Interested in learning more about security?

SANS Institute InfoSec Reading Room

Selecting an Intrusion Detection System

Selecting an intrusion detection system (IDS) to protect your network is a decision that should not be made lightly, quickly, or without a firm understanding of the technology, options, or the potential impacts. The decision process can be divided into the following steps: identify the need, gain a general understanding of intrusion detection systems, gain a detailed understanding of the network, evaluate various IDS systems, and determine policy and procedures.

Kathleen Buonocore
GSEC-SANS Security Essential Certification
Selecting an Intrusion Detection System

Selecting an Intrusion Detection System

Selecting an intrusion detection system (IDS) to protect your network is a decision that should not be made lightly, quickly, or without a firm understanding of the technology, options, or the potential impacts. The decision process can be divided into the following steps:

1. Identify the need
2. Gain a general understanding of intrusion detection systems
3. Gain a detailed understanding of the network
4. Evaluate various IDS systems
5. Determine policy and procedures

1. Identify the need

Many times the first obstacle is convincing management –that may not have an information technology background- that such an investment is required. Questions concerning the additional cost of equipment, staffing and training will have to be addressed.

The key is to demonstrate that what needs protection isn't the servers, workstations, file servers, or other network devices but what resides on those devices- the company data. The answers to a few questions can often help to illustrate the important role of increased network security:

- How important is the security of company data? What if one morning all the databases were blank or altered? What if a year's worth of research on a new product was in the hands of a competitor?

- What are the potential loses? Lost of data can result in unplanned costs required by efforts to recover or recreate the data, but also there can be a lost of confidence in the company, that over time may prove more costly. Customers want to believe their personal information is safe, business partners want shared company secrets to be just that.

- What is the potential for future attacks? Has the company been a target before? Have other comparable companies been targeted? Is the company involved in a sensitive or controversial field? Is there a relationship to a government agency that may increase the possibility of attack?

- Has your company been targeted before? Too often this is the one that will get the checkbooks opened-especially if the attack was successful, costly, and

caused public embarrassment.

2. Gain a general understanding of intrusion detection systems

It is important to insure is that the purpose of an IDS is understood. The name seems to imply the purpose but taking an extra step may help prevent future misunderstandings. Network security isn't something that a single system can provide. Passwords still need to be used, protected, and managed, anti- virus programs, proper file permissions, system audits all need to be employed, and overall good network practices and policies will be always required. No one should think of an IDS as a cure all or easy fix. What an IDS can do is detect, report, and provide limited response to an activity that maybe harmful to the integrity of the network and the data stored, processed, or shared by users of that network[3].

How does an IDS "know" what type of activity maybe harmful or unwanted? Detection can be based on anomaly detection or signature recognition:

- Using anomaly detection the IDS learns a baseline for a system in terms of CPU utilization, file usage, user logins and other activity. For example if a user is normally logged in Monday to Friday between 8AM and 5PM then suddenly attempts to login at 2AM on a Saturday morning the system can alert the administrator to activity not normal for the user[1].

- Using signature recognition the IDS examines each packet for a programmed match of known attack patterns. The string "/cgi-bin/phf?" can trigger an alarm that someone maybe looking for a vulnerable CGI script on a web-server. Many commercial IDS systems are signature based, having several hundred signatures available for selection in a database[1].

Unfortunately either anomaly or signature based detection are perfect. Both produce false positive alerts. A false positive is report of an event that is legitimate activity for the user, source, and/or destination system. The user that was logging in Monday to Friday had a normal work schedule rotation that caused the IDS to produce the alert. System administrators will have to study the alerts and causes to fine-tune the detection system to reduce the occurrences of false positive alerts. The probability is that false positives will never be totally eliminated but can be reduced. However it is better to have an IDS produce a manageable number of such alerts then ignore possible intrusions[5.]

Aside from different types of detection methods there are different types of intrusion detection systems-network- or host-based- each having a particular purpose:

- A network-based IDS examines all packets on the network. Depending on several factors more then one Network IDS may be required for full coverage of the network.[2] The strengths of a network- based IDS are:

- Low cost of ownership as one IDS placed at a critical network entry point can provide security for multiple systems.

- Network-based IDS examine the packet header and payload allowing identification of attacks host based systems can miss.

- Real time detection and response to an identified attack. The user determines the response and depending on the IDS deployed can include notification, termination of the session, and recording of the session for analysis and use as evidence.

- Detection and reporting/recording of unsuccessful attacks that can be used in the evaluation of the security posture/policies.

- Network-based IDS are not dependent on the host operating system to detect attacks. Host-based IDS rely on the audit logs of the operating system, application, or other system logs to identify an attack[3].

❖ Host- based IDS examines the packets intended for one computer. This is type of IDS is found on highly sensitive systems.[2] The strengths of a host-based IDS are:

- Host- based IDS can verify the success or failure of an attack since the reporting is based on examinations of the events recorded in the system logs.

- Specific system activities are closely monitored. For example file access, changes to file permissions, user logon/logoff, and administrator functions can be monitored at a level of detail greater then a on a network-based IDS.

- Attacks can be detected that don't cross the point of network entry protected by the network-based IDS. Actions that occur at the keyboard of the monitored server will be detected and reported by the host- based IDS.

- Encrypted traffic often leaves network IDS blind to an attack but the host-based IDS examines the traffic after it is de-encrypted by the host operating system.

- Host- based IDS are installed on the existing server-no additional system is required. The cost of initial deployment is reduced by the lack of equipment requirement[3].

