Global Information Assurance Certification Paper

Simone L. Crider
GSEC, Version 1.4b

Intrusion Detection System (IDS) Solution: A Choice for Our Computer Center

Our computer center started by establishing a need for the internet based distribution of environmental (or geospatial) data. The center services provide information and data to the public via the internet, as well as providing a private network for internal users. The building of the center entailed the planning, research and implementation of computer hardware and network equipment. Services were deployed to the public within the first two years. The management of this center requires that we comply with Federal Government Information Technology (IT) standards and mandates. With system and network management being such an important function for the initially minimal staff, the need for some type of IDS within the center had become critical. The focus of this paper will be to demonstrate the process followed to choose an IDS for the needs of our computer center which include:

- **Defining Intrusion Detection System types**
- **Define the center's Intrusion Detection System needs**
- **Identification and Evaluation**
- **Selection and Implementation**

Defining Intrusion Detection System types

What is an Intrusion Detection System? As we have learned from numerous of sources, intrusion detection can mean various things to different individuals and different organizations. For our definition, we have adopted one that defines it in simple terms, "Intrusion Detection is the process of monitoring the events occurring in a computer system or network, [and] analyzing them for signs of security problems".[1]

There are different types of Intrusion Detection Systems (IDS), network based and host based. A network based IDS monitors the network traffic of an organization. This is done typically by setting the network interface in promiscuous mode which allows a network device to intercept and read each entire network packet upon arrival to the network.[2] Some of the main strengths of deploying a network based IDS are the lower cost to initially deploy and real-time detection. A host based IDS typically uses a system's auditing resources, such as event and system logs. It alerts administrators of changes to the system and possible problems. Strengths of a host based IDS include capabilities to detect attacks that network based solutions sometimes miss and greater flexibility for fine-tuning which activities should be monitored.[3] While both have their advantages, there are also disadvantages. Some disadvantages of a network based IDS are the generation of large amounts of data, a lack of compatibility for all network environments and the for need of a highly skilled staff to maintain and interpret the data.[4] Disadvantages to host based IDS systems include unreliability of system information if the host is attacked, failure to detect network scans, and the software must be run on each system.[5]

Define the center's Intrusion Detection System needs

Our center's network, servers and workstations are solely managed by the IT staff. The computer architecture for the center consists of an array of Linux and Windows 2000 servers and Windows 2000 Professional workstations. The management of all of these systems is a full-time responsibility for a very small staff, two people, therefore some type of IDS is considered a necessary tool for managing and protecting the systems from intruders. As part of the security requirements, the IT Staff must provide certain levels of system service and log monitoring and reporting capabilities. Key considerations for choosing an IDS were to select those that would be easily managed and monitored and include a report generation capability. Other important factors to be considered were ease of installation and configuration. The network configuration consists of a CISCO router and an application firewall, which was configured by a consulting firm. The daily management of the network is maintained by the system administration staff, however any major configurations are done on a consulting basis. Therefore, a network based IDS was considered to be too complicated to implement and maintain without a dedicated network administrator. While there are many advantages to deploying a network based IDS, a host based IDS seemed to better fit the center's present needs with many of its strengths. Those strengths include a stronger forensic analysis, a close focus on host-specific event data and lower entry-level costs.[6] It is the responsibility of the IT system administration staff to define the requirements of the IDS, identify, evaluate and implement the products that fit the criteria and recommend these solutions to the manager.

Identification and Evaluation

After determining the type of IDS to deploy, the system administration staff started the task of finding the right IDS software for the two pertinent operating systems (OS):

- Windows 2000 (Server and Professional)
- RedHat Linux (7.1, 7.2 and 7.3)

Each system administrator was responsible for identifying an IDS product for each particular OS. Each system administrator took the following steps:

1) Reviewed information from our parent organization for IDS software that is in use by other agencies within the organization.
2) Researched internet sources for OS specific IDS software.
3) Read and reviewed software information and documentation.
4) Downloaded and installed evaluation software.
5) Evaluated each candidate for several days.

