Global Information Assurance Certification Paper

An Overview of PureSecure™

Abstract

This paper's objective was to examine the role of the Intrusion Detection System (IDS) in modern security strategies, establish a set of criteria for IDS evaluation, investigate the functionality of PureSecure™, an application developed and marketed by Demarc Security, and present conclusions concerning its desirability as a working IDS. The paper's objectives were accomplished by researching various sources, to include the PureSecure™ product documentation and the experience of the writer and other users who have installed and used the application. This paper documents the conclusion that PureSecure™ is an excellent low-cost product that can provide an essential part of the total security solution for many small to medium organizations.

This paper discusses the role of intrusion detection in an organization's security strategy and characteristics that an IDS should possess. It goes on to examine PureSecure™ in detail, including history, software components, architecture, installation, configuration, the graphical user interface (GUI), and offers an evaluation of the application based on the characteristics mentioned above.

Introduction

One of the major tools that is used by security administrators and security analysts to insure the safety and integrity of a network is the IDS. The IDS has become a necessary part of the security infrastructure of many organizations that use the Internet extensively. This paper will examine the role of the IDS in modern security strategies, establish some criteria for IDS evaluation, investigate the functionality of PureSecure™, an application developed and marketed by Demarc Security, and present conclusions concerning its desirability as a working IDS.

An IDS is not a substitute for a properly configured firewall. They perform different functions and the use of both at the same time is in keeping with the defense-in-depth concept[20] espoused by the Department of Defense (DOD).

The firewall is the most common device used today to safeguard and protect computer networks. Firewalls work on the principle of preventing attacks by "keeping the bad guys out" and as such provide excellent, cost-effective network protection. However, if an attack comes from within a network, the firewall will not provide protection. If an attack occurs across an unprotected link to an external system, the firewall will not provide protection. If one of a firewall's vulnerabilities (and they all have them) is found and exploited by an attacker, the firewall will not provide protection. [3]

Additional tools are necessary to provide an acceptable level of security for modern networks. These tools include: vulnerability scanners, antivirus protection, honeypots, risk assessment, and IDSs.[4]

This paper will focus on the IDS. An IDS examines network packets, audit trails, audit logs, and file system status and attempts to identify potential attacks. Its focus is on detection of attacks. As such, an IDS located inside a firewall will help protect a network from the attacks mentioned above. The IDS should be thought of as a tool that works in conjunction with a firewall to provide a higher level of network security.

IDSs may be classified as either network-based (NIDS) or host-based (HIDS). A NIDS sniffs the packets of a network and performs logging, notification, and attack responses based on this network data. A HIDS typically only examines the local network connections, audit trails, audit logs, and file system status for the host that it is running on. Its functions are based on local data.

IDSs may also be classified as "signature-based" or "anomaly-based." Signature-based IDSs attempt to identify attack signatures. Consequently, they can only detect previously known attacks. Anomaly-based IDSs attempt to identify abnormal or anomalous behavior. One of the major limitations of anomaly-based IDSs is the difficulty involved in defining exactly what constitutes "normal", i.e.—non-anomalous, behavior. Because of this, anomaly-based IDSs are not nearly as common as their signature-based cousins.[3]

Primary IDS Decisions

There are many decisions that security administrators must make when evaluating an IDS. Some of the more important decisions involve finding methods to:

- Control costs
- Control both false positives and false negatives
- Make certain that system performance remains at an acceptable level when the IDS is implemented
- Display the data in a form that allows security administrators to make an appropriate decision quickly
- Alert security administrators immediately when a critical attack occurs
- Make certain the IDS is easy to install, implement, configure, and maintain
- Make certain the IDS provides complete, accurate, high-quality documentation

In a perfect world, a network would have NIDSs between the firewall and the Internet router, between the firewall and the trusted network, and between the firewall and the demilitarized zone (DMZ). It would also have HIDSs on every host or at least the main Internet servers. In reality, this seldom happens. A typical commercial NIDS costs about $10,000 and a typical HIDS from $50 to $500. [1] Obviously this represents a major investment and management will have to make choices to keep the expense within acceptable boundaries.

