Global Information Assurance Certification Paper

Deploying IDS in Complex and Unpredictable Environments: A Consultants View

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b

Billy Stanley

February 28, 2004

Table of Contents

1.0 - Abstract

Intrusion detection systems have been available for quite some time now. These systems range from the relatively inexpensive open-source products to those that cost thousands of dollars. Along with the initial product cost, one must consider the costs associated with the hardware, labor, support and overall service delivery. Although we briefly cover the cost aspect, we will primarily concentrate on the service engagement model from a consultant's perspective.

From a high-level perspective, we will review of some of the portability options available to us with the Snort intrusion detection suite. We examine devices that are designed to fit in to the enterprise as a permanent fixture, to those that fit in your pocket, designed for emergency response scenarios. We will perform cost and functionality comparisons of each option, and will come out with a clear understanding of where each should be used in different environments for data collection. Although data analysis and reporting are just as important as data collection, there is a fairly straight-forward approach that fits most models. We will discuss this approach in more detail, and learn some of the best practices associated with data analysis and reporting.

2.0 - Legal Issues

The first and arguably most important step in delivering a service is to formally agree on the terms. This agreement is documented as a legally binding contract between two or more parties detailing the work that is to be performed. As with most contracts, this is a living document that is expected to change. Changes should be added in the form of amendments so it is clear to others what has transpired throughout the term of the agreement.

Verbal and electronic discussions are a critical part of any service engagement. It is important however, that any agreements made through verbal or electronic means are clearly documented in this contract.

2.1 - Legal Liability

Legal liability is one of the most important reasons for creating this formal agreement. Unfortunately, we no longer live in an era where we are able to do business on a hand-shake. Those were the days where one's word was one of the most important things he had. The worse thing that would happen to someone who contradicted his word was that his reputation would be destroyed. In today's society, it seems as though people are more concerned with making money than upholding their word.

With the world as our market place, destroying a relationship here or there may not be so bad, right? This type of attitude has brought us to a point in life where legal suits are the norm. It is also fair to say that the electronic era, whether we

believe it or not, have contributed to this behavior. Let's face it, technology changes at a pace that even we as consultants can barely keep up. How can we expect someone outside of this industry to even have a chance? The main point here is that it would be easy for technologists to unknowingly take advantage of someone who may be less familiar with the subject. By managing the engagement under the framework of a contract, we can mitigate many of the inherent sociological problems.

2.2 - Data Privacy

Another legal aspect to consider from a security point of view is data privacy. Since the consultant will have access to the traffic which they are analyzing, they must fully agree with and respect the laws that govern privacy of data. This should be clearly documented in the terms of service.

A few data privacy references include the 'Privacy Act of 1974', the 'Electronic Communications Privacy Act of 1986' and 'HIPAA – Health Insurance Portability and Accountability Act'. The 'Privacy Act of 1974' is primarily focused on regulating what governmental institutions can do with personal data. The Electronic Communications Privacy Act of 1986' is mainly focused on managing eavesdropping and wiretapping. HIPAA is primarily concerned with the confidentiality of medical records.

3.0 - Deployment Scenarios

Now that the legal issues are out of the way, we can begin investigating some of the IDS deployment scenarios. Although there are many ways to deploy Snort, it is important to categorize the options and provide a brief overview before we can proceed further. There will be a more detailed analysis of each option later.

3.1 - Overview

The first of the three deployment categories is the 'Appliance'. An appliance is typically thought of as an all-in-one, special purpose, hardened device. The appliance is usually a rack mountable device, often with a certain amount of hardware-based redundancy. For the sake of this review, we will make the same assumptions.

The second deployment category is the 'Portable'. The portable solution is technically any computing device that is not rack-mountable. Although workstations fall in to this category, most portable installations will be some type of laptop/notebook device. These devices can usually compete with the appliances in terms of processing horsepower, but the portable device lacks many of the redundancy features inherent in the Appliance.

The third and final category is the 'Portable File System'. There are many hardware solutions that fit this mold, including portable hard drives and miniature USB disks. To demonstrate some of the extreme portability options of Snort, we will limit our focus to the USB disk from this point forward.

3.2 - Hardware and Cost Comparison

Since we are looking at open source software for the data collection and analysis suite, our focus here will be limited to the hardware, operating system and labor costs.