For the Windows 2000 (Professional and Server) OS, six software packages were initially evaluated and five of those were installed and evaluated further. These

products are listed below along with a description and detailed information of each as well as the reasons why they were or were not selected. See Table 1, Windows IDS System Comparison, for a comparison of the installed software packages.

	Prism Micro-Systems	*GFI LANguard S.E.L.M*	*ELM Log Manager*	*Adiscon Event-Reporter*	*LogCaster*
Documentation	Poor	Good	Fair	Poor	Excellent
Ease of Installation	Very easy	Very easy	Very easy	Hard	Very easy
Ease of Configuration	Easy	Easy	Fair	2	Very easy
Stability	Good	Excellent	1		Excellent
Centralized Management, Monitoring and Logging	Good	Good			Excellent
Notification Capabilities	Good	Excellent			Excellent
Reporting	Good	Excellent			Excellent
Customer Support	Un-responsive	unknown			Excellent

Table 1: Windows IDS System Comparison

1: Software kept crashing on Client systems – so evaluation was terminated
2: Configuration was difficult and documentation was not adequate for our uses, therefore evaluation was terminated.

Big Brother – According to the vendor, this product monitors availability of system and network-delivered services. It is currently available in two versions, *Big Brother* and *Big Brother Professional*. *Big Brother* is available for a free download and is backed up by Quest Software's "Better Than Free" license, which basically means that it is offered "as-is", without warranty and without the intent of commercial gain. *Big Brother Professional Edition* is an enhanced version of *Big Brother* that is available for purchase and adds additional functionality that includes simplified installation, integration of additional products, complied versions for certain OS's, NT paging capability and telephone support.[7] This particular software was identified as being used by other agencies within our organization, and therefore was one of the first products to be evaluated. The product is compatible with both target OS's and this at the first appeared to be a plus. The system administration staff downloaded the software package and proceeded with review of the documentation and initial setup. After reading the documentation, it was determined that it would take a large amount of time to initially install and configure. It was concluded that this product would be too complex to configure on the Windows OS and therefore was not installed and evaluated further.

Prism Micro-Systems – The vendor states that this is an Event Management component for Windows that centrally consolidates & analyses log information from multiple platforms.[8] The product description appealed to the administration staff as it appeared to be a very capable tool. It was available for download with a 14-day trial license for the Windows OS. It was downloaded and installed with limitations of product functionality. The documentation was somewhat limited, but the product was easily installed and configured. The administration staff liked the notification tool functionality which included 90 days support with the purchase, and overall liked the product very much. The next step was to get a price quote for the product, so the administration staff tried to contact the vendor. After two phones calls to their sales department, each time leaving a voice message requesting purchase assistance, no response was received from this vendor. It was feared that lack of response from their sales department, would be indicative the type of service we could expect of their support department, as well. Without further information, the staff was forced to select another product.

GFI LANguard S.E.L.M – The vendor claims that this product monitors the security event logs of all Windows NT/2000/XP servers and workstations and alerts staff to possible intrusions/attacks in real time. It collects all events in one central database, and it is easy to create network-wide reports and custom filters.[9] This product was downloaded as a free evaluation copy for 60 days, and included good documentation. During the installation process, it was found that the actual configuration was very complex and the administration staff was unable to get this tool fully functional with in our LAN configuration.

ELM Log Manager – According to the vendor, this software gives system and security administrators the power to see all event log entries with unrivaled clarity by combining the core functions into a feature-packed, reliable, and scalable application. This tool automates a variety of the administrative functions required for monitoring and managing event logs, log files, SNMP traps and Syslog messages generated by Windows-based servers and workstations and TCP/IP systems and devices. It has a multi-layered architecture that enables you to deploy in a manner that fits your organizational needs.[10] The 30 day evaluation version of this product was downloaded and installed. The product included a client agent of which the staff installed and ran on a select number of client workstations. It was easy to install and configure. However, the client agent would crash on the workstations for no apparent reason and would notify the manager agent, as well as the user on each workstation, that the client agent had terminated. No documentation or resolution of this problem could be found, therefore this product was not selected.

Adiscon EventReporter – The vendor states that this product provides centralized monitoring and reporting of Windows NT and 2000 Event Log records. The messages are reported by either standard UNIX syslog protocol or standard Internet email. Some of it's key features include centralized logging, ease of use, syslog and

email support, local filtering and full Windows 2000 support.[11] The evaluation copy was downloaded and it included adequate documentation for installing and configuring this product. During the installation and configuration process, it became apparent to the administration staff that the product was not user friendly and overall functionality of this product was not what the center required for its IDS solution.

LogCaster – The vendor defines this product as the most results-oriented solution for Windows NT and Windows 2000 systems management. It was designed to deliver immediate results and is easy to implement, manage and use. Through the management console, distributed server management becomes simple. Its consolidated data management provides easy access to the information you need, when you need it. It uses a standard ODBC interface and is equipped with predefined reports for your most critical and crucial measurements. Customized reports can be created quickly and easily with the wizard-driven reporting tool.[12] The administration staff downloaded an evaluation copy which included the limitation of use for only ten clients. The product performed as the others did, in a master/client configuration and included documentation that the administration staff referred to as "wonderful". It was easily installed using a "quick start" installation to get the software running initially, and included more detailed documentation for further customizing this product, which we would use to meet the needs of our center. The administration staff also contacted their customer services group for purchase information and found them to be extremely helpful and attentive. The purchase of this product includes one year of customer support. Our system administration staff found this product to have an excellent reporting tool and that it helped to maximize the Windows event reporting. This product was highly recommended to the IT Manager for purchase.

For the RedHat Linux OS, the following software was installed and evaluated. They are listed below along with a description and specifics of each, as well as the reasons why they were or were not selected. See Table 2, Linux IDS System Comparison, for a comparison of the installed software packages.

Tripwire – The product documentation states that this product is a tool for file integrity assessment. It works by first scanning a computer and creating a database of system files, a "snapshot" of the system in an initial or presumed secure state. It can be configured very precisely, specifying individual files and directories on each machine to monitor, or a standard template can be created for use on all machines in an enterprise. By scanning the current system and comparing that information with the data stored in the database, this software detects and reports and additions, deletions, or changes to the system outside the boundaries of normal systems usage. If the changes are valid, the administrator can update the baseline database with the new information. If malicious changes are found, the administrator will instantly know what components have been affected.[13] This product is included as part of the base RedHat OS installation. It must be configured and activated for usage on each system. The administration staff downloaded the latest version of the binary RedHat Program Manager (RPM) and upgraded the base installation.

Using the *Tripwire* documentation[13] and several RedHat specific "how-to" documents[14 & 15], they were able to successfully implement and run *Tripwire* as a log monitor and reporting tool.

	Tripwire	*Nagios*	*Swatch*	*SNARE*	*Big Brother*
Documentation	Poor	Too Complex	Poor	Excellent	Fair
Ease of Installation	Easy	Easy	Too Complex (1)	Easy	Fair
Ease of Configuration	Easy	Too Complex (2)		Easy	Too Complex
Stability	Good			Good	Good
Centralized Management, Monitoring and Logging	Good			Poor	None
Notification Capabilities	Email			None (3)	None
Reporting	Good			None (3)	None
Customer Support	None			Developers support product	On-line list

Table 2: LINUX IDS System Comparison

1: Installation was determined to be too complex therefore evaluation was terminated.
2: Configuration was determined to be too complex therefore evaluation was terminated.
3: Feature is expected in future releases.

Nagios – According to the documentation, this product is a system and network monitoring application. It watches the hosts and services that you specify, alerting you when things go bad and when they get better. This product was originally designed to run under Linux, although it should run on most other Unix operating systems as well. The only requirement for running this product, on a Linux system, is a compiler. Included with this product are CGIs, which require using a webserver and gd library version 1.6.3 or higher.[16] The administration staff downloaded the software and found the build and installation to be easily done, with ample documentation for a "quick and dirty" install. However, there were no "quick" or "easy" instructions for the configuration process. The staff found the configuration process to be nested and very complex. After thoroughly reading the documentation

and example configuration files, the administrator was unable to get Nagios to successfully run. The decision to seek another product was made.