Controlling false positives and false negatives is one of the greatest challenges in implementing an IDS. An excessive number of harmless activities may be identified as intrusions (false positives) and can create an enormous amount of data. This can cause an attack to be overlooked simply because it is buried among a large number of false positives. On the other hand, if security administrators fail to recognize actual attacks (false negatives), the consequences can be even more severe. A good IDS will give security administrators the ability to control the amount of data logged quickly and easily.

System performance levels must remain at an acceptable level after the IDS is up and running. All security measures will place demands on system resources and cause system performance to be negatively affected. A good IDS will minimize that effect.

A good IDS will organize and display the data in such a way that security administrators can quickly identify a possible attack, easily access additional information concerning it, and make an immediate decision as to how to handle it.

Some attacks have the potential to cause a great deal of damage and often these attacks occur at inopportune times. An IDS must be able to notify the proper personnel when a critical attack occurs. This notification must be immediate and should be difficult to ignore.

Managing a network is a taxing, time-consuming task. Installation, modification, maintenance, and updates of the IDS should be quick, easy, have minimal effect of system operation, and (preferably) be automatic.

The IDS's system documentation should communicate the information necessary for security administrators to install, configure, use, and maintain the product in a straightforward manner.

PureSecure™ – Total Intrusion Detection System (TIDS)

PureSecure™ – History

Demarc Security, Inc., a private company headquartered in Santa Barbara, California, was founded in 2001.[5] While looking for a way to improve their network security, they were unable to find a single product that offered all the features they wanted. Consequently, they developed an in-house product, which they called Demarc, that provided all these capabilities.[6] (N.B.—From this point on the writer will use the term "Demarc" to refer to Demarc Security, Inc. and the term "Demarc 1.05" to refer to the product mentioned above.) The company recognized the commercial potential of the product and made it available as an open source offering later in 2001. Demarc went through a number of releases and in April 2002 changed the name of Demarc 1.05 to PureSecure™(1.6).[7] PureSecure™ is the flagship application of Demarc and is available free in a non-commercial version.[5,7] However when intended for commercial use, the product must be purchased. A new release is planned for early 2003 that will enhance reporting and rules management.[8] Demarc also

will offer a hardware intrusion detection appliance that provides similar functionality to PureSecure™ in the near future.[9]

PureSecure™– Software Components

PureSecure™ is an application written predominantly in Perl that integrates the following tools:

- Snort—the actual NIDS
- MySQL—the database to house attack information
- Apache—the local web server that displays the data from the PureSecure™ application (*nix)
  (N.B.—"*nix" is a common term that refers to Unix-like computer operating systems, e.g.—AIX, Linux, Solaris, Ultrix, HP-UX, FreeBSD, and OpenBSD.)
  - Mod_perl—the Apache module that allows a developer to write Apache modules in Perl
  - Mod-ssl—the Apache interface to OpenSSL
- Internet Information Services — the local web server that displays the data from the PureSecure™ application (Windows)

[6]

PureSecure™ – Architecture

A network protected by PureSecure™ consists of the following components:

- Console—acts as the server in a traditional client/server configuration
- Auxiliary Sensor—acts as the client in a traditional client/server configuration

The Console controls the functions of the PureSecure™ application on the network. It allows security administrators to configure, control, and monitor the network. Typically, it contains both the MySQL server and the Apache web server. The Console is frequently, but need not be, an auxiliary sensor. The Console accepts data from the auxiliary sensors, stores it in the MySQL database, retrieves the data, and displays it on the Console in a form that is easily usable by security administrators and other console users.

The PureSecure™ Auxiliary Sensor can perform a variety of functions to include integrity checks, local process monitoring, and log file monitoring.

The Auxiliary Sensor has the MySQL client installed as well as its own copy of Snort.

