Global Information Assurance Certification Paper

PureSecure™

Complete Intrusion Detection

GIAC Security Essentials Certification (GSEC)
Practical Assignment V1.4b – Option 1

Jason C. Oseen

February 3, 2003

Abstract

For those responsible for network security, it is a well-known fact that configuration, maintenance, and monitoring of systems that are intended to detect and report misuse can be quite a burden from an administrative standpoint. This cost of these measures can become compounded quickly as the size of a network becomes larger.

This paper briefly describes the functions of typical Intrusion Detection Systems (IDS), and outlines some of the problems associated with the different methods that are commonly in use. The main objective in this text is to provide an impartial overview of a product that the author believes is both a more complete and convenient alternative to many other vendors' software.

The Problem

With the cost of technology becoming increasingly more affordable, the number of businesses and individuals purchasing computers and other network devices seems to be rising exponentially. This is also fueled by the growing acceptance of the Internet, and advertising campaigns that are dedicated to convincing people that they will be left behind if they don't adopt new "E-Standards" in their homes and workplaces. Interconnected devices are rapidly becoming more commonplace in people's lives, and as a result, the data processed by these systems is becoming increasingly more valuable (Metcalfe's Law[1]). The value of this data in turn, magnifies the impact on the parties that depend on it if the systems are ever compromised.

Hardware and software vendors are aware of this, and it seems that there is an almost endless list of products available on the market to assist people in protecting their data, such as firewalls, and Intrusion Detection Systems. Unfortunately, it is difficult to know which one(s) to implement. Many of these products are often complicated to configure and monitor, particularly in larger networks. Administration must commonly be performed on multiple machines and the volume of reporting is often staggering, making it impossible to thoroughly review all the reports and extract the information that may be pertinent. To assist those that are responsible for protecting networks, it would be beneficial to consolidate the monitoring of network security systems to a single, simple to use interface.

Intrusion Detection Systems Overview

When it comes to protecting your network, a firewall between the Internet and your valuable data is only a modest beginning. If you require a firewall in the first place, and are physically connected to another network through it, obviously, it is likely that you require access to network services *through it*. Web (HTTP) and email (SMTP) are only two examples of the many services that may be required in your environment. Quite often, the applications that enable users to employ these services are themselves prone to exploits that can result in compromised

systems. Another threat that is often overlooked is that of the users themselves, who are internal to your network. In most cases, it is unlikely that these users reside behind firewalls and filters, and as a result, have a significant amount of access to the many resources available within your environment. The internal threats can take the form of a user who is willfully trying to cause damage, or unknowingly though malware found in email attachments, floppy disks brought in from home, etc.

In order to reduce the likelihood of compromise on your network, it is desirable to have sensors that will detect any threats as they are occurring, and provide notification in real time. Intrusion Detection Systems are able to provide these sensors and currently there are two general types available. These are Host-based Intrusion Detection Systems (HIDS), and Network-based Intrusion Detection Systems (NIDS).

HIDS

Host-based Intrusion Detection Systems reside within the specific machine that you desire to monitor. They can be configured to detect anomalies on a local network port, within log files, or within the file system itself.

Most operating systems available already come equipped with basic logging abilities. As an example, which is by no means a conclusive list, Unix-type systems have standard programs installed by default, like Syslog, which provides logging of system events which can record such events as successful or failed authentication attempts. There's also TCP Wrappers, which detects and logs network connection attempts based on who the client is and the service that is requested. Windows NT through to Windows XP come with "Event Viewer" which can log file system accesses based on configurable auditing settings. Other Microsoft systems that can provide such logging are Routing and Remote Access, and various IIS services such as Web, FTP, and Mail.

HIDS can parse through these different types of logs, detecting predefined strings that may indicate the occurrence of both successful and unsuccessful attacks.

NIDS

Network-based Intrusion Detection Systems "sniff" data packets off the wire and attempt to match them up with known attack signatures, similar to HIDS. With NIDS, however, the network interface is configured so that "promiscuous mode" is enabled, which allows that interface to collect data that is not specifically addressed to itself. What this means is that any packet, destined for any other machine on that particular network segment, can be analyzed, assuming that the network is not switched.

Both of these types of Intrusion Detection Systems can log their results to a file and usually can produce some type of notification for the administrator, such as

an email, or a pager message. Often, the log files can be consolidated and stored remotely from the machine that initially collected the data. This provides two advantages: It makes it more difficult for the intruder to alter or destroy the logs, and it helps to save time and resources required to analyze the data.

Disadvantages of HIDS and NIDS

One of the primary disadvantages of HIDS is that in order to be effective, it must be installed and configured on each machine that you wish to monitor. It should be apparent that even with a minimum quantity of machines, the amount of work required could become rather excessive.

The main problem with NIDS is that it can quickly become overloaded in large networks. "The current limits for Network-based IDS boxes are about 80 MB/sec fully loaded. Once a sensor's bandwidth limit is exceeded, its performance tends to degrade rapidly."[2] Switched networks are also limiting, as with switches, the IDS box will only see the traffic that is specifically intended for that one machine.

With both types of intrusion detection, the logging on the machines must individually be configured to meet the needs of each specific environment. The IDS must be set up so it's sensitive enough to be effective, yet not too sensitive as to create excessively large logs that would be impossible to review in great detail. On heterogeneous networks, running both Windows machines and Unix machines for instance, it can be difficult to consolidate the logs for easy perusal.