3.2.1 - Hardware Overview

The appliance is, by far, the most expensive hardware solution of the three. An important point to keep in mind however; is that an appliance is really a server-class machine that has been hardened and tailored for a specific purpose. Some of the qualities of an appliance include large amounts of horsepower, multi-processing capabilities, data capacity, network throughput and internal redundancy. Using the HP Proliant server class as our base, here is an example of the current price breakout:

Model	Processor Type	Processor Speed	Processor Quantity	Memory	Internal HD Quantity	Form Factor	Price Range
DL 140	Intel Xeon	3.2 GHz	2	1GB – 4GB	2	1U	$1149 - $2999
DL 145	AMD Opteron 200	2.2 GHz	2	1GB – 16GB	2	1U	$1599 - $2999
DL 320	Intel Pentium IV	3.06 GHz	1	128MB – 4GB	2	1U	$1394 - $2256
DL 360	Intel Xeon	3.2 GHz	2	1GB – 8GB	2	1U	$1799 - $3599

Although there are many other devices that could be deployed as appliances, these are the four that fit the 1U form factor.

The portable solutions are comparable in price to the appliance, but lack in terms of physical redundancy and throughput. Processing speeds are similar, but the portable will be limited to a quantity of one processor, limiting it to single processing tasks only. Portables are also limited on the memory and HD quantity/capacity. So what is the portable good for?

The portable is good for using in non-permanent, dynamic environments. It is easy to carry in to a customer site, plug in, make minor configuration changes as required, and let it go! Unlike the appliance, the portable comes equipped with its own keyboard, monitor and mouse, making it easy to adjust configurations or analyze reports. It is also normal for the portable to be used as a multi-purpose device by a consultant for other functions.

While the appliance and the portable are very similar in nature, the portable file system is at the other end of the spectrum. This device is small enough to fit in the palm of your hand and is not designed to compute. It is literally a data repository which will hold the Win32 version of Snort. While the portable file system is completely dependent upon a 'host' computer to function, it is also extremely portable. As long as the host meets certain pre-requisites (we will discuss these shortly), operation can be as easy as plugging the device in and issuing a command to initiate the process.

The cost for such a system is negligible, when compared to the previous two options. You can spend less than $100 and get an adequate USB disk capable of holding the required software. The costs that are avoided by pursuing this solution are the 'host' and operating system costs, which have already been previously spent. If you do not have an existing 'host' to support this type of installation, it is **not** recommended that you go out and buy one specifically for this function. It would make more sense to go buy an appliance or portable to service your needs.

3.2.2 - Integration Effort

From an integration perspective, the 'appliance' requires the most effort when compared to the other two solutions. Some of the qualities of an appliance include:

- Rack Mountable Hardware
- Redundant Power Supply Modules
- No Integrated Keyboard, Video or Mouse
- Special Cooling Requirements

In addition to the facilities requirements listed above, the appliance requires a considerable amount of time to install and configure. Once installed however, it is typically considered to be permanent. This makes this solution the ideal choice for long-term support engagements.

The 'portable' is much easier to install since it comes bundled with its own keyboard, video and mouse. This device can sit virtually anywhere, as long as there is a physical connection to the network. Ideally, we would like for any sensor to be placed in a secure area in order to limit some of the security risks. Since this device will have access to all data flowing on the monitored subnet, we need to make sure that everyone is aware of, and accepts, the associated risks. The device is more than likely pre-built so the deployment and integration effort should be minimal. This device is usually installed in situations where there is an immediate need for response.

The portable file system requires the least amount of effort of all. Since this solution is nothing more than a portable disk with the IDS software installed, there is no need for bulky hardware, complicated operating systems, facilities requirements, etc. The only requirement is that the customer has a capable desktop or server with USB support, capable of reading the file system. This system is not designed to be a long-term solution.

3.2.3 - Network Configuration Support

Before we dive in to what each option is capable of supporting, it is important that we understand the requirements of IDS. Snort, or any IDS package for that matter, is nothing more than an intelligent traffic analyzer. Snort's sole purpose is to 'watch' any and all traffic that it is capable of seeing, compare that traffic to a set of 'rules' that are pre-configured, and perform an action. The action, unlike firewalls, is to either disregard or log the data as an event. Firewalls are very similar, but they are expected to take action on the particular traffic, either allowing or disallowing it, similar to a traffic cop. Snort, as described above, is completely passive.

Network compliancy is one of the most important components of any IDS implementation. In order to get the most out of your solution, it is important to understand the environment for which you want visibility. As stated earlier, your network card has to be able to keep up and 'watch' all other network traffic on the subnet or the product is worthless.

From a network interface perspective, it is important that your network card is capable of keeping up with the aggregate amount of traffic on the network you wish to monitor. When we talk about aggregate network traffic, keep in mind that we are referring to all traffic on that particular subnet or VLAN. It's important to analyze traffic patterns and bandwidth before you deploy anything. You may decide that a 100MB switch port is incapable of delivering the amount of data you want to see from a subnet consisting of 20 other 100MB switched devices. A decision might be made to move the sensor up in the network hierarchy and watch the data with a gigabit interface. You can always consult your network support group for information on the average throughput of a subnet.

From a hardware perspective, a good rule of thumb is that any switched network greater than 100Mb should be monitored with an appliance or server-class machine. Factors such as the bus speed, RAM, multiprocessing capabilities and horsepower all come in to play. It is important, wherever possible; to monitor the network with a network card that has no other purpose on the network. Keep any management traffic on a live network card, bound with whatever protocol your network calls for and monitor traffic from another live interface card without any protocols bound.

While the appliance can be equipped with whatever type of network card is required, the portable solution is typically limited to speeds of 100Mb or less. Sure there is support for gigabit technology in the portable architecture, but the underlying infrastructure will often have trouble keeping up.

Since the portable file system solution is completely dependent upon the underlying host, it is important that similar rules of thumb are followed with regard to networking on the host.

3.2.4 - Data Logging

We will look at several different options for logging our captured data. It is important to understand the importance of a concise rule-base when configuring an IDS system. The more you enable, the more you (or someone) will have to sift through at a later time. The Snort analysis suite is packaged with hundreds of rules and triggers, designed to meet specific sets of needs. You should experiment with the amount of rules that are enabled at any given time and tailor the selection around specific problems you suspect.

Although Snort supports a wide range of logging options, we will focus on four distinct methods. Local and remote log files and database collection are the options that will be reviewed.

Before we discuss the logging details, it is important that we make a couple of critical assumptions. The first assumption is that any data collected by one of the sensors is considered sensitive and should be protected from any public access. The second assumption is that the internal or corporate network is protected in this manner through a combination of logical and physical security. Now that the baseline is set, let's look at some of the options.
The database collection method is our first priority for several reasons. A database provides us with a structured location for quick information retrieval and portability. The best analogy is to think about a file cabinet full of documents that have not been sorted, versus a cabinet where the documents are physically separated and marked through some meaningful scheme. The data in the file cabinet has not changed in either scenario, but the speed of data access and data portability has.

The log file method, while not the preferred, is still important because there will be scenarios where we will not be able send data directly to a database. In these scenarios, we will log the data to a log file first and then import the information in to a database later for analysis.

From a support perspective, there are several options to choose from when analyzing logging scenarios. See the chart below for more detail:

Logging Method	Supported Platform	Benefits / Service Engagement
Local Logging	Appliance, Portable, Portable File System	Local logging is typically used in emergency situations where a database may not be readily available. This is also a method that might be used for new installations where there is no existing infrastructure in place to support database logging. This is typically thought of as a short-term solution.
Remote Logging	Appliance, Portable	Similar to local logging, remote logging is not the ideal solution, but it is possible that there are other mitigating factors that affect how data can be transmitted between a customer and service provider. The reason that the portable file system is not supported for this implementation is that it is expected that an encrypted tunnel be set up between the capturing device and the service provider. This device is unable to originate or terminate the required encrypted tunnel.
Local Database	Appliance, Portable, Portable File System	The preferred method for installations where all data is to remain at the customer site. This may also be a desired solution for more complex installations where database replication is configured for off-site partners.
Remote Database	Appliance, Portable	Similar to the local database method, but used where the data will be analyzed by a service provider, remote network or security operations center. Just as with remote logging, the portable file system does not support this function since we do not typically have control of (or trust) the host device.

3.2.5 - Ongoing Maintenance

Ongoing maintenance is an extremely important aspect of any intrusion detection installation. Much like the anti-virus definition files on your workstation need to remain updated, so do the signatures within the Snort IDS system. With the exception of statistical-based IDS, these systems are only as good as the information that we currently know. If a brand new attack using exploits that have never been used before were unleashed, the chances are good that our system will not recognize it as a potential attack. This is typically ok since many of the attacks are either already known or are piggy-backing on other vulnerabilities that we are already looking for.

