Global Information Assurance Certification Paper

Name: Lynn Bogovich
Version: 1.2f GSEC Practical Assignment
Title: Host-Based Intrusion Systems for Solaris

Abstract

Locating a Host-based Intrusion Detection System (HIDS) that will run on only Sun SPARC Solaris Unix machines is almost an impossibility. Most Intrusion Detection Systems (IDS) include PC or Intel-based computers as part of the required hardware for commercial IDS software. Narrowing the field of all available IDS packages to those that support Sun SPARC Solaris Unix machines was not an easy task. IDS requirements are presented, with an analysis of currently available IDS software packages and a recommendation of the best HIDS package to manage a suite of Solaris machines.

Background

As Senior Unix System Administrator, I was given the task of installing an Intrusion Detection System (IDS) on sensitive Unix servers. Our organization is a conglomeration of many different operating systems: Sun SPARC Solaris, Windows 2000, MacOS, a few Linux machines, IRIX, VMS, and Compaq Tru64. The computers are located in a switched environment. The portion of the network for which I am responsible is composed of Solaris/Tru64 machines.

Prior to attending SANS Security Essentials, our management had purchased Internet Security Systems (ISS) RealSecure software, but we really didn't find out everything we needed to know about the software and hardware prior to the actual purchase. During the SANS Security Essentials track, ISS RealSecure was presented as a very good Unix IDS. But to my surprise, the course material mentioned using a PC.

After the SANS Security Essentials class, I followed up by reading the RealSecure Manuals supplied with the installation CD. The RealSecure manuals spend a lot of time describing PC hardware and installations of the different components of the Management Console on PCs, but nary a word about Solaris machines. Solaris was mentioned in the Network and Server Sensor installs and hardware requirements only. [8] Follow-up discussions with our sales representative and a RealSecure Software Engineer confirmed the fact that, yes indeed, the Management Console only runs on PCs.

Did we purchase the wrong software? We were looking for a Sun SPARC Solaris Host-based Intrusion Detection System (HIDS). Since our division of the company does not use PCs, a decision to use RealSecure was an important architectural and financial decision. Using material learned in the SANS Security Essentials class, we put together a "Business Case for Intrusion Detection…to convey the 'Big Picture' " [14] for presentation to our Division Manager so that we could petition our parent company for more monies for 1-3 PCs, depending upon the distributed configuration we would plan on using, if any. To help our management justify this business decision, I was tasked with identifying our requirements, evaluating available HIDS packages based on those requirements, and recommending a solution.

To evaluate the HIDS software, I used portions of Six Sigma methodology to identify key requirements and rank HIDS software solutions based on those requirements. The body of this paper is the presentation of those requirements and subsequent analysis to determine the best HIDS software for our organization.

Requirements for Solaris HIDS Software

The objective of the work assignment is to "lockdown" the Solaris systems by installing HIDS on specific servers in the de-militarized zone (DMZ). Since the Network Manager is dealing with the Network Intrusion Detection System (NIDS), I will not be covering this item in any detail. However, to sufficiently analyze the candidate software solutions, it was necessary to include NIDS in the definition of the key requirements.

IDS (HIDS/NIDS) – Our security policy requires us to put mechanisms in place "to provide real-time detection of patterns…that may indicate anomalous or malicious activity, and respond to this activity through automated countermeasures. In addition, these mechanisms should also support the pursuit of individuals responsible for malicious activity through the collection and correlation of event data. [9]" At the present time, we do not know if the evidence we collect in tracking a perpetrator will stand up in court, but we will continue to collect the data.

Currently, aside from TCP Wrappers (with hosts.allow/deny), md5sum (on a few select, critical servers) and Perl/Shell scripts trying to watch the logs of over 350 Solaris machines (which take awhile to generate and test), our company does not have any HIDS software package to regularly look for possible malicious user activities (e.g. password cracking, NFS file sharing exploits) and intruder alerts (e.g. replaced binaries, new SUID/GUID executables, unknown devices, port activity on selected ports). In addition to HIDS alerts by either email or (in the extreme case) beeper, we would like them to "respond automatically to the event…[e.g.] logging off the user, disabling a user account and launching some scripts. [3]"

Therefore, our primary requirement is software that detects intrusions from users via the console, looking for attack signatures and monitoring system activity. [12] According to ISS, "host-based scanners are excellent tools for evaluating security risks associated with all types of user risks. These include risks caused by ignorant users, malicious users, and all users in between. [4]"

Although we would prefer a HIDS with true real-time capability, responses will not be 'real-time' but after-the-fact. HIDS monitor system logs, which capture actions that have already occurred. If an anomaly shows up in the system log, the system has already been attacked. In contrast, NIDS work in real-time, watching data packets as they transverse the network. So by working in conjunction with NIDS, HIDS can catch intrusions that are not captured by NIDS (e.g. attacks from the console itself, switch environments, and certain types of encryption). [5] [6]
Since the protection of the network is not our primary objective, NIDS capability would be a plus for future expansion of our defense perimeter, but is not a key requirement.

Another consideration of the HIDS should be whether the package is tunable enough to reduce

the guaranteed "false positives" that will be produced once the HIDS becomes activated. Our environment is too critical for administrators to simply "tune out" needless chatter from packages because there is no feature or controls to "minimize the number of false alarms. [11]" HIDS would be acting as a silent partner with the system administrators to spot intrusions and malicious activity so that computer forensics can begin.

Operating Systems – The HIDS must run on all versions of the operating system above Solaris 2.6. Solaris is of particular concern, because "in the old days, Trusted Solaris had a reputation of being difficult to manage. [2]" Articles like the referenced one by Galvin indicates that Trusted Solaris 8 is easier to manage than previous incarnations, but given Solaris' track record, it is especially important that we protect this operating system with an HIDS. "The Solaris Security Toolkit is not a traditional Sun[tm] product, and as such, is not supported by Sun Microsystems. [15]"

Hardware – The HIDS must run on Sun SPARC workstations. It would be ideal if no other hardware platforms were required, as this would reduce our cost for purchasing and maintaining the hardware. However PCs are too prevalent in candidate solutions to totally ignore.

Console – The console is responsible for collecting the information from the servers and depositing the data in a central location [13]. The following requirements will be used to evaluate the implementation of the console in the candidate IDS packages.

- Central Monitor Collection Point – A standard design of console applications is for one machine to be responsible for collecting and analyzing data. This design is sufficient to meet the needs of our organization. On the downside: "…in a highly distributed and high-volume event environment, a single repository combined with a single analysis engine can act as a choke-point. It also provides a single point of failure should the repository become unavailable or tainted. [9]"

- Distributed Monitor – A distributed monitor solution spreads out across a few machines to prevent bottlenecks and avoid high-intensive CPU number crunching. By being distributed, the upgrading of the different components will be easier and not affect the other components as much. This feature is desirable, but not necessary.

- Real-time Visual Notification – Reports and visual graphics from the console will help in analysis and real-time intrusion detection. One consideration is whether the visuals require yet another software package to work. It is desirable to minimize the number of software packages that must be implemented and maintained.

Integrates with other third-party IDS suites – It would be desirable to be able to export data between central collection databases for generating reports, spreadsheets and the like. Therefore, the package software should be able to integrate between other third-party software packages leading to a "centralized logging and reporting capability. [1]"

Ease of Installation – The preference is to minimize the learning curve. The ideal product could be installed out of the box with a small number of modifications. It is understood that rules will need to be generated for the sensor operation to work properly.

Upgrades – The software must be able to be upgraded without a complete re-installation with every new version. De-installs/Installs of some portions are acceptable.

Customer Support – The support should be local; i.e. here in the USA. This requirement is important as our company deals with critical real-time data that must be available at all times. The ASAX software is supported out of Belgium, which makes this package less desirable.

Proven Technology – To minimize risk to our organization, the technology must be stable. For example, the Emerald package appears to be in the early research stages. [10]

Real-Time Rule Generation – Some packages are based on expert systems, generating rules about new intrusions that may not have been initially identified. "The fields of the resource object [operating parameters] are defined and utilized during monitor initialization. In addition, these fields may be modified by internal monitor components, and by authorized external clients using the monitor's API [application programmers' interface]. Once fields are modified, components can be requested to dynamically reload the configuration parameters defined in those fields. [9]" This feature is interesting, but not a key requirement.

Supports Concept of Least Privileges – This concept is one of role-based access, where a user only has privileges to do those actions that are required for their job. In our organization, operators should be able to monitor the console for real-time intrusions, but they should be prohibited from generating reports (e.g. database access).

Analysis of Candidate Packages

To analyze potential IDS packages, a Quality Function Deployment (QFD) tool was used. This tool can be used to assure that a solution, in this case the HIDS, meets a customer's needs.

In the QFD table below, the requirements are listed down the left hand column. Priority ratings of 1 to 5 were assigned, with 5 being the highest, desired attribute. Across the top of the table are listed the products that were researched and that basically fit the requirements. In order for the true values of the product to stand out as to which was the most desirable to use, a rating scale of: 9 – highly qualifies, 3 – mostly qualifies, and 1 – slightly qualifies was chosen. A rating of zero (0) means that the product does not have this feature or I was unable to determine if the feature existed.

Solaris HIDS Evaluation Matrix

		Products									
Requirements	***Priority***	RealSecure	Snort	Tripwire	Solaris Security TK	Kane Secure Enterprise	SunScreen Lite	Emerald	ASAX	Trusted Solaris 8	Swatch
HIDS	5	9	0	3	0	3	9	9	9	9	9
NIDS	1	9	9	0	0	9	0	9	0	1	0
Solaris 8 Support	5	9	9	9	9	0	9	9	0	9	9
Solaris 7 Support	1	9	9	9	9	0	0	9	0	0	9
Solaris 2.6 Support	1	9	9	9	9	9	0	9	1	0	9
Hardware - No PC Required	5	0	9	9	9	0	9	9	9	9	9
Central Monitor Collection Point	5	9	9	0	0	9	3	9	9	9	0
Distributed Monitor	2	9	0	0	0	9	3	3	9	9	0
Real Time IDS	5	9	9	9	0	9	9	9	0	3	3
Real Time Visual Notification-self	3	9	0	9	0	9	0	9	0	3	0
Real Time Visual - no other pkg	4	9	0	9	0	9	9	9	0	9	9
Integrates with third-party IDS	5	9	0	9	0	9	0	9	0	0	0
Ease of Installation	5	9	9	9	9	9	9	0	0	9	9
Upgrades	3	3	3	0	9	0	9	0	0	0	0
Customer Support Local to USA	5	9	9	9	9	3	9	9	0	9	9
Proven Technology	5	9	9	9	9	9	3	0	0	9	9
Real Time Rules Gens	1	3	0	0	0	0	0	9	0	0	9
Support Concept of Least Priv	5	9	0	0	0	0	0	0	0	9	0
Final Score		471	342	396	270	330	324	366	109	393	303

Detailed Analysis

As shown in the final scores above, RealSecure, Tripwire, and Trusted Solaris 8, were the packages that best meet the requirements. In order to make the best decision, I decided to analyze the key differentiators among the three packages.

RealSecure – In looking at the requirements that are rated at a priority of 5, RealSecure had a rating of 9 on all of them, except the 'No PC Required'. Upgrades are average, with deinstalls coupled with new installs. With respect to the low priorities, NIDS is rated high. This is good for future expansion of incorporating Network Analysis into the Monitor for centralization of monitor data.

Tripwire – With respect to the high priority requirements, Tripwire falls short on 'HIDS', 'Central Monitor Collection Point', and 'Support Concept of Least Priv'. This tool is highly respected for its monitoring of server data compared to a baseline configuration. (17) Unfortunately, looking for intruders in logs, suspicious port activity, console attacks and password cracking are not monitored. Current Perl/shell scripts and sudo would continue to be needed in order to monitor the system logs and allow operators to do jobs like backups and creating accounts.

Trusted Solaris 8 – Since this tool only records events that it is configured to monitor, based upon the rules generated at installation time or dynamic modification of the database configuration rules by the security administrator, security breach attempts will pass by undetected. "Trusted Solaris auditing collects user actions and non-attributable (in the class na, non-attribute) events into audit classes." (16) The table provided in the 'Sun Doc' contained thirty-three (33) classes, followed by 33 tables defining the various events for each one of these classes. The learning curve for this setup is beyond the range of time we need to implement a solution.

Chosen Solution

RealSecure seems to be the best choice of the three for the following reasons. The package is a hybrid of HIDS/NIDS. The Network Sensor Capability using NIDS is already a part of the package, so in the future it will be easy to activate this functionality and incorporate network data into the Central Monitoring Console.

The OS Sensor Capability using HIDS will be monitoring the logs and port activity to see if an intruder has actually gained access to the host or identify unauthorized activity on the system based upon our security policies.

The Server Sensor Capability hybrid combines the OS Sensor functionality along with the Network Sensor functionality. The Server Sensor will monitor and block suspicious traffic by intercepting packets before they reach the Operating System. In this manner, the Server Sensor will monitor and control all the inbound and outbound communications traffic. Third party packages will also be able to be integrated with the Central Monitoring Capabilities in order to add more pointed diagnostics to the overall IDS. (7)

For the best coverage of our Intranet, I am proposing that we implement all portions of the RealSecure software package. Its features give us: the detailed tracking we need for the pursuit and prosecution of intruders; the means to formulate triggers for rapid responses to unauthorized intrusion and malicious activity; and the early detection of intruders as they transverse across the network, prior to reaching our critical servers within and behind our DMZ.

Summary

It was a challenge to try and locate a good IDS for Solaris that would run solely on Sun SPARCs and have all the capabilities that were required for our organization. RealSecure meets so many of the other requirements that we are now convinced that it is the right package for the job, even if it does require the use of PCs. Using the research presented in this paper, our Division Manager has sufficient data to convince our parent company that we need additional hardware for this Intrusion Detection Plan to succeed. In the meantime, I will be continuing to monitor the Internet for new developments in IDS, looking forward to the next generation of IDS that is completely Sun SPARC Solaris Unix based.

References

[1] Check Point Software Technologist, Ltd., *Check Point FireWall-1 Technical Overview*, November 2001, http://cgi.us.checkpoint.com/rl/resourcelib.asp?state=1&item=FW1Tech

[2] Galvin, Peter Baer, *Can You Trust Trusted Solaris 8*, Sys Admin, the journal for UNIX system administrators, December 2001, http://www.samag.com/documents/s=1769/sam0112i/0112i.htm

[3] Innella, Paul and Oba McMillan, *An Introduction to Intrusion Detection Systems*, 6 December, 2001, http://www.securityfocus.com/infocus/1520

[4] Internet Security Systems, *Network and Host-based Vulnerability Assessment*, http://documents.iss.net/whitepapers/nva.pdf

[5] Internet Security Systems, *Network versus Host-Based Intrusion, A Guide to Intrusion Detection Technology*, October 22, 1998, http://documents.iss.net/whitepapers/nvh_ids.pdf

[6] Internet Security Systems, *RealSecure 6.0 Frequently Asked Questions*, 14 June 2001, http://documents.iss.net/literature/RealSecure/rs60_faq.pdf

[7] Internet Security Systems, *RealSecure Getting Started Guide Version 5.5.2*, May 2001

[8] Internet Security Systems, *RealSecure System Requirements*, 24 October 2001, http://documents.iss.net/literature/RealSecure/rs_sysreqs.pdf

[9] Neumann, Peter G. and Phillip A. Porras *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances*, 9 October 1997, http://www.csl.sri.com/intrusion.html

[10] Neumann, Peter G. and Phillip A. Porras, *Experience with Emerald to Date*, 1st USENIX Workshop on Intrusion Detection and Network Monitoring, Usenix Assoc., 1999, http://www.csl.sri.com/users/neumann/det99.html

[11] Raikow, David, *IDS Bolster Network Defense, IDS downsides*, ZNET, October 22, 2001, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2819361-3,00.html

[12] Raikow, David, *IDS Bolster Network Defense, Know your options: HIDS & NIDS*, ZNET, October 22, 2001, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2819361-2,00.html

[13] Rebecca Bace and Peter Mell, *Intrusion Detection System*, 16 August 2001, http://cryptome.org/sp800-31.htm

[14] SANS Institute, *SANS Security Essentials I: Information Security, The Big Picture*, 10 August, 2001, http://www.sans.org

[15] Sun Microsystems, Inc., *Solaris Security Toolkit (JASS)*, December 2001. http://www.sun.com/security/jass

[16] Sun Microsystems, Inc., *Trusted Solaris Audit Administration*, October 2001, http://docs.sun.com/ab2/coll.175.4/TRSOLAUDADMIN/@Ab2TocView?Ab2Lang=C&Ab2Enc=iso-8859-1

[17] Wyk, Kenneth R. van, and Richard Forno, *Incident Response*, August 2001, O'Reilly Book Excerpts, 13 December 2001, http://www.onlamp.com/pub/a/onlamp/excerpt/incidentres_07/index2.html

Bibliography

Atkins, Todd and Stephen Hansen, *Centralized System Monitoring With Swatch*, Proc. LISA VII, Usenix Assoc., 1993, http://oit.ucsb.edu/~eta/swatch/lisa93.html

CERT Coordination Center, *Installing, configuring, and using Tripwire to verify the integrity of directories and files on systems running Solaris 2.x*, 4 June 2001, http://www.cert.org/security-improvement/implementations/i002.02.html

Coast Intrusion Detection Systems Collection, ASAX, http://www.cerias.purdue.edu/coast/intrusion-detection/ids.html

Internet Security Systems, *RealSecure Installation Guide Version 6.0*, May 2001

Intrusion.com, Inc., Kane Secure Enterprise, http://www.ei-europe.com/kane_secure_enterprise.html

Noordergraaf , Alex and Glenn Brunette, *The Solaris Security Toolkit – Quick Start*, Sun

BluePrints Online, June 2001, http://www.sun.com/security/jass

Noordergraaf , Alex and Glenn Brunette, *The Solaris Security Toolkit – Internals*, Sun BluePrints Online, June 2001, http://www.sun.com/security/jass

Roesch, Marty, *Snort – The Open Source Network Intrusion Detection System*, http://www.snort.org/about.html

Spitzner, Lance, *Armoring Solaris: PreparingSolaris for a firewall*, 19 August 2001, http://www.enteract.com/~lspitz/armoring.html

Spitzner, Lance, *Armoring Solaris: II, Preparing Solaris 8 64-bit for CheckPoint FireWall-1 NG*,
05 November, 2001, http://www.enteract.com/~lspitz/armoring2.html

Spitzner, Lance, *How to automate your log filtering, Watching Your Logs*, 19 July 2000, http://www.enteract.com/~lspitz/swatch.html

Sun Microsystems, Inc., *Trusted Solaris Installation and Configuration*, October 2001, http://docs.sun.com/ab2/coll.175.4/TRSOLINSTALL/@Ab2TocView?Ab2Lang=C&Ab2Enc=iso-8859-1

© SANS Institute 2000 - 2005 Author retains full rights.