One product that seems to be able to successfully balance a solution, integrating both HIDS and NIDS, as well as eliminating perceived boundaries between operating systems in a mixed network, is PureSecure™, an Intrusion Detection system, created by Demarc Security.[3]

PureSecure

PureSecure combines the functionality of both a HIDS and NIDS. Although still limited by some of the disadvantages listed above, it reduces administrative overhead by presenting all available features through a single, web-based, graphical user interface, which allows:

1.) collection of all pertinent data in one database
2.) independent configuration of each sensor
3.) viewing of network events at a glance
3.) the ability to easily remove data that is outdated or irrelevant while retaining the information that may still be useful

This package is capable of running on a wide variety of operating systems including: Unix, Linux, Solaris, OpenBSD, FreeBSD, NetBSD, HP-UX and Windows 95/NT/2000/XP. The NIDS functionality is provided by Snort, which in itself is a "complete open source network intrusion detection system."[4] Snort is free of charge and is based on a program called 'libpcap'[5], that allows user-level

packet capture. WinPcap,[6] a version of libpcap that was ported to the Win32 architecture, allows packet capture on Microsoft platforms.

Snort offers the flexibility of many different options for output, including screen, file, syslog, and even pop-up windows. PureSecure however depends on Snort's ability to send its alerts to a MySQL[7] database (also open source and free of charge under the GNU General Public License[8]).

Network traffic is compared against easily configurable Snort rule sets. Data that matches the rules is stored in the database. The remaining information is ignored, preventing unnecessary data storage and allowing the capturing of packets to remain as efficient as possible. Snort rules for each sensor can be configured through the single, graphical, front-end in PureSecure. If desired, updated rule sets can be downloaded from Demarc's website either automatically or manually. This feature is also front-end configurable.

Host-based intrusion detection is performed through what Demarc calls the "Extensible Service Monitor", or ESM and the "System Integrity Verification" or SIV. These are two very powerful features that can let an administrator easily view and assess the overall health of network devices.

The ESM is responsible for the monitoring of Unix logs; Windows Event Logs; monitoring of standard services, such as ftp, telnet, and http; and monitoring of running processes, like Syslogd in Unix, or Print Spooler in Windows. It can periodically send ICMP requests (ping) to ensure continued connectivity. The ESM is able to monitor load on Unix-based systems or processor utilization on Windows, and can be set up to report when remaining hard drive space becomes scarce. The ESM also allows for plugins that enhance the overall functionality of the product, and Demarc provides information to assist users in creating their own plugins that are customized to their needs.

The SIV is responsible for providing file integrity checks that determine if a specific file or hierarchy has been tampered with or even if a web page on a remote system is changed.

With all its abilities, the versatility of PureSecure should be apparent. It is easy to see why Demarc Security touts their product as a one of a kind "Total Intrusion Detection System", combining HIDS, and NIDS as well as a plethora of other features.

Licensing

Prior to going into more detail, the licensing terms of the product should be summarized at this point. Demarc states that non-commercial/not for profit entities may install and use the Personal Edition[9] of the product free of charge. Commercial or for profit entities may install and use the Professional Version[10] of the product for a period of 30 days free of charge, after which they must

purchase the Professional version. More detail is provided on their website and the URLs of each of the licensing agreements are provided in the References section of this paper.

The testing environment used to facilitate the creation of this document is based on a home network consisting of three Pentium 120 MHz systems, two running Windows 2000 Professional, one running Redhat Linux 7.2; one Pentium II 350 MHz running Windows 2000 Professional; and one IBM RS6000 PowerStation 220 running AIX 3.2. One Linux and one Windows station have PureSecure installed. Neither the test network, nor this research is generating revenue.

Installation

The installation of PureSecure is fairly straightforward, but some consideration must be given to the locations that the sensors and the database are installed. These will be unique to the requirements of each environment, so planning ahead to determine what your goals are is essential. It is easy to start with a single machine hosting the first sensor, the database, and the console, then expanding the number of sensors as you begin to understand the capabilities and limitations of the sensors.

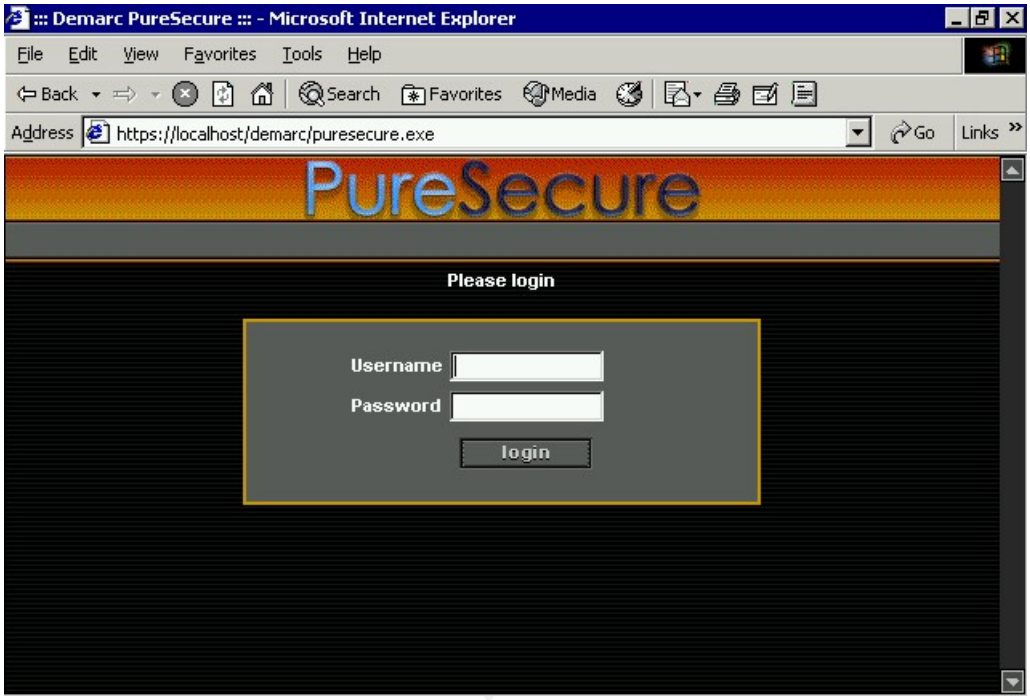
You can find the installation instructions for your preferred platform on Demarc's website, along with the binary or source code. These instructions are step-by-step and easy to understand so they will not be repeated here. The interactive installation script prompts you as it automatically downloads and configures additional pieces of software that you may require, such as Snort, MySQL, libpcap and others. Depending on the speed of the system that PureSecure is being installed on, the total time required for setup should easily be within half an hour.