Swatch – The product documentation defines this product as an active log file monitoring tool. This tool started out as a "simple watchdog" for actively monitoring log files produced by UNIX's syslog facility. It has since evolved into a utility that can monitor just about any type of log.[17] It was also identified as a software product that is used by other agencies within our organization. After an extensive internet search, the administration staff was able to locate the current host site for this product. The previous site is referenced by numerous other internet sites, that instantly redirects to the current site at http://swatch.sourceforge.net/. The administration staff found this site uninformative about the product and offered no information about available documentation. There was only a link to the latest version, swatch-3.0.4. This version was downloaded and an installation attempt was made. The documentation was consisted of README and INSTALL files. The installation process appeared to be straightforward, however, errors were encountered because we lacked the perl CPAN modules necessary for installation, as they were not available on the target platform. An attempt to find the CPAN modules was made, however all of the required modules could not be obtained. Therefore, the result was in an incomplete installation and no further evaluation.

System iNtrusion Analysis & Reporting Environment (SNARE) – According to the product documentation, this product was designed to “enhance the security of the Linux operating system by providing a comprehensive event logging facility”. It is a host based IDS that offers three main components: a dynamic kernel audit module, an audit daemon, and a front-end GUI. The kernel audit module wraps critical system calls such as mkdir, open, and execve and gathers information about the process and the user that executed the call. The user-space audit daemon reads the event data from the temporary buffer via the /proc/audit device and converts it from binary format to a delimited text format. It also offers a GUI to display these events in a colorful, easy-to-read window and it additionally provides configuration screens to define which events should be logged.[18] The administration staff downloaded the binary RPM files for installation, and installed the product without any problems. A base configuration was installed and used via its GUI interface. However, problems were encountered due to a conflict with the latest versions of the system kernels. With assistance from the InterSect SNARE developers who provided a pre-released workaround, the product was successfully installed and is operating on the targeted systems. Overall, the product provides a very nice GUI front-end and the capability of remote logging from other workstations to the master server (i.e. log server) /var/log/audit directory. However, the present version lacks email notification and the ability to monitor remote workstations within the GUI interface. It also lacks a report generation capability. Even though this product, in present form, does not offer all the features that are desired of an IDS tool, it can be used as a simple system’s monitoring tool. It is definitely a product that will be watched for future releases.

Big Brother – As stated previously, this product monitors availability of system and network-delivered services. It is currently available in two versions, *Big Brother* and *Big Brother Professional Edition*.[7] This product is being used by other agencies with our organization as a monitoring tool. The administration staff downloaded the *Big Brother* version of this product for installation. The documentation was found to be ample for the Linux platform, but not easily followed. After attempting the software installation several times, the product was installed and ready to be configured for running on the server. The staff used a base configuration that took some tweaking. Once the master server was configured and running, the client version of the software was installed on several remote systems. It was determined that this tool is adequate for monitoring the services that are running on each server, but lacked in the ability to provide log monitoring or a reporting capability.

Selection and Implementation

At the completion of the initial identification and evaluation phase, the administration staff made their recommendations and gave an overview of the implementation of the selected products.

For the Windows 2000 (Professional and Server) OS, the system administration staff recommended the purchase of Ripple Tech's *LogCaster.* The overall performance and capability of this product convinced the staff that it would serve our center's needs for the Windows suite of servers and workstations. In addition to this basic capability, excellent technical support is provided with the purchase of this product. The installation procedure for *LogCaster* began with the following process.

Prior to deploying *LogCaster* Agents to each server/workstation to be monitored, validity tests were performed to ensure proper administrator privileges and to verify remote registry access. The appropriate tests are defined in the *LogCaster* documentation.

In considering where to install the *LogCaster*'s Event Dispatcher Server (EDS) component and where the database would reside, it was determined that a dedicated server was not required and that a Windows 2000 Professional workstation would be sufficient as it exceeded the minimum recommended system and disk space requirements. An administration staff workstation was chosen to be the EDS for convenience in accessibility and monitoring.

The software comes with an InterBase database or can be configured to store data using Microsoft SQL Server, which must be purchased separately. The administration staff determined that the InterBase database was sufficient to meet our current needs. If the organization grows to the point where a more robust database is needed, the upgrade will be made at that time.

Installation of software was performed in two stages. The first stage was to install the basic setup of the EDS on the Windows 2000 Professional workstation using the

quick start documentation as a guide. The instructions were straightforward and no installation problems were encountered. The second stage involved deploying the *LogCaster* Agents to every computer to be monitored. From within the *LogCaster* server program it was a simple procedure to browse through and select the target computers.

After monitoring the basic setup for approximately one week to ensure stability, configuration modifications relative to the needs of our organization were implemented. The fine-tuning of this powerful tool is on-going and under constant review.

For the RedHat Linux (7.1, 7.2 and 7.3) OS, the system administration staff recommends the use of multiple open source products. Until there is a more fully developed Linux product that meets the entire IDS needs of our center, the system administration staff will use *Big Brother* as it's service monitoring tool and *Tripwire* for log monitoring and reporting. Both have an email and paging notification capability for alerting the system administration staff to system and service issues. The configuration and installation process for both products is as follows.

The installation of *Big Brother* entailed using the "really quick and dirty" install procedure. This installation procedure was fairly straightforward with the exception of the URL setup within the initial configuration. It is recommended that a new user (bbuser) be setup to actually run the installed software. For security purposes the initial software configuration and installation processes require root privileges, but the software setup and configuration can be done as the user bbuser.

The *Big Brother* installation process began by running the configuration script, bbconfig. Within the configuration process, defining the URL locations were found to be very confusing to the administration staff. It took the configuration of a web server, Apache, to figure out where to define *Big Brother*'s URL locations. Finally on the third configuration attempt, this problem was resolved. Once the configuration was complete, the installation required a "make" and "make install" to compile and install the monitoring software into the *Big Brother* root directory, /home/bbuser.

Once *Big Brother* was installed, the administration staff then configured the software prior to starting it. The software configuration process entailed customizing the bb-hosts (host table) and bbdef.sh (alarm level script) files. Once those files were modified, a couple of confirmation scripts, bbckkcfg.sh and bbchkhosts.sh, were run to confirm the accuracy of the scripts and defined hosts.

The final step in the installation of *Big Brother* entailed changing file permissions and ownership of key files and directories that were installed as root to bbuser. The administration staff also added a symbolic link within the /home/bbuser directory to the web server "Document Root" directory.

The *Big Brother* software was started by bbuser executing the main script, "runbb.sh start". This script starts all the necessary processes for monitoring the configured services on both master and client servers via a web browser. In order to monitor CPU, disk, log files and processes on client servers of the same OS, the *Big Brother* client installation script must be run on the master server. The administration staff ran, bbclient, within the master server's installation directory. This script generates a tarball for the client within the same directory structure as the master server. This tarball can be extracted onto the client servers. The same initial procedure is followed for starting *Big Brother* on the client. Once all clients are started, they can be viewed as part of the master web services.

The installation of *Tripwire* began with the installation of the latest RedHat binary RPM. At the completion of that installation, it is recommended that the /etc/tripwire/twinstall.sh be run to setup the initial configuration. This script creates the encrypted policy and configuration files that are stored in /etc/tripwire. Prior to initially running the twinstall.sh script, the system administration staff made an initial modification to the /etc/tripwire/twpol.txt file to customize the policy file for email notifications. This is not activated by default.

The system administration staff then initialized the *Tripwire* database with the following command, "tripwire –m i". Once the initial database was created, the staff then attempted to customized *Tripwire* to eliminate a large number of false alarms. This was accomplished by running the following command, "tripwire –m c | grep Filename >> false.out", thus generating a listing of files that are not necessary to monitor in a local system. The twpol.txt file was again modified, commenting out the files identified within the false.out. Anytime the policy file is edited the policy must be reinstalled and the database recreated. To reinstall the policy, the following command was used, "twadmin –m P /etc/tripwire/twpol.txt". To recreated the database the following was used, "tripwire –m i".