Staying in touch with the technical community is an important aspect of maintenance. There are many mailing lists that one can subscribe to get regular updates on snort rules and product suggestions. These are usually open forums

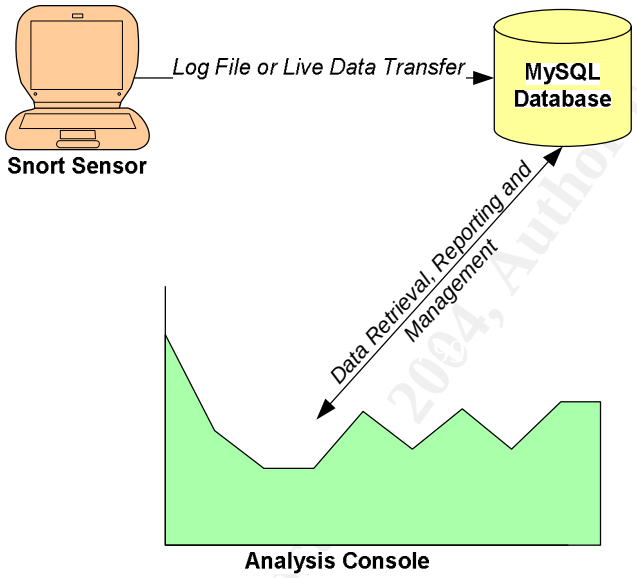
where anyone can submit data, so it is important that any new signature or rule base is tested prior to implementing.

4.0 - Data Analysis

4.1 - System Architecture

Once the data has been captured and logged, we can begin to think about data analysis. As we discussed before, it is important that the snort rules have been carefully configured if the plan is to use this in a high-traffic environment. It is not abnormal to produce hundreds of thousands of events in a matter of seconds if you enable every possible scenario. Be concise.

The overall flow of data will be something similar to the following:



ACID (Analysis Console for Intrusion Databases) is the specific product we will be using for data analysis. Although ACID is designed to support several different data sources including database feeds, log files, syslog dumps, etc., we will be focusing on using it with MySQL. The web-based interface allows the user to sort through the various alerts, analyze the traffic, sort the alerts based on a number of criteria, graph out patterns, etc.

As data is managed via the web-based ACID console, the system updates the information source (MySQL database in our case) accordingly. For tracking purposes, some people feel it is necessary to store the information in more than one database in order to preserve a copy of the information for historical and/or

tracking purposes. There is usually, however; an ACID feed that is continually updated as security engineers or analysts acknowledge alerts.

4.2 - Analysis Technique

One of the largest caveats regarding IDS is the fact that there are usually a large number of false-positives to deal with. It is imperative that intrusion analysts understand how to tell the difference between normal traffic and that of an attack. As an example, it is very possible to mistake legitimate DFS traffic as a DCOM attack. Since DFS uses DCOM services, it is possible that this type of traffic might be flagged as an attack. Once you get familiar with the network you are monitoring, you will be able to differentiate between these types of events.

Intrusion detection systems, in the end, are not a single silver bullet. To be effective in this business, it is important that you have a myriad of tools available to assist. Fortunately, there are plenty of excellent open-source tools available, so building your arsenal shouldn't break your pocket book.

5.0 - Data Reporting

From a service provider perspective, it is important that the customer feels good about the security service he or she is paying for. Although it is fairly easy to run reports from ACID and hand them over to a customer, this may not always be the route you want to take. There are other tools that complement the IDS service offering, which should be considered.

5.1 - Reporting for Dummies

There are many reporting packages available, depending on your requirements. Since we are talking about reporting extremely technical information, we need to set some basic rules.

- *Know the Audience* - This will very likely vary from client to client. Larger companies typically have more of an IT staff capable of understanding technical jargon. A smaller company, however; might have the CEO as the audience of the report. In either case, make sure that you tailor the report based on the readers' level of comfort of the subject.
- *Be thorough, but not too thorough* - As we previously discussed, one of the downfalls of IDS is that it is not an exact science. Because we are making determinations based on specific traffic patterns, it is important that you leave yourself a little room for error. In other words, it is important that you make a determination based on the data, but always suggest that the customer validate your suspicions.
- *Offer suggestions, but leave it that* - This will obviously depend on the service you are contracted to provide, but the main point here is that there are many ways to accomplish a task. What may seem logical to us as

consultants may not be the path chosen by the customer. Make your suggestions, but keep it to that unless you are asked to provide more information.

- *Meaningful Information* - We all know that management likes to see pictures and graphs, but accompany this information with readable text. The most important goal of any service provider in this field is to identify threats and notify the appropriate people or take the appropriate action as soon as possible. Make sure that the message you are trying to send actually makes it to the intended recipient through whatever reporting you provide.