After the setup, you should immediately be able to open your browser and point it to "*https://my_host/demarc/puresecure.exe*", where "my_host" is the hostname of the machine that you just completed the installation on. Note that in the URL above, the protocol is *https.* Although the installation instructions don't specifically mention this configuration, I would recommend using the Secure Socket Layer (SSL) if possible on the web server to ensure that the data transmitted is encrypted. The reason for this is that when alerts are triggered and the console is updated from the web server, the sensors may pick up the clear text sent from the server to the browser and mistakenly interpret it *again* as a potential intrusion (Demarc actually does present this information deeper in a configuration text file called 'puresecure_config.pm' that can be found on both Windows and Unix based systems.)

After the URL is launched in your browser, you should see the login screen as shown in Figure 1. This is where you enter the PureSecure username "admin" and the password that you specified during the installation process. After a

successful login, you are given another opportunity to review the license agreement, before you are redirected to the Summary screen.

Figure 1. – Login Screen



Configuration

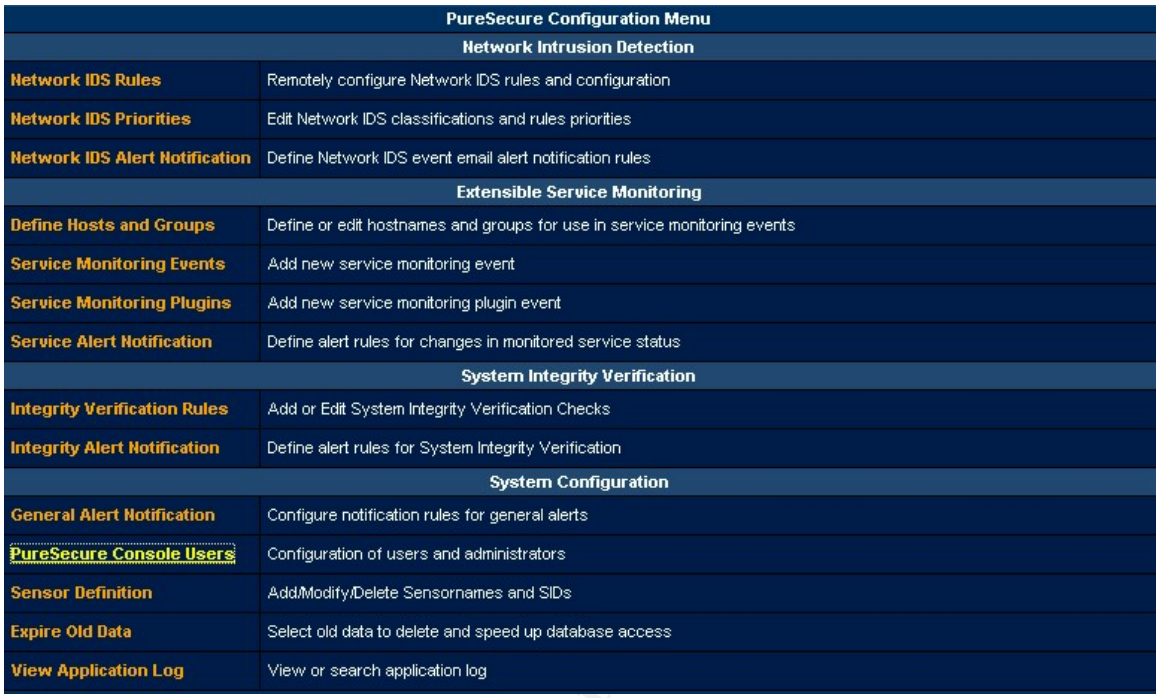
This section will provide an overview of the initial setup and functionality of PureSecure. For detailed information and configuration guidelines, please refer to the PureSecure User Guide.[11]

The Summary screen, with which you are first presented following the login, is where the administrator is able to check all configured sensors at a glance and determine if any alerting events have occurred. The status of network services, system integrity, and suspicious network traffic is presented here, along with brief details regarding the event. Each section also provides hyperlinks to view the events in greater detail.

At this point, if you have not gotten curious and jumped ahead, your Summary console should be fairly void of any useful information. You must set up the criteria you wish to monitor, and this is done via the Configuration screen, which is accessed by pressing the button of the same name along the top row of the screen, beneath the title.

On the Configuration menu are several sections: Network Intrusion Detection, Extensible Service Monitoring, System Integrity Verification, and System Configuration. There are also subcategories below each of these, as shown in Figure 2.

Figure 2. – Configuration Menu



PureSecure Configuration Menu	
Network Intrusion Detection	
Network IDS Rules	Remotely configure Network IDS rules and configuration
Network IDS Priorities	Edit Network IDS classifications and rules priorities
Network IDS Alert Notification	Define Network IDS event email alert notification rules
Extensible Service Monitoring	
Define Hosts and Groups	Define or edit hostnames and groups for use in service monitoring events
Service Monitoring Events	Add new service monitoring event
Service Monitoring Plugins	Add new service monitoring plugin event
Service Alert Notification	Define alert rules for changes in monitored service status
System Integrity Verification	
Integrity Verification Rules	Add or Edit System Integrity Verification Checks
Integrity Alert Notification	Define alert rules for System Integrity Verification
System Configuration	
General Alert Notification	Configure notification rules for general alerts
PureSecure Console Users	Configuration of users and administrators
Sensor Definition	Add/Modify/Delete Sensornames and SIDs
Expire Old Data	Select old data to delete and speed up database access
View Application Log	View or search application log

The first item that should be introduced here is under the System Configuration Heading and is titled "PureSecure Console Users". The features available here are particularly important if the primary security administrator has subordinate staff members that share the responsibility for monitoring the security of the network. It is possible to provide each desired user with a personal username and password to log in to the console. Each login can also be customized with different levels of ability depending on what the user should be permitted to configure. For example, the user can be set up with rights to administer any combination of the NIDS, ESM, or SIV consoles, or have superuser rights to the entire package. Similarly, here it is possible to restrict the IP addresses of machines on the network, which can provide the ability to log on to the console.