Network- and host-based IDS each have strengths and purpose. Together the two can be deployed to provide general protection for the entire network and specific protection for select systems. Either can be deployed separately to provide specific protection depending on the requirement. A mixture of both network and host based IDS can provide comprehensive protection. One decision point in selecting an IDS is network and/or host based IDS-to make this decision knowledge of the network is key.

3. Gain a detailed understanding of the network

Understanding the network topology, as well as the purpose and function of various systems is essential. Depending on the size and complexity of the company network identifying critical systems and the network configuration maybe quite simple or not. A comprehensive examination of the network is mandatory:

- Is there a single network management division or is the network management functions divided between various departments based on function? Identifying domain controllers and mail servers is only the start. Does the Human Resources Department have a database server that contains sensitive employee insurance records? Does the Research and Development Division have separate systems for complex applications?

- How many entry points are there to the network? Explaining that a successful intrusion wasn't detected by the network-based IDS because the intruder came in "the other, unknown, unprotected door" isn't good material for the next evaluation.

- Are there firewalls on the network? (If so, the deployment of the network-based IDS- in front of or behind the IDS-will have to be determined. In front of the firewall the IDS will record attacks that may be blocked by the configuration of the firewall but this data can be used to tune the IDS. Behind the firewall only attacks that got though the firewall would be reported and require attention.)

- Are there switches on the network? This information is needed to determine the placement and types of IDS systems deployed.

- How much money is available? The amount will have a definite impact on the selection. A decision may have to be made to provide host- based IDS to protect selected systems while going without network -based IDS.

4. Evaluate various IDS systems

Evaluating IDS systems can be time consuming but is a very important factor in the decision process. First there is the need to learn who offers what and compare that to the identified requirements. Most vendors offer trial programs for use and evaluation. Aside from network vs. host based systems there are other considerations:

- Can the network- and host- based systems be integrated into a single management system that allows for alert viewing on the same console.

- Are there event correlation capabilities that decrease triage efforts and response time?

- What operating systems are supported?

- How often is the signature database updated?

- Which system supports the network topologies?

- What kind of system best fits with the existing operation?[12]

There are many vendors of IDS systems as well as free systems available. There is no intention to list all the vendors or makers of these systems or to recommend one system over an other. The only purpose in identifying any particular systems is to demonstrate available options. There are several systems for selection:

- Cisco offers the Cisco Secure IDS product line of network-based systems.[6]

- Internet Security Systems' Real Secure offers both network - and host -based solutions and the NetworkICE line of products.[7]

- Symantec offers Intruder Alert, a host -based IDS[10] and NetProwler a network -based IDS.[9]

- Okena offers StormWatch for critical server protection[12].

- Snort is advertised as "The Open Source network intrusion detection system and is available for download.[11]

5. Determine policy and procedures

There are further concerns that must be addressed despite what system is selected:

- What new skills will be required?

- Is 24/7 monitoring required or is scheduled review of data sufficient?

- What alerts will require immediate response and what alerts can be viewed and managed later?

- Will additional staffing be required or can the present staff absorb the tasking?

- Are there any legal or policy concerns that should be addressed before the IDS are implemented? IDS systems are capability of capturing and logging information such as user name, passwords, IRC sessions, even email. Local, State, and Federal laws should be reviewed for any impact.

- How will an intrusion be handled? Who needs to be notified within the company? Who is in charge of response and recovery? Does the local police have the ability to handle the case? Talking to the local or Federal authorities before an intrusion is a good idea. Knowing what type of evidence will be needed for a successful investigation and possible prosecution, before the stress of incidence response is helpful.

- Would a Managed Solution be better? A Managed Solution basally out sources network protection. A company will install, operate, and monitor the network following agreed procedures in the event of a detected attack.

The steps outlined here to select an IDS are far from being hard and fast but are meant to provide an outline. It isn't necessary that each step be done in the order given, or perhaps done at all. Each situation will have its own unique needs but in general the steps outlined here will in one way or another need to be addressed by any organization in the process of selecting an intrusion detection system.

List of References

1. FAQ: Network Intrusion Detection Systems
   http://www.robertgraham.com/pubs/network-intrusion-detection.html#2.1

2. Meinel, Carolyn. The ABCs of IDSs (Intrusion Detection Systems)
   http://www.messageq.com/security/meinel_2.html

3. Internet Systems Security. Network- vs. Host-based Intrusion Detection
   http://documents.iss.net/whitepapers/nvh_ids.pdf

4. Cisco Systems, Inc. Cisco Secure Intrusion Detection Systems Technical Overview
   http://cisco.com/warp/public/cc/pd/sqsw/sqidsz/tech/ntran_tc.htm

5. Norton, Peter, Stockman, Mike. Peter Norton's Network Security Fundamentals. SAMS, Indiana (pg 198)

6. Cisco Systems, Inc Cisco Secure Intrusion Detection
   http://cisco.com/warp/public/cc/pd/sqsw/sqidsz/

7. Internet Systems Security. Intrusion Detection
   http://www.iss.net/securing_e-business/security_products/intrusion_detection/

8. Symantec Corporation. Intruder Alert
   http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=48&PID=na

9. Symantec Corporation. NetProwler
   http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=50&PID=na

10. Okena, Inc.
    http://www.okena.com/index.html

11. Snort: The Open Source Network Intrusion Detection System
    http://snort.sourcefire.com/

12. Internet Systems Security. Evaluating an intrusion Detection Solution
    http://documents.iss.net/literature/RealSecure/ids_eval.pdf

Last Updated: June 24th, 2018

Upcoming SANS Training

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

SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced