping sweep.
- Notice insider hacking.
- Provide additional checks for holes/ports opened through firewalls, intentionally or unintentionally.

Types of Intrusion Detection

Now that reasons to consider having intrusion detection are defined, next issue to determine is what type of intrusion detection system best suits an organization's requirements to strengthen its network security.

IDS can be viewed two different ways: how to detect, where to detect.

How to detect: These are the *types* of Intrusion Detection tools. Intrusion can be detected by signature/pattern analysis, or anomaly/heuristic analysis.

- **Signature/pattern based IDS** is also known as the *knowledge based* IDS. This intrusion detection system contains a database of known vulnerabilities. It monitors traffic and seeks a pattern or a signature match. IDS can be placed on a network to watch network vulnerabilities and can be placed on host.

  Benefits of Signature/Pattern based IDS

  - Provides very low false alarms as compare to Heuristic based IDS.
  - Provides detail contextual analysis providing steps for preventive or corrective actions.

  Drawbacks of Signature/Pattern based IDS

  - It is difficult to gather knowledge about known attacks and keeping up-to-date with new vulnerabilities.
  - Signatures and corrective recommendations are generalized; thus it makes it harder to understand them.
  - Knowledge about attacks is very focused, dependent on the operating system, version, platform, and application. As a result, intrusion detection tool is closely tied to a given environment.

  Signature/Pattern based IDS are more popular and commercially used than Heuristic/Anomaly detection based IDS. Major vendors such as ISS offer network based and host based signature detection.

- **Heuristic/Anomaly detection** is also known as the *behavior based* IDS. These types of IDS tools analyze traffic patterns and infer *normal* activity. It then, applies statistical or heuristic measures to events to determine if they match the

model/statistical *normal*. Events outside accepted *normal* behavior generate alerts.

Benefits of Anomaly/Heuristic based IDS

- Identify any possible attack.
- Identify attacks that we haven't seen before – Or close variants to previously-known attacks

Drawbacks of Anomaly/Heuristic based IDS

- *Normal* can change over time, introducing the need for periodic online retraining of the behavior profile, resulting either in unavailability of the intrusion detection system or in additional false alarms.
- Current implementations provide high false alarms.
- Requires expertise to figure out what triggered an alarm.

There are many research projects in works right now with utilizing Heuristic/anomaly based IDS such as IDES (Intrusion Detection Expert System), GrIDS (Graph-based Intrusion Detection System), and Emerald (Event Monitoring Enabling Responses to Anomalous Live Disturbances).

Where to detect: These are *deployment techniques* of Intrusion Detection. A sensor can be placed on a network segment or on a host. They represent the products of Intrusion Detection System.

- **Network based Intrusion Detection Systems** monitor the traffic on the entire network segment. Similar to a network sniffer, network based IDS tools collect raw network packets as the data source from the network or a hub/switch. However, network based IDS can reassemble packets, look at headers, determine if there are any predefined patterns or signatures match from the network traffic to generate alerts, and automatically take action based on the content of the packet. RealSecure network agents from ISS and SecureIDS from Cisco are examples of Network based IDS.

  Benefits of Network based IDS

  - Monitor network for port scans.
  - Monitor network for malicious activity on known ports such as http port 80.
  - Identify various sorts of spoofing attacks.
  - Does not impact network performance.
  - Increased tamper resistant.
  - Operating systems independent.

  Drawbacks of Network based IDS

  - Packets lost on flooded networks.
  - Reassemble packets incorrectly.
  - No understanding of O/S specific application protocols such as SMB.
  - No understanding of obsolete network protocols.
  - Does not handle encrypted data.

- **Host-based IDS** operate on information collected from within an individual computer system. Host-based IDSs utilize information sources such as operating system audit trails, C2 audit logs, and system logs. Operating system audit trails are usually generated at the innermost (kernel) level of the operating system, and are therefore more detailed and better protected than system logs. System logs are collected in very compact form but contain application or system specific events. Host based IDS operate on the logs and not actual traffic. RealSecure host agents from ISS is an example of Host based IDS.

  Benefits of Host based IDS
  - Monitor events local to a host, and can detect successful or failure of attacks that cannot be seen by a network-based IDS.
  - Operate in an environment in which network traffic is encrypted.
  - Unaffected by switched networks and is independent of network topology.
  - Monitor system specific activities such as file access, user access, etc.
  - Provide thorough information gathered via logs and audit; for example Kernel logs know who the user is.
  - No additional hardware is needed to implement Host based IDS solution.
  - When Host-based IDSs operate on OS audit trails, they can help detect attacks that involve software integrity breaches.

  Drawbacks of Host based IDS
  - Host based IDS are harder to manage as information must be configured and managed for every host individually.
  - Host based IDSs are network blind and cannot detect a network scans or other such surveillance that targets entire network.
  - If the host is compromised, collected log data by the Host based IDS can be subverted.
  - Disabled by certain denial-of-service attacks.
  - Uses operating system audit trails as an information source. The amount of information can be immense and can require additional local storage on the system.
  - Inflict performance deficiency on monitored host.

Effectively Deploying an IDS Solution

Choosing IDS is not easy as picking a technology or product or vendor. Effectively deploying an IDS solution requires planning, strategic deployment, maintenance, monitoring, responding to an incident, and handling of an incident.

Planning

None of the IDS products or technologies can deliver a silver bullet for solving security problems, but combined intelligently, they provide a solid solution for detecting threats to a network. Both host based and network based deployment strategies have unique benefits and strengths that compliment each other. Financial investment and

budgetary limitations are major factors in deciding an IDS solution. No single product or technology is an answer to security solution, but combining both of the IDS technologies will greatly improve any networking environment resistance to attacks and misuse. The following scenarios give some information about how different IDS solutions are more effective for a given environment.

Scenario 1: A small office network has only users requiring file/print servers, and emails in a network segment and the DMZ has private web servers. In this scenario, Network based IDS solution in both segment may be sufficient to monitor internal attacks, malicious users, SYNFlood attacks, etc.

Scenario 2: A company has critical web servers at a hosting facility. These web servers are vulnerable to SYNFlood, Smurf, TearDrop, Back Orifice, Port Scan, web page defacement, etc. Implementing a combination of both Network based and Host based IDS will provide best solution; the Network based IDS tool will detect attacks such as SYNFlood, and Port Scan, Host based IDS tool will detect attacks such as web page defacement.

Planning begins by establishing organization's acceptable tolerance for *Threat/Vulnerability/Risk/Impact*. In order to accomplish this tolerance, first identify the threats to a system, compare them to vulnerabilities. Secondly, determine how these systems are at risk. And then, determine if systems are compromised in any way, how it will impact these system and the business. Such analysis may be beyond technical requirement and may involve management decision. Management team has to be the decision maker in establishing an acceptable ratio and security team should design countermeasures for risks greater than what management is will to accept.

Strategic Deployment

Security community believes less than 15% of the intrusions to any systems are detected. A poorly deployed security solution provides a false sense of security. After determining what must be secured, other necessary requirements are listed below:

- Where IDS should be placed.
- How IDS will assist in securing systems.
- What method of intrusion to use in detection such log base detection, signature based or heuristic base detection.
- Where should the detection sensor be placed, on a network or on a host or combination as needed.

Successfully deployment of an IDS solution does not make it fully secured. As Bruce Schneir put it, *"security is a process not a product."* Process has just began.

Maintenance

New vulnerabilities that threaten any business are being discovered regularly. As

business requirements change, so will the security needs. Therefore, a security policy will also change to accommodate these changes. Along with other security products, IDS product will also need to be updated. IDS product vendor will also provide patches and upgrades that will be needed to keep up to date. Sensors can detect only vulnerabilities they know about; if they don't know about new vulnerabilities, they can't detect them. Having a process in place that keeps IDS up-to-date with latest knowledge base and detection definitions is a vital part of maintaining the IDS effectiveness.

IDS Monitoring

Counterpane Security, mentions in a white paper a crucial need for monitoring IDS by stating "*If security products were perfect, there would be no need for detection. If computer programs never had security bugs, there would be not need for monitoring. But protection mechanisms are not perfect, and programs have bugs. They work but they need to be monitored."* If it is not monitored, Intrusion detection by itself offers a little value. Let's say a bank has security cameras. Having various cameras do not make bank secured. If no one watches these cameras, they would not be able to detect as a suspicious person coming in to the bank and robbing them. Sure everything is recorded but it could have been prevented. Just like that, monitoring IDS is very important. Network attacks can happen any time of the day not just in business hours. The monitoring goal of IDS is to positively identify real attacks from false positives and false negatives.

Incident Response

Security products provide protection, and that protection is primarily useful as a delaying tactic: it gives the defender time to detect the attack and respond. Why bother detecting an attack in the first place, if nothing is going to be done about it? Detection without response is useless; it's an alarm ringing with no one listening. Incident response team is needed to sort out real attacks from false positive and false negatives. Response to an incident can be automatic or manual. Automatic response work against automated attacks but a manual response may be required for an intelligent attack. The mind behind the attack is the real enemy.

Incident Handling

Stephen Nortcutt gave a very good example in his book, *Network Intrusion detection*.

> *For example, you are certified in administrating CPR. Once you are certified, how confident would you feel if you had to administrate CPR after few months of your training? Stephen calls these "gulp" moments.*

It is very important to have a well-defined and well-documented security policy that contains incident handling procedures. Define incident handling team and their designated tasks. Improperly handled information gathering may not be admissible in court of law.

Once an attack is detected, even certified incident handler may panic. Experience incident handlers have recommend following steps:

- Remain calm; don't hurry.
- Notify your organization's management.
- Provide a game plan (with options if possible).
- Apply need-to-know.
- Use out-of-band communications; avoid email and other network-based communications channels.
- Take good notes, good enough to serve as evidence in a court of law.
- Determine how the incident happened and how it was detected.
- Contain the problem; pull the network cable if needed.
- Back up the system(s), and collect evidence.
- Assess the impact and damage from the incident
- Eradicate the problem and get back in business.
- Lessons learned, apply what you have learned.