The Configuration menu option entitled "View Application Log" provides a listing of all operator changes that have been made to the PureSecure database. This is a detailed log that includes the name of the operator, the action performed, the target sensor (if applicable), the time and date of the change, as well as the IP address from which the user executed the modification. Filtering for specific administrative events, such as changes to the sensors, or deletion of alerts is a simple task.

The "Expire Old Data" option provides the ability to select data to delete based on the date that it was collected. This screen also provides a cumulative count, by date, of how many database records would be purged at a specific point in time.

Under "Sensor Definition", one is able to manually add or edit the sensors available on the network. From my personal experience, it is not recommended that one experiment too much in here until they are completely comfortable with the way that PureSecure operates in its entirety. For example, if you're not one hundred percent sure how to tell that your network interface name is similar to:

"DeviceNPF_{2671E9AC-4FFF-453F-BD57-9E4C75DBC72C}",

then you may want to leave well enough alone unless you have some spare time available!

The link entitled "General Alert Notification" allows the specification of an email address to send alerts to, based on the urgency of the alert, the sensor sending the alert, the amount of detail preferred in the alert, and the work shift that the person monitoring the network is available. A sample NIDS notification email configured with a high level of detail is below, in Figure 3. Alerts may also be suspended here temporarily, while you investigate a situation that may be occurring. A mailbox full of the same notification can quickly become a nuisance.

Figure 3. – NIDS Email Notification

From: snort@mydomain.com
Subject: NIDS ALERT - 1 in past 5 mins - Demarc PureSecure 1.6

```
-----------------------------------------
Total Alerts: 1
Highest Alert Priority: 1
-----------------------------------------
Network Intrusion Detection Events
-----------------------------------------
NIDS Alert at: 2003-01-26 18:08:01
Signature: TFTP GET passwd
Priority: 1
Class Name: successful-admin
Class Desc: Successful Administrator Privilege Gain
Sensor: dc1
SID: 1
Event ID: 1448
Src IP: 192.168.200.34
Src Host: ws1.mydomain.com
Dst IP: 192.168.200.10
Dst Host: dc2.mydomain.com
-----------------------------------------
00 01 2E 2E 2F 65 74 63 2F 70 61 73 73 77 64 00   ..../etc/passwd.
6F 63 74 65 74 00                                 octet.

-----------------------------------------
```

Network Intrusion Detection

Now that we have the basic system configuration set up, we can move on to configuring the individual sensors to meet our requirements. In the "Network Intrusion Detection" section of the Configuration console, we begin by setting up the Network IDS rules. Clicking on this link brings up the details of each sensor that is currently set up on the network. Once again, if you have followed this paper methodically, you probably have just your main sensor available on this screen. From here you should be able to see which interface the sensor is running on, when the rules were last changed, when the program was last restarted to incorporate the rule updates, and whether the service is currently utilizing the latest updates. The name of each sensor here is a hyperlink, which if clicked, will bring you to the rulesets for that particular sensor as shown in Figure 4.

Figure 4. – Sensor Details

Sensor Details					
SID	Sensor	Interface	Ruleset Last Updated	Ruleset Last Implemented	In-Sync
1	dc1	DeviceNPF_{2671E9AC-4FFF-453F-BD57-9E4C75DBC72C}	11:53 PM - 1/27	11:53 PM - 1/27 (3.82 minutes ago)	YES

Sensor Rulesets		
Select Sensor to Edit	1 - dc1	Go
Edit Snort Configuration File	Edit "snort.conf" for this sensor	Go
Edit Class/Priorities	Edit global classification and priority definitions	Go
Add Ruleset for Current Sensor		Go
Modify Ruleset on Current Sensor	-Select-	Go
Delete Ruleset on Current Sensor	-Select-	Go
Validate Rulesets for Current Sensor	Validate configuration and rulesets	Go
Update Rulesets for Current Sensor	Update rulesets from demarc.com	Go

"Select Sensor to Edit" allows you to switch between the sensor that is currently selected for editing, and all other configured sensors on the network. The "Go" buttons on this screen are actually what invokes your choice.

The Snort Configuration File is where the heart of the NIDS lies. Demarc has provided an almost foolproof configuration file that should suffice in getting started, with immediate monitoring capabilities as well as a template to begin molding it to each individual environment. The snort.conf file itself is fairly well commented, and should be enough to get most installations operational, but the documentation provided in the PureSecure User Guide[11] provides a bit more detail with examples for those who may wish to begin writing or modifying their own rules. As Snort is a very comprehensive product, one may ultimately wish to research the Snort website and peruse the available resources there.

Snort rules can be grouped by type of attack using named "Classtypes". Each classtype is assigned a numerical priority that can be used to determine the severity of the problem. Notifications can be configured based on these event

priorities. Under the "Edit Class Priorities" link, classtypes and priorities can be added, modified, or deleted.

