

Running head: OPEN SOURCE INTRUSION DETECTION AND PREVENTION

Open Source Intrusion Detection and Prevention: Tools for Today's Corporate Market?

Craig Gosselin

Eastern Carolina University

Abstract

There are literally hundreds of reported network attacks each day. Our systems are being compromised by persons trying to intrude, stop, obtain or destroy our precious data. The ability to detect intruders and monitor the network systems that you operate is not just an option. The Sarbanes Oxley Act is a warning to our publicly traded companies that we are not going to be allowed to sit idle as corporate leaders or IT professionals while there might be huge gaps in our network defenses. Network tools for monitoring intrusion and tools to prevent intrusion can be completely cost inhibitive to a company that has not prepared to budget for their implementation or has little exposure to their use. This paper discusses two open source tools, Snort and Bro that are either no cost or low cost that you can obtain and train to use. These tools are designed to monitor traffic, analyze protocols, capture packets, map networks, port scan and prevent intrusion. Whether the attack is from the outside of your LAN or from the inside, do you have the tools and training to meet the demands of securing your network data?

Open Source Intrusion Detection and Prevention: Tools for Today's Corporate Market?

Somewhere between December 2004 and March 2005 over 4000 credit card numbers were stolen by intruders from the Rhode Island State government website (Rosencrance, Linda. 2006). The breach was discovered in December 2005. The intrusion has caused a series of issues with the persons affected not only having had their lives changed due to the financial concern over a stolen credit card but also that of identity theft lingering over their lives. The Rhode Island system of operation that once allowed for renewal of certain licenses and services over the web has also been affected. The US Secret Service is involved as an investigative agency and several security companies have been hired to examine the operation of the network and secure it against possible reoccurring attack (Rosencrance, Linda. 2006). The Rhode Island website operated by NEI (New England Interactive) is not alone in the fact that its security was breached. Many companies are defenseless and in a similar position. They have no expertise amongst the excellent systems administrators employed in their corporate ranks to maintain an aware system that simply detects intruders rather than trying to block them, like that of the firewall or router administration.

Reputation lies upon the ability of a company's IT security to keep spyware, malware and virus in check and fraudsters from phishing right under the nose of IT (Wilson, Tim 2006). Network Intrusion Detection Systems (NIDS) are designed on the principle that there is a low possibility of stopping all types of attacks, due to the nature of network design (Grace, Clive. September 2000). There are fists full of application ware to consider when selecting a NIDS. Many NDIS suites are very expensive and require special training and certification before proficiency can be claimed. The combined costs of revamping an IT program to include a fully developed NIDS within your company can be staggering. The Certified Computer Security

Incident Handler is a certificate yielding training program and can cost in excess of \$10,000US for the courses and the exam for each candidate (Carnegie Melton). This is just one of many training/certification programs available to the corporate IT public to help improve the knowledge and proficiency in the area of intrusion detection. IDS (Intrusion Detection System) software suites are often cost prohibitive for companies that run a lean IT budget and for that reason the entire topic of NIDS is usually brushed under the carpet by those decision makers that budget corporate funds. The reality is that companies are really only lacking one element of good network defense, expertise (Grace, Clive September 2000). Open Source Intrusion Detection System (IDS) software suites are available at no charge. Training and expertise becomes the sole hurdle and that blocks project acceptance of a NDIS program in a corporate environment.

The key to minimizing the risk of attacks from outside sources is in the basic knowledge of the risks your network faces (Wilson, Tim. February 2006). The trained NIDS and IDS administrator is the person with the expertise to manage the network defense by looking at the locations where a breach can occur and then by monitoring that area. As experts in our IT fields, we already understand that there are certain risks that companies must accept in order to maintain their presence on the Internet. By having the software and expertise to monitor the risks our mission becomes safer and less stressful from a network security standpoint. This paper will examine two of the most popular open source IDS and NIDS applications and introduce several available other products that may help you to open your thinking once again to NIDS as a possibility where you once found the thought denatured by budget constraints and fear.