Finally, the system administration staff created a daily cron script to check the system integrity on a daily basis. The script "runtw.sh" was created within the /etc/cron.daily directory and contained the following command, "/usr/sbin/tripwire –m c | mail –s "Tripwire Daily Report from Master Log Server" root@localhost".

Conclusion

Now that our center's IDS needs have been defined and a solution has been implemented, the system administration staff will continue to fine-tune the current deployment as well as evaluate it to ensure that it continues to address the center's needs. The staff realizes that the IDS products are only effective if they are well maintained and kept current with the changing needs of the center. The staff will continue to keep abreast of the evolving security risks and IDS product market and be prepared to make changes as required by the center's security policy.

References

[1] Bace, Rebecca Gurley, Intrusion Detection, Indianapolis, MacMillian Technical Publishing, USA, 2000, page 3.
[2] Search Security.com Definitions, URL:http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci518283,00.html, (March 11, 2003)
[3] Andress, Mandy, "Free dependable IDS", InfoWorld, January 24, 2002. URL:http://www.infoworld.com/article/02/01/24/020128tcsnare_1.html, (January 21, 2003)
[4] Matt Joyce, "Introduction to Network Intrusion and Misuse Detection", June 4, 1999, URL:http://www.iacptechnology.org/PowerPoint/LEIM%20Presentations/Network%20Intrusion%20and%20Misuse%20Detection/Network%20Intrusion%20and%20Misuse%20Detection.pdf, (March 4, 2003)
[5] Goeldenitz, Thomas, "IDS – Today and Tomorrow", January 22, 2002, URL:http://www.sans.org/rr/intrusion/today.php, (March 4, 2003)
[6] Internet Security Systems, "Network- vs. Host-based Intrusion Detection, A Guide to Intrusion Detection Technology", URL:http://documents.iss.net/whitepapers/nvh_ids.pdf, (January 30, 2003)
[7] Quest Software, "Big Brother", URL:http://bb4.com/index.html, (March 5, 2003)
[8] Prism Micro-Systems, "EventTracker for Windows", Version 3.0, July 2002, URL:http://www.prismmicrosys.com/eventtracker/doc/ETW30WP.pdf, (March 5, 2003)
[9] GFI, "GFI LANguard S.E.L.M", URL:http://www.gfi.com/lanselm/, (March 14, 2003)
[10] TNT Software, "ELM Log Manager™ 3.0", URL:http://www.tntsoftware.com/products/ELM3/ELM30/, (March 5, 2003)
[11] Adiscon IT-Solutions, "The EventReport User Manual", October 11, 2002, URL: http://www.eventreporter.com/en/Manual/manual.htm, (March 5, 2003)
[12] RippleTech, Inc., "Ripple Tech's LogCaster", URL:http://www.rippletech.com/pdf/logcaster_brochure.pdf, (March 5, 2003)
[13] Tripwire, Inc., "Tripwire Documentation", URL:http://download.sourceforge.net/tripwire/tripwire-2.3.0-docs-pdf.tar.gz, (March 5, 2003)
[14] RedHat Linux, "Installing and Configuring Tripwire", URL: http://www.redhat.com/docs/manuals/linux/RHL-7.3-Manual/ref-guide/ch-tripwire.html, (March 5, 2003)
[15] Lynch, F. William, "Getting Started with Tripwire (Open Source Linux Edition)", March 21, 2001,URL:http://www.linuxsecurity.com/feature_stories/tripwire-2.html, (March 5, 2003)
[16] Galstad, Ethan, "Nagios® Version 1.0 Documentation", August 28, 2002, URL: http://nagios.sourceforge.net/docs/1_0/, (March 14, 2003)
[17] Hansen and Atkins, "Centralized System Monitoring With Swatch", URL:http://www.oit.ucsb.edu/~eta/swatch/lisa93.html, (March 5, 2003)
[18] Intersect Alliance, "SNARE System iNtrusion Analysis & Reporting Environment", URL:http://www.intersectalliance.com/projects/Snare/Documentation/index.html, (March 5, 2003)