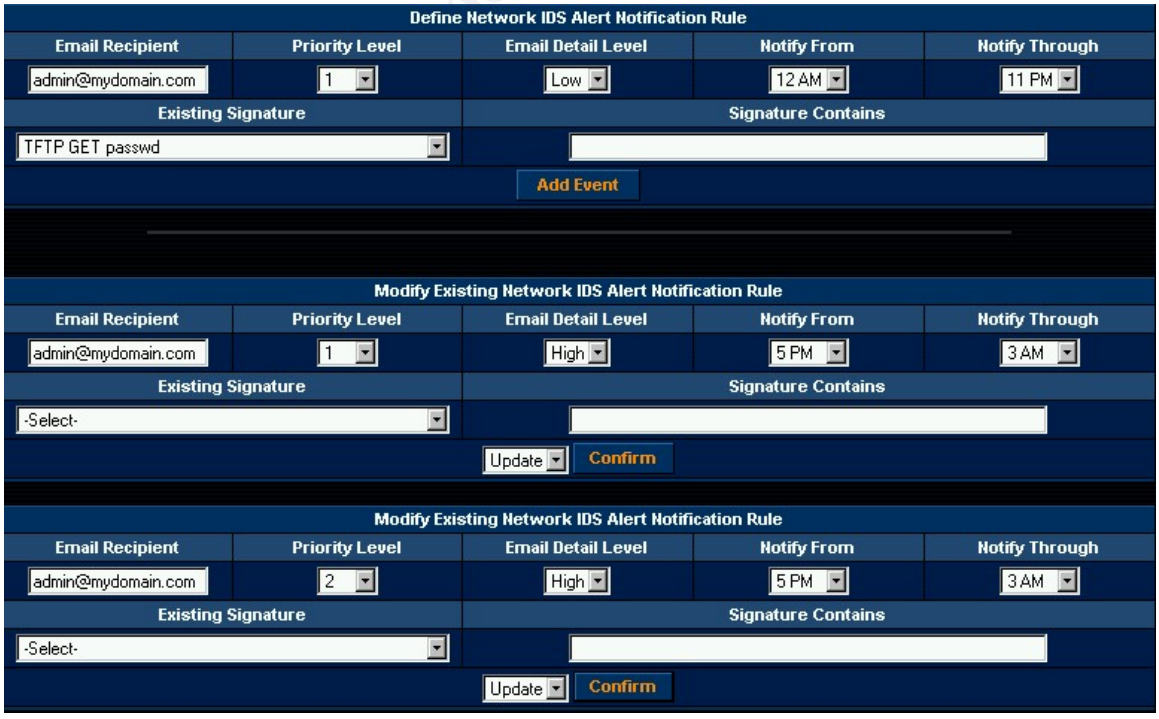
"Add Ruleset for Current Sensor" allows you to add new rules by either creating a ruleset from scratch, or providing the name of a ruleset that already exists in your Rules folder or directory. "Modify Ruleset on Current Sensor" provides an easy to use textbox for manually modifying rules, and "Delete Ruleset on Current Sensor" removes the ruleset only from the Snort configuration leaving the actual rules file in the local rules folder.

The "Validate Rulesets for Current Sensor" link ensures that there are no syntax errors in either the Snort configuration file or the rulesets. The PureSecure service must then be restarted for the changes to take effect. The "Update Rulesets for Current Sensor" checks the Demarc website for updated rulesets.

Back on the PureSecure configuration menu, the next choice is "Network IDS Priorities". This is the same screen as "Edit Class Priorities", mentioned above.

The "Network IDS Alert Notification" screen, shown in Figure 5, allows the specification of criteria that would trigger an email notification. In this example, there are two existing rules. The only difference between these two is the Priority Level. The top part of the illustration shows the creation of a new notification. It is based on a Snort rule with "TFTP GET passwd" as the signature.

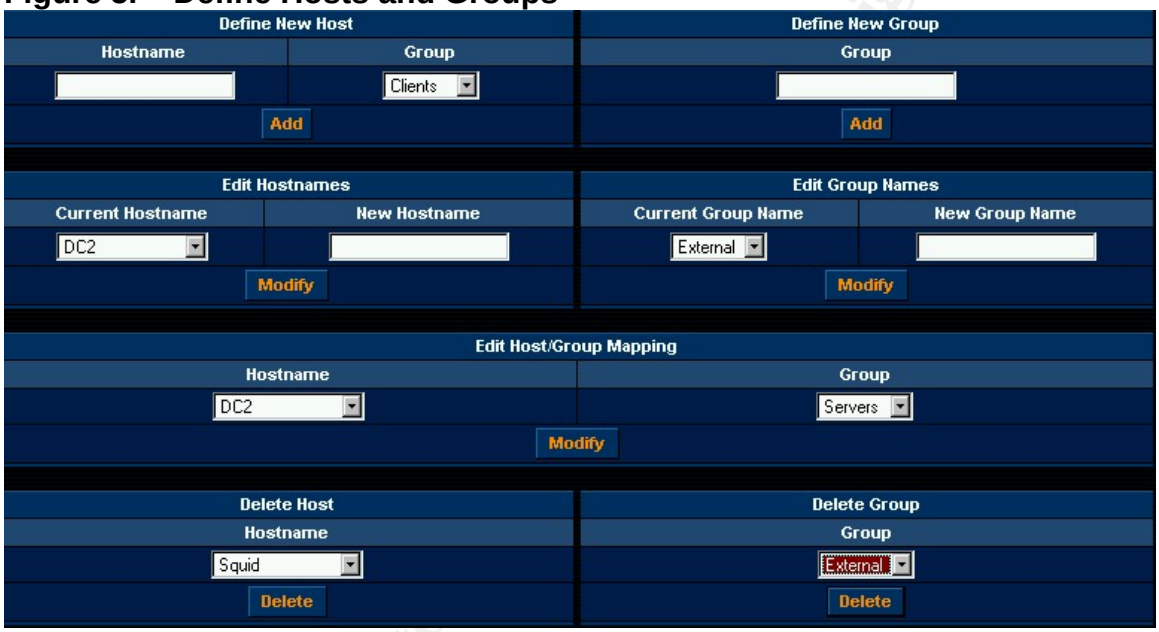
Figure 5. – Network IDS Alert Notification



Extensible Service Monitoring

To use the ESM features, each host you wish to monitor must be added under "Define Hosts and Groups", on the configuration menu. In addition, a minimum of one group must be created prior to adding any hosts to the ESM. Groups are used for organizational purposes and can make the console easier to interpret visually. An example of the use of groups could be the consolidation of machines that perform a similar function, such as File Servers, or Database Servers. As shown in Figure 5, hosts and groups names can be changed or deleted, and the mapping between the two can also be changed.

Figure 5. – Define Hosts and Groups



The "Service Monitoring Events" screen, shown in figure 6, allows for the configuration of services, host by host. There are many services available in the "Service" list box, including DNS, FTP, and HTTP, to mention only a few. When the service is chosen, the description text box automatically populates with information relating to that service and can be manually changed if desired.

Figure 6. – Define New Service Monitoring Event

For network-based services, the "Sensor to Perform Check" list box should typically be the closest sensor to the monitored host to help reduce network traffic. On local-based services such as "disk" and "load", the sensor must be located on the machine that is being monitored. The "Port" text box enables you

to manually specify the port that the service is running on. For example, if you wanted to monitor the default MySQL network port to ensure that it was still accepting connections, then from the "Service" list, you could choose a generic service called TCP1 and assign it port 3306.

The "DNS Check" box allows you to specify if you would like PureSecure to send an alert if the DNS entries for a particular host change. If the service has configurable options, such as username and password, or timeout values, they may be entered into the "Advanced Options" text box. For more information on the options, there is a 'help' link beside the box that will pop up a separate window that contains examples of options for the different services.

On the main Configuration screen again, the "Service Monitoring Plugins" link allows you to set up add on modules if they are available. On the "Service Alert Notification" screen, shown in Figure 7, ESM alerts can be sent to different recipients based on the hostname, group, or service in the alert, as well as the level of that alert and the time frame that the recipient may be able to respond to the alert.

Figure 7. – Service Alert Notification

Figure 8 shows an example of a notification warning of low disk space on a host.

Figure 8. – ESM Email Notification

From: snort@mydomain.com
Subject: WARNING - disks - DC1 - Demarc PureSecure 1.6

```
----------------------------------------
Service Status Change Alert
----------------------------------------
Host: DC1
Service: disks
New Status: WARNING
Group: Servers
Duration: 34 dy  3 hr 6 min 23 sec
IP Address: 192.168.200.5
Old Status: Maintenance
Timestamp: 2003-02-01 14:19:08
----------------------------------------
Sat Feb  1 14:19:08 2003
Disk Space at warning level
```

```
Drive C is 93 % full - 9311924 / 9992396 KB used (680472 KB free)

-----------------------------------------------
Monitoring all non-removable disk drives:
-----------------------------------------------
Critical Percent set at 95 %
Warning Percent set at 85 %

-----------------------------------------
```

System Integrity Verification

The main Configuration screen provides access to the "Integrity Verification Rules", and "Integrity Notification" setup screens. The rules are defined by:

- alert level
- path to the file or directory
- if the monitoring will be recursive from the specified path
- description to be displayed on the console with the alert

A semicolon separates each section of the rule. A sample Windows rule follows in the order corresponding to the description just given.

RED;c:/autoexec.bat;0;System Configuration Changed!

The integrity notification is set up in a similar way to the ESM notification and the previously mentioned rule produces a resulting message similar to Figure 9, below, when the file is different from what PureSecure expects.

Figure 9 – SIV Email Notification.

From: snort@mydomain.com
Subject: SIV ALERT - 1 Alerts - Demarc PureSecure 1.6

```
----------------------------------------
1 Total Alerts
----------------------------------------
1 Critical Alerts
 - 1 Files Modified
----------------------------------------
MODIFIED FILE: c:/autoexec.bat
----------------------------------------
Priority: Critical   Sensor: dc1
File Last Changed: 2003-02-01 15:11:17
-------------[ SIZE ]--------------------
Expected: 0
Observed: 8
-------------[ MTIME ]-------------------
Expected: Sat Jun  1 00:59:50 2002
Observed: Sat Feb  1 15:11:00 2003
-------------[ MD5 HASH ]----------------
```

```
Expected: d41d8cd98f00b204e9800998ecf8427e
Observed: 2ee4cd2d8df1c4eee97ca95a85318c47

----------------------------------------
----------------------------------------
```

Monitoring

Now that some hosts and monitoring criteria have been set up, the Summary console should begin to populate with information. It displays the most recent activity in each of the NIDS, ESM, and SIV categories as shown below, in Figure 10.

Figure 10. – Summary Console

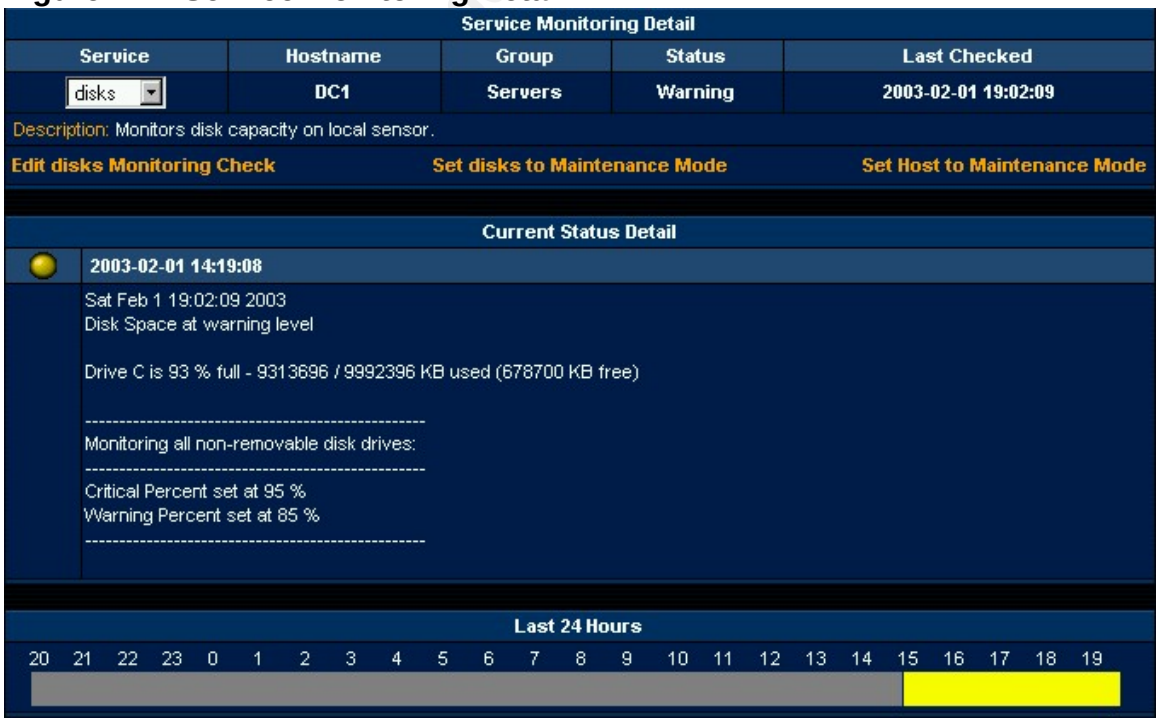
By default, on the left-hand side of the console is a "Quick Stats" bar that is present on every screen within the PureSecure console. Optionally, this bar can be launched in a separate window or closed completely to provide more room for the main part of the console. The Quick Stats bar displays the Last NIDS event, monitored services that are currently in alarm, monitored files that have not been acknowledged, and whether any General Alert conditions exist. Below the alerts are graphs that represent the amount of traffic that has been collected within the last six hours, by the hour. Following this is, the quantity of events that have