The first basic need is to introduce intrusion detection and assist your corporate entity by elevating the knowledge that you have about the topic. The IDS systems are

available in two types, Anomaly/Misuse Detection or Single/Multiple Host (Grace, Clive September 2000). Anomaly/Misuse Detection provides two different philosophies of intrusion detection: anomaly detection and misuse detection.

Anomaly detection packages use statistical detail rules that examine the profile of use by a typical network client or a typical user. The profile of a particular user has information like the average duration of a telnet or ftp session, the average packet size in bytes typically transmitted; the time that terminals are accessed by this particular client/user. The profile retrieved from a host machine contains important information like, average CPU utilization, the average number of users logged in at specific times and the addressing of the client PCs based on IP and MAC addressing. Anomaly detection software packages constantly compare these typical profiles of users and host systems to current network traffic. Should the Anomaly type package detect a large change in the network traffic based on the “normal” profile it uses as comparison, it launches an alarm to the predetermined administrator.

Misuse detection works by employing a database of known attacks similar to of a database of antivirus definitions. The Misuse type detection system uses a set of rules called signatures that see a pattern in the network activity of an intrusion and logs the results of the attack.

The Single/Multiple host detection type intrusion detection system is amongst the first types of available intrusion detection systems. This type of IDS takes a less complicated approach in that these types of IDS systems scan log data collected from a single machine or multiple machines (network equipment).

The Single host IDS creates a decision based solely on information data offered from one client PC. This type of IDS is not capable of detecting attacks deriving from several sources at the same time. Though this is not the de facto standard of open source NDIS today, this system can still provide worthy information and indication of an attack.

The Multiple host IDS has advanced the capability of the Single host IDS. It uses several client PCs or network devices to make its comparison of the activity on the network. This form of IDS is incorporated in many of the current NIDS packages even though it still relies on logs generated by the client operating system, which categorizes this IDS type as architecture-dependent. Even though the system is vulnerable to Denial of Service attacks, stealth logging can help elevate this type of IDS to a useful tool (Grace, Clive September 2000).

Figure 1 represents a graphical view of a modern IDS system that uses leaf agents placed on the client network PCs and network devices to monitor the network. It represents a general overview of any of the above mentioned systems.