PureSecure™ – Installation

Platforms

Demarc Security's Knowledge Base, Case ID PS2002071716443 describes the various platforms that PureSecure™ is compatible with as follows:

PureSecure is compatible with all the major Linux distributions; FreeBSD, Open BSD, NetBSD, Solaris, as well as many other Unix-based operating systems.

PureSecure is also compatible with Windows NT, Windows 2000, and Windows XP. Other versions of Windows, such as 3.1, 95, and 98 are not compatible with PureSecure, since they do not support services to be run."[11]

[11] Demarc Security, Inc., "Support – Knowledge Base (PS2002071716443)"

Procedure

The most difficult portion of the installation of Demarc 1.05 was the configuration and installation of all the component parts, e.g.—Snort, MySQL, Apache, and ModSSL. Security administrators will experience these same difficulties when installing other similar packages, e.g.—ACID and SnortSnarf. PureSecure™ handles these details through an interactive script. In order to successfully install the product, there are relatively few questions to answer, beyond the obvious ones, like IP addresses and user name/password. The whole installation takes about 25 minutes on *nix. (Slightly longer on Windows.)

PureSecure™ – Configuration

Network Intrusion Detection

PureSecure™ can configure the Snort rules from the web interface. PureSecure™ can:

- Edit Snort's configuration file **(*snort.conf*)**
- Add/Edit/Delete Snort rulesets
- Validate an auxiliary sensor's rules
- Control automatic updating of Snort rulesets [12]

For the most part, administration of the PureSecure™ NIDS is simply Snort administration with a GUI interface. It is highly desirable for security administrators to understand Snort to correctly configure the network. PureSecure™ makes it easier to edit ***snort.conf*** and to add/delete/modify the rulesets, but the administrators must be familiar with the format of these files or they will have serious difficulty configuring PureSecure™ to function efficiently on the network. PureSecure™ has two additional features that make NIDS configuration easier. First, security administrators can validate the Snort rules to determine if there are any syntactical errors. Second, they can manually or automatically update the Snort rulesets from a mirror of the Snort rules database found at the Demarc web site.

Extensible Service Monitoring (ESM)

ESM is one of the features that distinguishes PureSecure™ from most other IDSs. It is unusual to find ESM-like features included with a NIDS application. ESM allows security administrators to perform a variety of functions on specified services on a host-by-host basis. These functions can range from simple connectivity checks to full-blown maintenance

procedures. They are specified in PureSecure™'s pre-written routines or in routines created by end users or third parties through an application program interface (API) provided by Demarc. They may check different types of services, such as:

- Well-known network services like HTTP or FTP.
- PureSecure™ provided local services, for example checking disk space (Disks), processor load (Load), log files (Logs), and processes (Proc).
- Extended services created by end users or third parties through the API. [12]

ESM requires that security administrators create a distinct database of hosts and logical groupings of hosts to run any of its monitoring events. This is done from the GUI. [12]

ESM checks the desired services every five minutes and evaluates their status as either good, warning, or critical, indicated respectively by a green, yellow, or red LED icon displayed on the PureSecure™ GUI.

System Integrity Verification (SIV)

SIV is another of PureSecure™'s distinguishing features. SIV works on the same principle as Tripwire; it creates a cryptographic hash of selected files and then compares subsequent hashes with the original. By default, files are checked every 30 minutes.

In addition to the cryptographic hash, PureSecure™ checks the following file characteristics:

- Inode number (*nix)
- File permissions
- User ID of owner
- Group ID of owner
- Size of the file
- Modification timestamp
- Creation timestamp[12]

PureSecure™ also compares the size and cryptographic hash of selected web pages for signs of tampering.

Notification Alerts

When PureSecure™ detects an attack it can send out a notification to a specified email recipient, cell phone, or pager. Security administrators can configure it to send a notification for every attack that generates a NIDS alert, every defined ESM event, every instance of SIV tampering, and every general alert that it detects. This is generally not desirable. In order for the system to perform properly, security administrators must choose parameters carefully to ensure that notifications are kept at a manageable level. Parameters for each notification are logically "AND-ED" together; so all parameters to the notification must be true to trigger the alert.