5.2 - Recommendations

The final report should include recommendations of preventative actions. Preventative actions are those actions taken to limit or remove exposure to a given threat. Examples of these actions might be:

- The implementation of a firewall and/or firewall rules
- The implementation of access control lists on routing devices
- Password policy enforcement
- User or computer-based policies or restrictions
- Proxy device implementation
- Physical barriers
- Access card devices
- Etc.

The list goes on and on and on. One important point that needs to be made is that intrusion detection is NOT a preventative action. Intrusion detection is technically nothing more than an investigative tool. Preventative measures typically follow the detection of an event.

Based on this fact and from a service provider perspective, it is important that you always follow up any incident report with a recommendation of action. The customer may, in the end, choose to ignore the recommendation or accept the risk, but at least the offer was made. From a legal liability and technical competency point of view, this is important.

6.0 - Summary

With any service engagement, it is important that we are always cognoscente of the ramifications associated with the lack of due care. As security consultants, we are responsible for the data that we secure. Prior to taking on this responsibility, it is important that consultants are aware of the many legal liability and data privacy issues. We briefly covered a few examples in this document, but there are many more to be aware of.

Our primary focus was to provide structure around intrusion detection service provided by consultants. We limited our study to the Snort, ACID and MySQL products and discovered how each can be deployed in different environments. It became obvious that, depending on the service engagement and/or criticality, this would directly affect the proposed solution. The 'appliance' seemed to be a good fit for long-term engagements where high-availability was a requirement. The 'portable' solution worked well for consultation and demonstrations and in cases where there may or may not be a long-term engagement, yet there was an immediate requirement for advanced IDS service. The 'portable file system' seemed to fit in for the emergency response scenarios where there was typically not a long-term engagement and there was an immediate need for service. The idea behind the portable is that it is a low-cost, low-risk solution to provide to a customer for basic analysis. It does require that the customer have a compatible Win32-based device, capable of reading a USB file system. This is also handy for situations where an engineer can not be sent to the site. This device can be shipped with basic instruction for any on-site person to execute. All three options have their pro's and con's, and all three options together seem to cover just about every required scenario.

We also scratched the surface of data analysis and reporting. Anyone who has performed this service in the past understands that collecting the data is the easiest part of the job. Data analysis requires that you have an in-depth understanding of the customers' environment, including the topology, protocols/ports in use, services being offered, etc. We learned that there are quite a bit of false positives with network-based IDS and that the human element is a required piece of the puzzle. We covered the fact that successful reporting is also key and that the consultant should always consider their audience prior to sending a report. With threats and vulnerabilities at an all-time high, more and more customers are getting involved with IDS in some way. It is up to us to know how to communicate based on the customers level of comfort of IT security.

This is, by no means, intended to be a complete reference or guide to providing IDS services. This is meant to raise the awareness around intrusion detection from the consultant's point of view. It was also designed to give consultants information regarding some of the portability opportunities associated with the Snort analysis suite, and how it can be used in different environments.

7.0 - References

Roesch, Martin, Green, Chris. “Snort Manual.” Feb. 12 2004. http://www.snort.org/docs/snort_manual.pdf

Neal, Christina. “Snort Install on Win2000/XP with Acid, and MySQL.” May 8 2002. http://www.sans.org/rr/papers/index.php?id=362

McCarty, Alan. “Distributed NIDS: A HOW-TO Guide.” Nov. 6 2003. http://www.sans.org/rr/papers/index.php?id=1249

Danyliw, Roman. “ACID: Installation and Configuration.” Oct. 9 2002. http://www.andrew.cmu.edu/~rdanyliw/snort/acid_config.html

Anonymous. “Centers for Medicare & Medicaid Services: Current Enterprise Architecture Version 3.0.” Feb. 2002. http://www.cms.hhs.gov/it/enterprisearchitecture/it_direction.pdf

Riddle, Michael. “The Electronic Communications Privacy Act of 1986: A Layman’s View.” 1988. http://www.eff.org/Privacy/Email_Internet_Web/ecpa_laymans_view.article

Bushkin, Aruthur, Schaen, Samuel. “History of the Privacy Act of 1974.” 1975. http://www.cavebear.com/nsf-dns/pa_history.htm

Harris, Shon. “Mike Meyers’ Certification Passport: CISSP.” Berkeley: McGraw Hill, 2002

Northcutt, Stephen. “Network Intrusion Detection: An Analyst’s Handbook.” Indianapolis: New Riders, 1999

Scott, Steven J. “Snort, MySQL, SnortCenter and ACID on Redhat 9.0.” Apr. 2003. http://www.superhac.com/docs/snort_enterprise.pdf