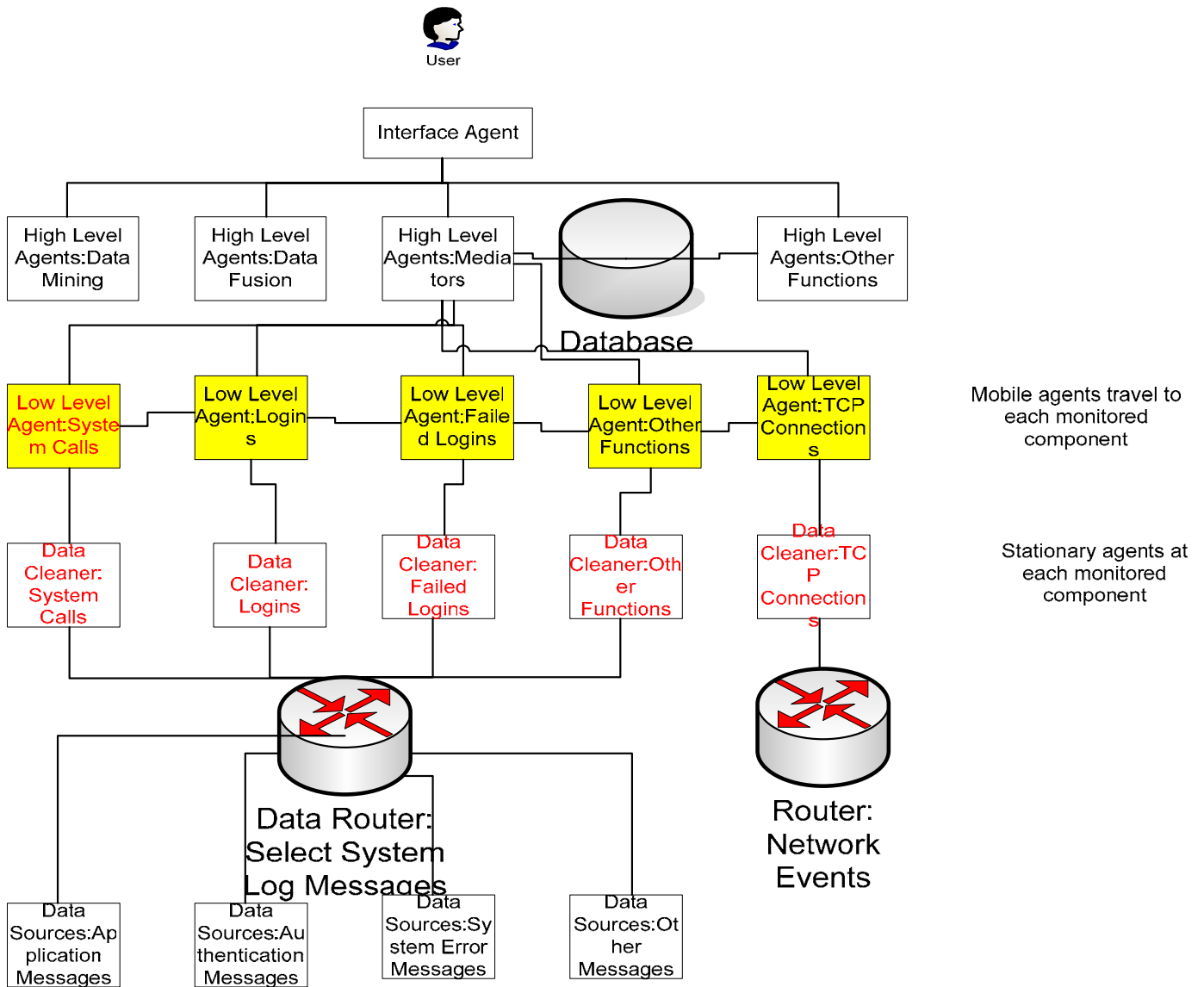


Figure 1: Typical Mobile Agent IDS

Helmer, Guy., Honovar, Vasant., Miller, Les., Wang, YanXin., & Wong, Johnny. (2003).

The most popular and best rated open source NIDS application is Snort (Vossen, JP. May 2005). Snort is such a great weapon against network maladies that it competes against most enterprise-grade IDS tools. Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language (misuse type of IDS), which combines the benefits of

signature, protocol and anomaly based inspection methods (www.Snort.org). ISS RealSecure and Symantec Manhunt are two highly thought of enterprise IDS applications. Manhunt purchased from ECost.com is in excess of \$20,000US for the 2.0GB open platform install, while Snort is available to your company for a no fee price. The value to the corporate enterprise team offered by Snort is more than the sum of its cost free price. The adoption of Snort into the corporate IT/IS arena is accompanied by a decent amount of support. Support and expertise are usually the main reason that open source tools are usually pushed aside.

Snort has been under development for more than ten years. There is a huge amount of documentation and expertise available to assist the untrained IT/ IS team to come to speed on its use and its capacity to monitor your network. This is a bonus to the needy company and may make the selling point a bonus when the proposal is offered to management. The documentation is available at the SNORT web site (Vossen, JP. May 2005).

The SNORT engine can run on all of today's most popular operating systems and is not confined to a fully vested server hardware platform. (Vossen, JP. May 2005). Hardware and OS licensing issues alone makes it a huge cost and infrastructure bonus to a company seeking a NDIS software solution to network security. A solution that can be run on a non-server operating system and a non server hardware platform is a positive feature. The SNORT service can also be run as a stealth tool. It can be hidden from the network and be better protected from the attacker so it can continue logging intrusion if the network should become compromised (Bauer, Mick October 2002).

Mick Bauer, in the October 2002 article titled *Stealthy Sniffing*, *Intrusion Detection and Logging*, describes a great benefit designed into the SNORT application, that of stealth logging. A service that can be run in the

background without an IP address is certainly a self-protecting system. Network probes and log servers form a group of unique services due to the fact that their roles are basically passive. They are designed to retrieve data and log the capture, rather than send data. Fact, this feature can be a super tool in the security of the service and a great advantage to the SNORT application. By making SNORT inaccessible from the networks they protect you have allowed the log to continue even during an intrusion and thus the tool will help prepare the infrastructure from future attacks. This increases its value in a proposal and makes a lot of sense (Bauer, Mick October 2002). The Bauer article also is a great how-to for those looking to hide other logging services on their networks.