The parameters that security administrators can set for NIDS alerts are:

- Email recipient—To whom security administrators are sending the notification
- Classification priority level—As defined in ***snort.conf***
- Email detail level--Low for mobile phones and pagers; high for regular email
- Notify from/Notify through--Date/time for sending email
- Existing signature
- Signature contains—A particular string in the signature [12]

The parameters that security administrators can set for ESM events are:

- Email recipient—To whom security administrators are sending the notification
- Hostname—Monitored Host
- Group
- Service—Monitored Service
- Notify of REDS until resolved—Option for continual RED alerts
- Notify of YELLOWS until resolved—Option for continual YELLOW alerts
- Notify from/Notify through--Date/time for sending email
- Email detail level--Low for mobile phones and pagers; high for regular email
- Maximum alert frequency—Specify the maximum frequency of continual alerts
- Notify After Minutes Unresolved [12]

The parameters that security administrators can set for SIV instances and General alerts are:

- Email recipient—To whom security administrators are sending the notification
- Sensor—Monitored Auxiliary Sensor
- Alert level
- Email detail level--Low for mobile phones and pagers; high for regular email
- Notify from/Notify through—Date/time for sending email[12]

Configuring Console Users

PureSecure™ has the ability to create and maintain a database of users that have access to the information on the Console. PureSecure™ has six levels of user access. They are:

- Super User—has unlimited administrative power in the Console. This is the only user class that can add/delete/modify users
- NIDS Admin—has the ability to administer the NIDS portion of the Console
- ESM Admin—has the ability to administer the ESM portion of the Console
- SIV Admin—has the ability to administer the SIV portion of the Console
- Regular User—has Read-Only access but may enter new "Alert Rules" to receive notification of certain events
- Anonymous User—has Read-Only access. This user's access may be disallowed. [12]

PureSecure™ GUI

The PureSecure™ GUI is a useful tool employed by security administrators to determine how to identify an intrusion, investigate the intrusion, and decide quickly how to handle the intrusion.

Security administrators can access PureSecure™ by pointing a web browser to ***http://localhost/Demarc/PureSecure***. After the user logs in, the web server will display the "Summary Screen." A typical summary screen is found in **Figure 1.**

The PureSecure™ GUI consists of six main screens that correspond to the major functional areas of the product. They are: summary, events (NIDS), monitor (ESM), integrity (SIV), search, and configure.

The summary screen is quite comprehensive and the labels are self-explanatory, if security administrators are familiar with the application. On the other hand, it displays quite a bit of information, arguably too much. The screen looks cluttered and the users may have difficulty locating important information until they became familiar with it. Something should be done to make the screen more user-friendly. For example, there is a Quick Stats frame that could be a screen by itself.

The drill down capabilities of the summary screen are impressive. They allow the security administrators to access detailed data and additional functions concerning the entries. The added functionality includes:

- Determining the actual signature in the Snort rule set
- Performing a "whois", "traceroute", "ping", and/or DNS query on either the source or destination IP address
- Displaying graphs of the number of occurrences of unique network events over predetermined time periods
- Varying the amount of data displayed by interactively changing the time frame or the protocol

Evaluation of PureSecure™

PureSecure™ will now be evaluated against the primary IDS decisions mentioned above.

Control Costs

A PureSecure™ Console on either a *nix or Windows platform with unlimited auxiliary sensor coverage within the local segment is available for $2,350.[14] At this price, PureSecure™ offers a lot of value for the money. You can accomplish the same objectives at no cost with open source products, e.g.—SnortSnarf and ACID, but configuration, installation, and usability are at a significantly lower level than that offered by PureSecure™. You can also buy a more full-featured product, e.g.-NetRanger and RealSecure, but these products cost from $10,000 [15] to more than $20,000 [16] to protect a similar network. A large number of organizations will be able to afford a PureSecure™ solution that cannot afford the higher priced solutions.