been collected by each sensor, percentage wise. Further down on the bar are sections for Protocol Breakdown, "Top 8 Source IPs" and the "Top 4 Destination IPs", for the last 24-hour period. Both the Summary console and the Quick stats bar can be configured manually to define what is displayed by editing the puresecure_config.pm file.
Service Monitoring Events are displayed with colored circles representing the status of each monitored service. Green means no alert is present, yellow is a warning, and red represents a critical condition. There is also a gray circle, which means the sensor is in "Maintenance Mode" and it will not test that particular sensor until it is put back into service. A blue icon means that the sensor that is supposed to be reporting the service has not responded in over ten minutes.

Figure 11 – Monitoring Totals

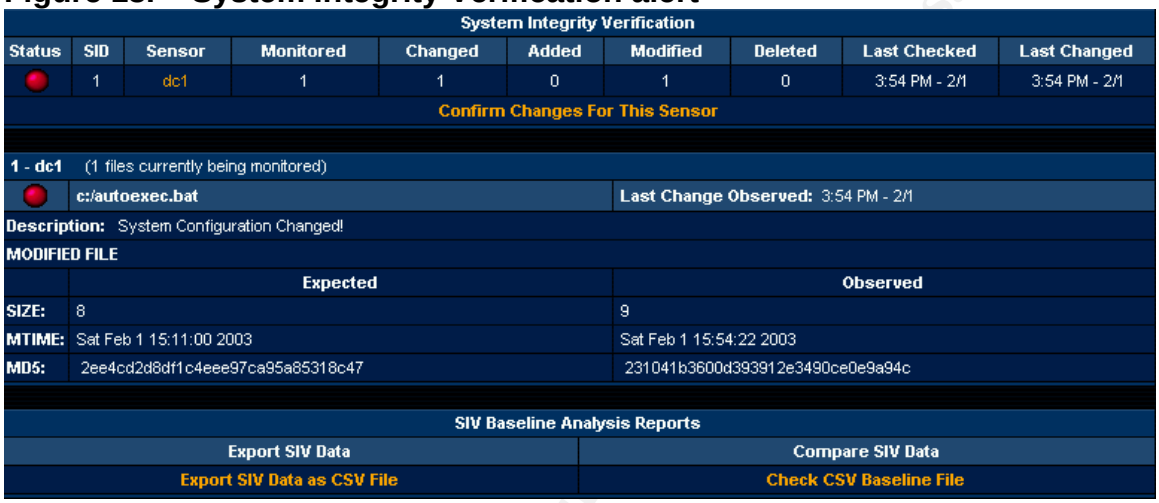
A large part of what is displayed in the console has hyperlinks that enable you to view more detail on each topic. It is simple to maneuver between event overview, detail, and configuration screens. For example, in Figure 10, if we were to click on the yellow icon in the service monitoring section, under the heading "Disks", we would be presented with the screen shown here, in Figure 12.

Figure 12 – Service Monitoring Detail



This screen allows for a detailed view of the alert as well as easy access to edit the properties of the sensor and host. The System Integrity Verification alert, shown by a red alert on the summary page, links to the screen shown in Figure 13. This screen allows the user to acknowledge the presence of the alert, and hence "silence" the alarm state. From here a detailed account of the event can be viewed and if desired, exported to a text-based CSV (Comma Separated Value) file or compared against a previously generated baseline file.

Figure 13. – System Integrity Verification alert



System Integrity Verification

Status	SID	Sensor	Monitored	Changed	Added	Modified	Deleted	Last Checked	Last Changed
	1	dc1	1	1	0	1	0	3:54 PM - 2/1	3:54 PM - 2/1

Confirm Changes For This Sensor

1 - dc1 (1 files currently being monitored)

c:/autoexec.bat **Last Change Observed:** 3:54 PM - 2/1

Description: System Configuration Changed!