A second network based NIDS is Bro. Bro was created by Vern Paxson at the Lawrence Berkley National Laboratory and International Computer Science Institute. It is a powerful tool used as a NIDS system.

Bro is an open-source, UNIX platform Network Intrusion Detection System. The capabilities of Bro are similar to those of Snort. Bro monitors network traffic using an open source set of rules to look for suspicious traffic. Since Bro is customizable by your own development persons, the policies and the unique language are open source, which allows an administrator/developer to determine and control Bro's capabilities on the network. As new forms of network attacks are discovered the site rules can be modified to contain the signatures of those new attacks and better monitor them. Like Snort, Bro can detect anomalies in network traffic. These anomalies can be captured and placed in a log file for later investigation or an alert can be generated.

Bro is not intended as a solution for a non-UNIX aware corporate enterprise IT/IS team . It was created with the intention that it would be administered by a UNIX expert that has additional training and knowledge of Bro and this might be a limiting factor for a corporate decision-maker to understand. The attraction and benefits, making Bro a real world tool on your network, is its capabilities in the hands of an expert. Bro can provide excellent enterprise NIDS at a low cost. Bro is adopted to use Snort signature scripts. The Bro platform is an open-source system. It is run on UNIX, which is a highly stable OS. The hardware requirements are very liberal. Bro does not require a server hardware setup to run.

Bro detects intrusions by comparing network traffic against a customizable set of rules describing events, like that of Snort, that are deemed troublesome. If Bro detects something of interest, it can be instructed to either generate a log entry, alert the operator in real-time, or initiate the execution of an operating system command. Bro is touted as being a more powerful tool for NIDS than Snort, since its tools are created to be more network aware and will detect and report (or act upon) foreign activity on the network as it is detected (Paxson,Vern., Rothfuss, Jim., Tierney, Brian. December 1, 2004).

Snort and Bro are designed to completely integrate into a network. The expertise to fully take advantage of the features offered by these two tools is certainly only answered by the enterprise that is integrating them. The tools are both open source and the code is available for any company to further develop. By properly understanding the tools and allowing for development and maturity on your network, these tools will offer the second layer of protection that is necessary to properly understand the weaknesses that might

allow your network to be compromised. Once the understanding of the network vulnerabilities are known and the decisions are made on how to best protect the organization a program of upgrade and monitoring can be implemented.

Snort and Bro are just two of the NIDS systems available as open source tools for your consideration. AIDE, Advanced Intrusion Detection Environment, is a Source Forge supported NIDS tool that will run on the UNIX platform (<http://www.cs.tut.fi/~rammer/aide.html>).

AIDE was not chosen to be fully represented in this paper due to the lack of full support and product documentation. This product is still in its infancy and may turn out to be a real great find. It should not be dismissed from your list of choices if you are looking for a UNIX based NIDS. SHADOW IDS is a second IDS, open source tool that was not fully discussed in this paper (<http://www.nswc.navy.mil/ISSEC/CID/index.html>).

SHADOW is a portion of a project that was initiated by CIDER (Cooperative Intrusion Detection Evaluation Response). The Naval Surface Warfare Center is the backbone of this open source project along with several other government agencies. The project has been in development since 1998 and has been well documented. Shadow uses tcpdump and libpcap library as its under laying code. Shadow has an advantage over the Snort tool. Shadow allows the administrator to place sensors throughout the network to offer a more distributed IDS (Dubrawsky, Ido 2006).

Linux Intrusion Detection System (LIDS) (<http://www.lids.org/>) is a patch to the Linux kernel that can be applied to the Linux OS and used as an admin tool. This tool applies to the kernel 2.2.19 and requires that once the patch is applied that the kernel be

rebuilt. There is a good set of documentation available for this tool at the LIDS website (<http://www.lids.org/>).

Tripwire is a host based IDS (HIDS) (<http://www.linux-sec.net/IDS/>) that is a project of the Purdue University (Dubrawsky, Ido 2006). It is available for purchase from the University of Texas (<http://www.utexas.edu/its/sds/faq/tripwire.html>) or the open source version is available at <http://www.tripwire.org/>. Tripwire is one of the oldest developed IDS (1992). It was developed by Dr Eugene Spafford and Gene Kim at the Purdue University COAST Laboratory. It can be installed on a Linux or FreeBSD system.

There are many other tools used as IDS systems valued for consideration on your list but the ones mentioned in this paper hold the highest attention in the open source development of IDS. Please evaluate every software product before considering the possibilities of its use on your network. Each application has its strengths and disadvantages. The best approach is to first begin the process by getting started with the education necessary to understand the implications of a NIDS. Then choose the model and product best suited for your network, budget and expertise.

References

- *Bauer, Mick. (October 2002). Stealthful Sniffing, Intrusion Detection and Logging. *Linux Journal*, 15, 503-522. Retrieved February 18, 2006, from <http://www.linuxjournal.com/article/6222>.
- Carnegie Melton Software Engineering Institute (n.d.) CERT-Certified Computer Security Incident Handler. Retrieved February 19, 2006, from <http://www.cert.org/certification/>
- *Dubrawsky, Ido. (2006). Freeware Intrusion Detection Tools. *Sys Admin: the Journal for UNIX and Linux System Administrators*. Retrieved April 9, 2006, from <http://www.samag.com/documents/s=1147/sam0108o/0108o.htm>
- *Grace, Clive (September 2000). Understanding Intrusion Detection Systems. *PC Network Advisor. Issue 122*. Retrieved February 18, 2006, from <http://www.itp-journals.com>
- *Helmer, Guy., Honovar, Vasant., Miller, Les., Wang, YanXin., & Wong, Johnny. (2003). Lightweight Agent for Intrusion Detection. *Journal of Systems and Software*, 109-122. Retrieved February 18, 2006, from <http://www.cs.iastate.edu/~honavar/Papers/jss-lightweight.pdf>.
- Holden, Greg. (July 2003). *Guide to Firewalls and Network Security: Intrusion Detection and VPNs* . Boston: Thompson Publications.
- Jacobson, Van., Leres, Craig., & McCanne, Steven. (n.d.). *TCPDump-dump traffic on a network*. Retrieved February 19, 2006, from http://www.tcpdump.org/tcpdump_man.html .
- Laing, Brian. (2000). Internet Security Systems: How to Guide-Implementing a Network Based Intrusion Detection System. Retrieved March 21, 2006, from <http://www.Snort.org/docs/iss-placement.pdf> .

- Lamping, Ulf., Sharpe, Richard. & Warnicke, Ed. (2005). *Ethereal User's Guide*. Retrieved February 18, 2006, from http://ethereal.hostingzero.com/docs/eug_html_chunked/
- Paxson, Vern., Rothfuss, Jim., Tierney, Brian. (December 1, 2004). *BRO User Manual*. Lawrence Berkley Laboratory. Retrieved April 5, 2006, from <http://Bro-ids.org/Bro-user-manual.pdf>
- *Rosencrance, Linda. (January 2006). R.I. government site hacked, credit card numbers stolen. *ComputerWorld*. Retrieved February 19, 2006, from <http://www.computerworld.com/securitytopics/security/holes/story/0,10801,108199,00.html>
- *Vossen, JP. (May 2005). *Snort Technical Guide*. *SearchSecurity.com*. Retrieved May 18, 2000 from http://searchsecurity.techtarget.com/general/0,295582,sid14_gci1083823,00.html
- Weaver, Randy. (January 2006). *Guide to Network Defenses and Countermeasures* (2nd ed). (pp. 70-84). New York: Thompson Publications.
- Wilson, Tim. (February 2006). *IT Security: Small Companies, Big Problems*. *CNS Magazine*. Retrieved February 20, 2006 from <http://www.cnsmagazine.com/itsupplement/articles/article2.asp>