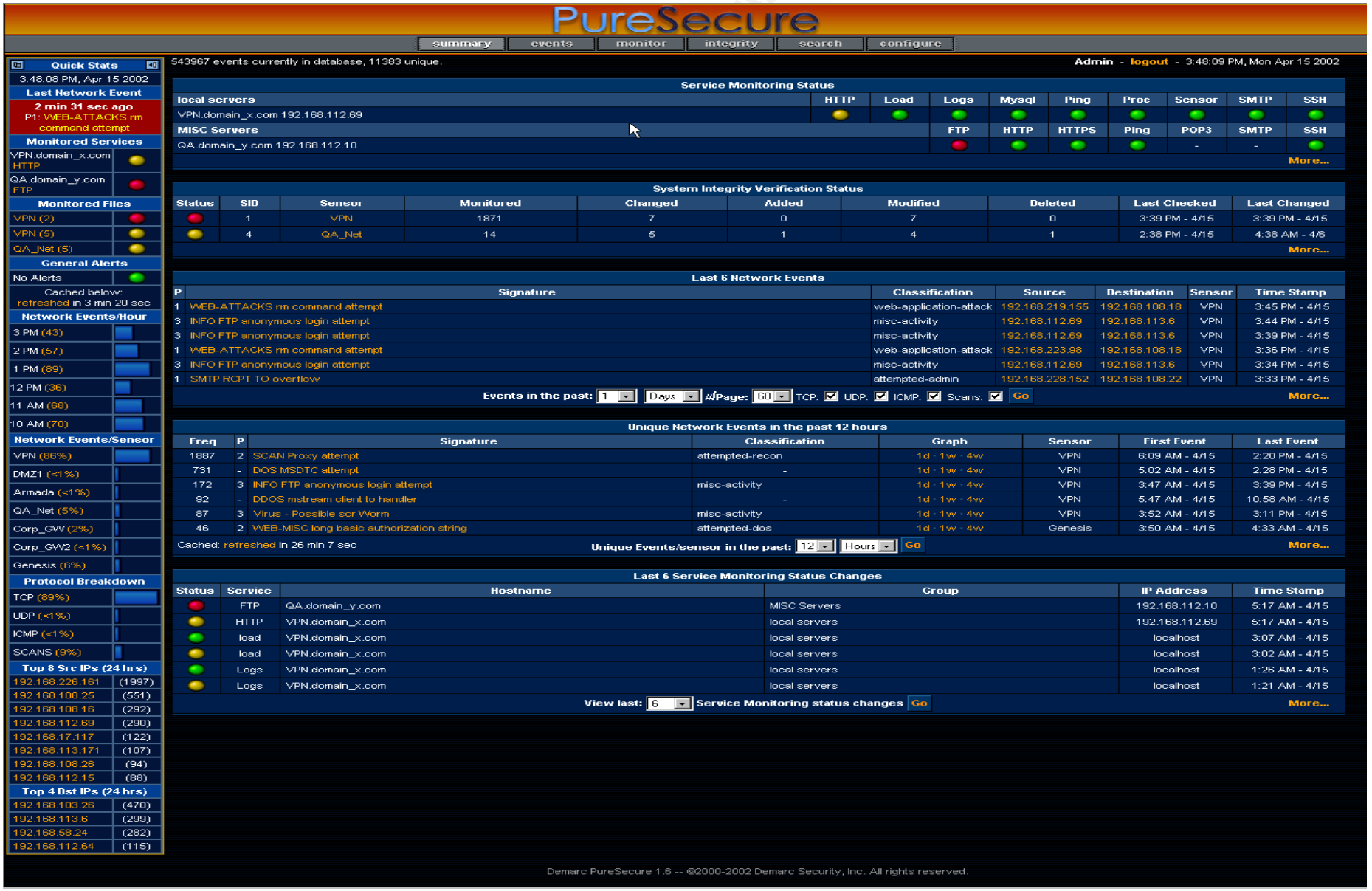

Figure 1 – PureSecure™ Summary Screen[13]

[13] **Demarc Security, Inc., PureSecure™ Summary Screen**

Control both false positives and false negatives

This is a trade-off. If the security administrators log too much, they will spend too much time deciding which attack to investigate and too little time fixing the vulnerability. If they log too little, a "real attack" will not be logged and they will not be aware of it until too late. This is a problem for all IDSs, including PureSecure™. What PureSecure™ does do, however, is make it easy to add, modify, and delete the NIDS rules and notification alerts.