And depending on the seriousness of the attack, an organization may choose to pursue legal action against who was responsible for the attack. For such process, consulting with Network Forensic experts may become necessary.

Conclusion

As Marcus Ranum put it, an ounce of prevention is worth pound of detection. While, I agree with that, my experience says, prevention may not be sufficient without detection. Intrusion Detection Systems are becoming crucial part of security implementation.

Continuing with the example of the security cameras, motion detectors and burglar alarms, these tools can provide added security to a home but cannot stop break-ins. Similarly, IDS devices can provide additional security but cannot stop intrusions. If security guards are monitoring the home burglar alarms systems and provide assistance by calling police when an alarm goes off. Security professionals who can react when an IDS alarms, can provide additional depth to a line of defense, therefore, making it likely for attacker to give up before much damage has been done.

As discussed, security is not about putting sensors on a network and/or hosts; it requires skills and expert resources to successfully run the operation. If an organization does not have the proper in-house resources to monitor and respond to IDS alerts, third party assistance should be sought. By utilizing their expertise and resources to monitor and respond to a network 24 hours a day, can serves as a critical defense shield.

Intrusion detection systems are crucial in securing any systems but the effectiveness comes only from proper planning, deploying, monitoring, and responding to intrusions.

References

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

http://www.nswc.navy.mil/ISSEC/CID/

http://csrc.nist.gov/publications/drafts/idsdraft.pdf

http://www.counterpane.com/msm.html

http://documents.iss.net/whitepapers/nva.pdf

http://documents.iss.net/literature/RealSecure/ids_eval.pdf

http://documents.iss.net/whitepapers/int_detect.pdf

http://documents.iss.net/whitepapers/nvh_ids.pdf

http://www.sans.org/newlook/resources/IDFAQ/knowledge_based.htm

http://www.sans.org/newlook/resources/IDFAQ/behavior_based.htm

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

http://secinf.net/info/ids/IDFAQ/incident_handling_steps.htm

http://www.sdl.sri.com/programs/intrusion/

Class notes from *Intrusion Detection & Network Forensics* by Marcus Ranum

Network Intrusion Detection, An Analyst's Handbook, Second Edition by Stephen Northcutt and Judy Novak

Intrusion Detection by Edward Amoroso

Last Updated: June 25th, 2018

Upcoming Training

SANS London July 2018	London, United Kingdom	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, Singapore	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DC	Jul 14, 2018 - Jul 21, 2018	Live Event
SANSFIRE 2018 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 16, 2018 - Jul 21, 2018	vLive
Mentor Session - SEC401	Jacksonville, FL	Jul 17, 2018 - Aug 28, 2018	Mentor
Community SANS Annapolis Junction SEC401	Annapolis Junction, MD	Jul 23, 2018 - Jul 28, 2018	Community SANS
SANS Riyadh July 2018	Riyadh, Kingdom Of Saudi Arabia	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PA	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, India	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MA	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, Australia	Aug 06, 2018 - Aug 25, 2018	Live Event
San Antonio 2018 - SEC401: Security Essentials Bootcamp Style	San Antonio, TX	Aug 06, 2018 - Aug 11, 2018	vLive
Mentor Session - SEC401	Ankara, Turkey	Aug 08, 2018 - Oct 03, 2018	Mentor
SANS New York City Summer 2018	New York City, NY	Aug 13, 2018 - Aug 18, 2018	Live Event
Northern Virginia- Alexandria 2018 - SEC401: Security Essentials Bootcamp Style	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	vLive
SANS Northern Virginia- Alexandria 2018	Alexandria, VA	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VA	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Chicago 2018	Chicago, IL	Aug 20, 2018 - Aug 25, 2018	Live Event
Mentor Session AW - SEC401	Raleigh, NC	Aug 22, 2018 - Aug 29, 2018	Mentor
SANS San Francisco Summer 2018	San Francisco, CA	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, Japan	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, Netherlands	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FL	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS Baltimore Fall 2018	Baltimore, MD	Sep 08, 2018 - Sep 15, 2018	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201809,	Sep 11, 2018 - Oct 18, 2018	vLive
SANS Munich September 2018	Munich, Germany	Sep 16, 2018 - Sep 22, 2018	Live Event
SANS London September 2018	London, United Kingdom	Sep 17, 2018 - Sep 22, 2018	Live Event
SANS Network Security 2018	Las Vegas, NV	Sep 23, 2018 - Sep 30, 2018	Live Event
Mentor Session - SEC401	Columbia, SC	Oct 02, 2018 - Nov 13, 2018	Mentor
Community SANS Ottawa SEC401	Ottawa, ON	Oct 15, 2018 - Oct 20, 2018	Community SANS