Choosing an Intrusion Detection System that Best Suits your Organization

Dennis Mathew
GSEC Practical v1.4b
Option A

Table of Contents

Choosing an Intrusion Detection System that Best Suits your Organization

I. Abstract

There is a wide variety of Intrusion Detection Systems currently available, from network based IDS' to host based IDS', commercial and freeware. Its difficult to determine exactly what best fits your organization. To establish what you should be using, as with anything else, is a process. If this is your first attempt at securing your organization it may take more time and effort than for one that has made security a priority over the years. The technology, however, is only as effective as the people and processes that support it. Security is not simply a technology, but a mindset that must pervade the organization.

Choosing an intrusion detections system (IDS) can be a complex and time consuming project. This is especially true if the organization does not have a corporate security program. It is important to note that an IDS is in no way an all inclusive security solution, but if implemented correctly it can assist in detecting unauthorized activity and alert personnel to take action in the event of a security breach. In the following pages I will delve into exactly what an IDS is. This includes the various types of IDS' on the market and approaches taken to detect intruders. I will also identify key steps an organization should undertake prior to implementing an IDS solution. Performing a risk assessment of your organization and understanding existing controls and control deficiencies is a key step in securing the organization. Implementing a tool such as this is most effective when there is a grounded understanding of the organization as a whole and the critical processes within the company. Additionally, the organization should invest time and money into developing their personnel to ensure they are appropriately equipped to utilize the tool in a manner that will make full use of the systems functionality. Finally I will take a look at various commercial IDS' on the market today and the ever-evolving functionality of this technology. Although freeware tools are a very real and practical alternative I will limit the scope of this paper to the commercial market.

II. What is an IDS?

Primary Purpose

A security breach occurs when an individual gains unauthorized access to your systems. This unauthorized access can be further divided into two primary categories, intrusions and misuse. Intrusions occur when the security breach originates from outside the organization whereas misuse is an attack that originates from the inside, i.e. employees, intruders, etc. This unauthorized access can be for something as critical as stealing proprietary data or as trivial as utilizing your systems to play resource intensive role-playing games. Intrusion Detection Systems (IDS) is a security monitoring system that will gather and analyze data from various areas within a system or network to identify/detect possible intrusions and/or misuse. Intrusion Detection Systems perform a wide array of functions, which include:

- Monitoring and analyzing both user and system activities,
- Analyzing system configurations and vulnerabilities,
- Assessing system and file integrity,
- Ability to recognize patterns of typical attacks,
- Analysis of abnormal activity patterns, and
- Tracking user policy violations.

The system can be a key asset in pinpointing where attacks are coming from and when they are being made. It will also indicate the primary targets of the attack and the types of attacks being utilized. The IDS can be your eyes and ears into your system and/or network.

Network Intrusion Detection System

NIDS monitor the network wire and attempt to detect an attacker targeting company systems. An attacker may attempt to break into your system or may cause a denial of service attack. NIDS utilize raw network packets as its data source. A basic example of a monitoring technique is a system monitoring TCP connection requests (SYN) to a wide range of ports on a target machine to determine if someone is attempting a port scan. A NIDS can run on a host machine, monitoring all traffic to that machine or on an independent machine, promiscuously monitoring network traffic. The system can be configured to analyze traffic passing through a network segment to pinpoint patterns and trends that may be indicative of an attack. These systems provide near real-time event monitoring to a centralized console.

NIDS, in general, are less expensive than their host-based counterparts, but are very different in nature. The NID sensors generally will not monitor or identify activity at the host level.

Host-based Intrusion Detection System

Host-based IDS (HIDS) typically monitor event, and security logs at the operating system level. When any of these critical files change, the IDS compares the new log entry with attack signatures to see if there is a match. If there is a match, the system will respond with various types of administrator alerts to initiate incident response procedures. Some also monitor activity and issue alerts if specific ports are being accessesed. This technology continues to develop, but managing HIDS' have become simpler than the past. Agents can be installed on multiple hosts and monitored from a central console. HIDS can be critical in determining whether or not an attack was successful. The HID data can also be used should legal matters arise and the altering of data needs to verified.

Commercial IDS’ on the market

There are an array of Intrusion detection systems on the market as this space continues to grow. Free ware tools have been known to be very effective and if configured and managed properly are powerful tools. Since it would be difficult to discuss both free and commercial tools in the limited size of this project I will focus my attention on the commercial tools. Some of the leaders in this space are listed below:

Network Based IDS
Internet Security Systems Real Secure
Network Security Wizards Dragon IDS
Symantec Net Prowler
Cisco Systems Net Ranger
Network Flight Recorder Intrusion Detection Appliance
Network Ice Black Ice Defender
CyberSafe Centrax

Host Based IDS
Internet Security Systems Real Secure
Symantec Intruder Alert
Cyber Safe Centrax
Tripwire

Approaches to Intrusion Detection

There are multiple approaches taken to perform intrusion detection. The primary methods are rule-based intrusion detection (RBID) and statistical-based intrusion detection (SBID).

Statistical-Based Intrusion Detection (SBID)

SBID systems will attempt to identify security violations by systematically analyzing audit trail data. The system will compare log activity with typical or predicted attack profiles. This eliminates the need to manually sift through log files to try and identify unusual network traffic or system activity. The system automates this process and will perform this analysis in a structured manner. For this analysis to be effective there must be a preexisting classification of system or user activity that is considered to be normal. This characterization is usually called a profile. This profile is based on a series of events found in system audit data and can be used to configure expected behavior. User profiles can be customized to each user and are maintained dynamically. This allows the user’s profile to change as the user’s behavior changes. Administrators should be able to review these profiles to ensure that they make sense for their organization. This method of using profiles is not used by RBID’s. Statistically significant deviations above the predefined profile are considered intrusion attempts.

Rule-Based Intrusion Detection (RBID)

RBID systems are considered expert systems that will analyze extensive log files to differentiate between intrusive and normal day-to-day behavior. The system is centered on the assumption that it is possible to identify intrusion attempts based on a specific sequence of user activity that typically resembles activities that lead to system compromises. RBID expert system properties will initiate pre-defined rule sets when log data and system files indicate what appears to be

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.