Make certain that system performance remains at an acceptable level when the IDS is implemented

This is another trade-off. If security administrators give the system a lot to do, performance will suffer. If they place performance at too high a premium, something will get by the IDS. Although the writer has not done extensive research, he hasn't heard any complaints about PureSecure™ adversely affecting system performance. Demarc has built safeguards into the code to insure that PureSecure™ does not slow system performance. For example, when SIV is monitoring a large number of files the SIV process will fork to free up the auxiliary sensor to perform other checks.[12]

Display the data in a form that allows security administrators to make an appropriate decision quickly

As was mentioned previously, the PureSecure™ summary screen contains a great deal of data and this makes it difficult for someone unfamiliar with the system to quickly identify intrusions. On the other hand, PureSecure™ gives security administrators the ability to access low-level data when investigating potential intrusions. This is an important capability as it makes it easier for them to detect false positives.

Alert security administrators immediately when a critical attack occurs

PureSecure™ uses the Notification Alert feature to inform security administrators of a critical attack. This is easily configurable. The writer would prefer that PureSecure™ use a direct method to deliver its alerts to mobile phones and pagers rather than making it dependent on the email system.

Make certain the IDS is easy to install, configure, implement, and maintain

PureSecure™ is clearly easy to install. Configuration is accomplished relatively easily from the "configure" button of the GUI. Implementation and maintainability are trade-offs. The more security administrators expect the IDS to do, the more difficult it will be to implement and maintain. Allowing security administrators the option of automatic update of the Snort rule sets makes the maintenance task significantly easier.

Make certain the IDS provides complete, accurate, high-quality documentation

PureSecure™'s documentation needs a great deal of improvement. In particular, the User's Guide has no "Table of Contents" and there is no "Reference Guide." There are individual overviews for some of the features, but only for some of them, and there is no description that defines how the parts comprise the whole. Much of the documentation is focused on the "how-to" with little or no explanation of "why." In particular, if the security administrators don't have an understanding of Snort, they will not be able to configure PureSecure™ properly. There should be something in the documentation to tell the security administrators that they need to have a "working knowledge" of Snort and where to find the information if they don't. The writer has not used Demarc's support services enough to evaluate them.

Summary

An IDS is one of the primary tools required to provide network security. Before the security administrators evaluate an IDS, they have to make several decisions to determine its suitability for their particular network. Some of the more important decisions involve finding methods to:

- Control costs
- Control both false positives and false negatives
- Make certain that system performance remains at an acceptable level when the IDS is implemented
- Display the data in a form that allows security administrators to make an appropriate decision quickly
- Alert security administrators immediately when a critical attack occurs
- Make certain the IDS is easy to install, implement, configure, and maintain.
- Make certain the IDS provides complete, accurate, high-quality documentation

Demarc Security, Inc. markets a product called PureSecure™ that bundles network intrusion detection, extensible service monitoring, and system integrity verification into a single easy to use package. PureSecure™ uses Snort as its actual NIDS, stores the information in a MySQL database, and displays the data to security administrators in a GUI through a web browser, driven by either Apache or IIS. It works equally well on *nix or Windows platforms.

When Demarc bundled three products into one to create PureSecure™, they created an application that provides a comprehensive level of security that fits well with the defense in depth strategy. PureSecure™ is also quite affordable. This combination of capability and low cost make PureSecure™ an excellent choice to protect small to medium networks.

References

[1] S. Northcutt, SANS Security Essentials online course, Day 3, Section 3, "Host-based Intrusion Detection"; 14 May 2002.

[2] S. Northcutt, SANS Security Essentials online course, Day 3, Section 4, "Network-based Intrusion Detection"; 15 May 2002.

[3] G.A. Fink, B.L. Chappell, T.G. Turner, and K.F. O'Donoghue, "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems.", *Proceedings of the 16th International Parallel and Distributed Processing Symposium;* Apr 2002.
URL: http://www.nswc.navy.mil/ITT/documents/2002_ipdps_gf.html (26 Dec 2002)

[4] S. Northcutt, SANS Security Essentials online course, Day 3, Section 1, "An Overview of the Information Risk Management Framework"; 14 May 2002.

[5] Demarc Security, Inc., "Company Overview."; 2002.
URL: http://www.demarc.com/company (26 Dec 2002)

[6] Joe Barr, "How to install PureSecure, the painless IDS.", Linux World ; 30 Apr 2002.
URL: http://www.linuxworld.com/site-stories/2002/0430.puresecure.html (26 Dec 2002)

[7] Freshmeat.net, "Demarc PureSecure 1.6"; 22 Apr 2002.
URL: http://freshmeat.net/releases/81882/ (26 Dec 2002)

[8] Demarc Knowledge Base Response Kbresponder@demarc.com, "Demarc Security History (Control # PS2002121028963)," Private email message to Jeff Slonaker; 11 Dec 2002.

[9] Demarc Security, Inc., "Products – PureSecure Hardware." ; 2002.
URL: http://www.demarc.com/products/hardware/ (26 Dec 2002)

[10] Malcolm Graham, "Performance-based Documentation".
URL: www.writedoc.com/webdocs/perform.pdf (26 Dec 2002)

[11] Demarc Security, Inc., "Support – Knowledge Base (PS2002071716443),"; 17 Jul 2002.
URL: http://www.demarc.com/support/knowledgebase/answers/kb/PS2002071716443 (26 Dec 2002)

[12] Demarc Security, Inc., "PureSecure 1.6 User Guide v1.1,"; 2001-2002.
URL: http://www.demarc.com/support/documentation/ps1.6-userguide.pdf (26 Dec 2002)

[13] Demarc Security, Inc., PureSecure™ Summary Screen ; 2002.
URL: http://www.demarc.com/products/puresecure/screenshots/summary.html (26 Dec 2002)

[14] Demarc Security, Inc., PureSecure™ pricing information; 2002.
URL: http://www.demarc.com/products/puresecure/pricing.html (26 Dec 2002)

[15] SC Magazine, "June 2000 Test Center; Intrusion Detection; RealSecure 3.2,"; Jun 2000.
URL: http://www.scmagazine.com/scmagazine/2000_06/testc/prod2.html (26 Dec 2002)

[16] Network Computing, "Intrusion Detection, Take Two; Cisco Systems Cisco Secure Intrusion Detection System/NetRanger"; 15 Nov 1999.
URL: http://www.nwc.com/1023/1023f14.html (26 Dec 2002)

[17] Demarc Security, Inc., "Demarc PureSecure 1.6; Unix Installation Guide v1.1,"; 2002.
URL: http://www.demarc.com/support/documentation/ps1.6-unixinstall.txt (26 Dec 2002)

[18] Demarc Security, Inc., "Demarc PureSecure 1.6; Windows Installation Guide v1.1" ; 2002.
URL: http://www.demarc.com/support/documentation/ps1.6-win32install.txt (26 Dec 2002)

[19] Demarc Security, Inc., "Demarc PureSecure 1.6; ESM Plugin API Documentation v1.0"; 2002
URL: http://www.demarc.com/support/documentation/esm-plugins-api.txt (26 Dec 2002)

[20] S. Northcutt, SANS Security Essentials online course, Day 2, Section 1, "Threat and the Need for Defense in Depth"; 02 Jan 2002.