MODIFIED FILE

	Expected	Observed
SIZE:	8	9
MTIME:	Sat Feb 1 15:11:00 2003	Sat Feb 1 15:54:22 2003
MD5:	2ee4cd2d8df1c4eee97ca95a85318c47	231041b3600d393912e3490ce0e9a94c

SIV Baseline Analysis Reports

Export SIV Data	Compare SIV Data
Export SIV Data as CSV File	Check CSV Baseline File

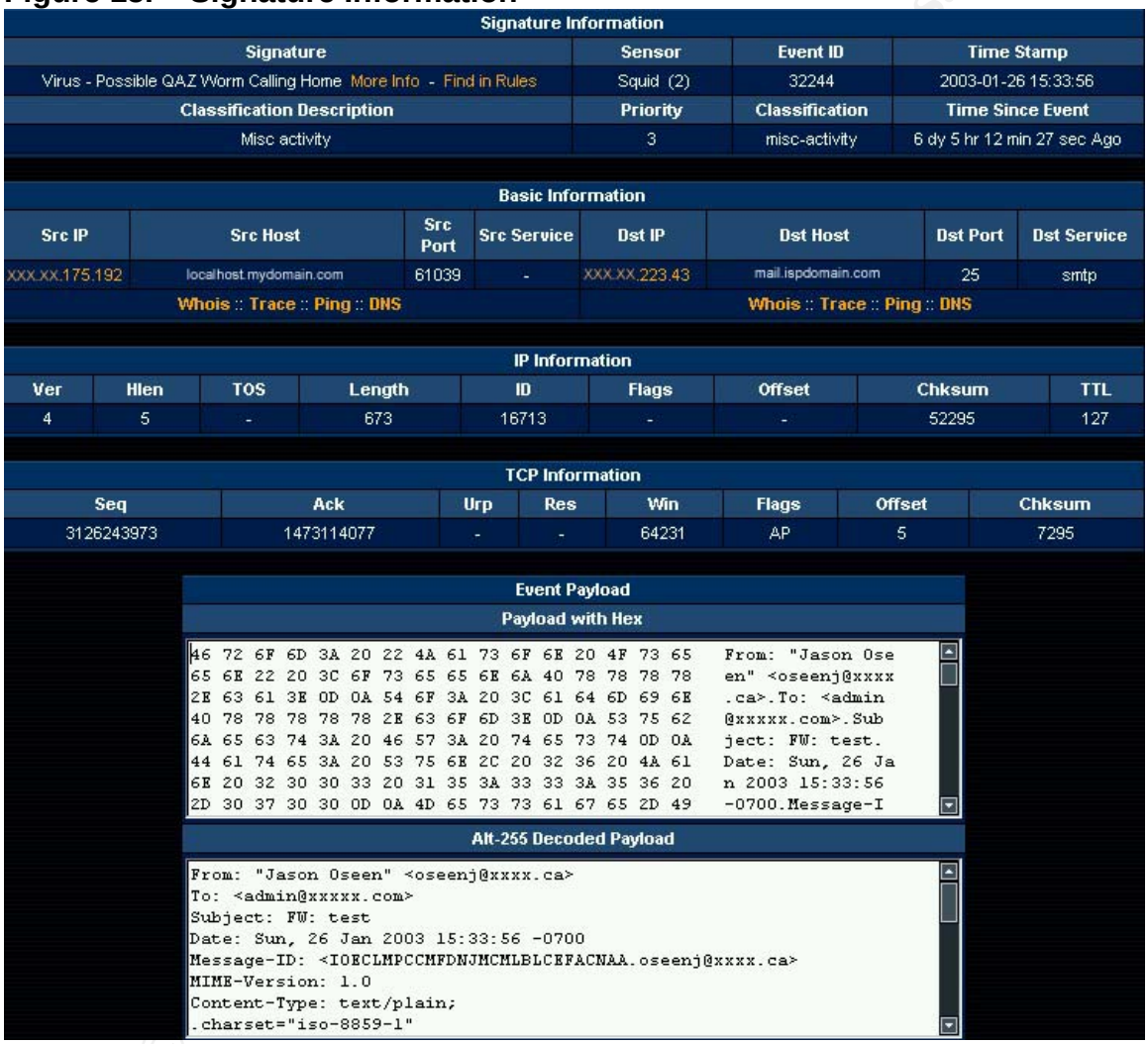
Figure 14. – Event List

Event List

P	Signature	Classification	Type	Source	Destination	Sensor	Time Stamp »
-	spp: possible EVASIVE RST detection	-	TCP	xxx.xx .26.81:80	xxx.xx .175.192:3977	Squid	5:52 AM - 2/1
-	spp: possible EVASIVE RST detection	-	TCP	xxx.x .223.43:110	192.168.200.34:2615	Squid	1:29 PM - 1/31
3	Virus - Possible scr Worm	misc-activity	TCP	xxx.x .223.43:110	192.168.200.34:4501	Squid	10:35 AM - 1/29
3	Virus - Possible scr Worm	misc-activity	TCP	xxx.x .223.43:110	192.168.200.34:4501	dc1	10:35 AM - 1/29
-	spp: possible EVASIVE RST detection	-	TCP	xxx.xxx.193.51:80	xxx.xx.175.192:2167	Squid	7:15 PM - 1/27
-	spp: TTL EVASION (reassemble) detection	-	TCP	xxx.xxx.193.51:80	xxx.xx.175.192:2167	Squid	7:15 PM - 1/27
-	spp: Multiple Acked Packets (possible fragroute)	-	TCP	xxx.xx.175.192:4710	xxx.xx.203.38:80	Squid	6:56 PM - 1/26
1	TFTP GET passwd	successful-admin	UDP	192.168.200.34:33591	192.168.200.10:69	dc1	6:08 PM - 1/26
1	TFTP GET passwd	successful-admin	UDP	192.168.200.34:33588	192.168.200.10:69	dc1	6:08 PM - 1/26
-	spp: STEALTH ACTIVITY (Vecna scan) detection	-	TCP	192.168.200.34:12030	192.168.200.10	dc1	6:03 PM - 1/26
-	spp: STEALTH ACTIVITY (SYN FIN scan) detection	-	TCP	192.168.200.34:12029	192.168.200.10	dc1	6:03 PM - 1/26
-	spp: STEALTH ACTIVITY (FIN scan) detection	-	TCP	192.168.200.34:12027	192.168.200.10	dc1	6:03 PM - 1/26
2	ATTACK RESPONSES 403 Forbidden	attempted-recon	TCP	192.168.200.10:80	192.168.200.5:1499	dc1	5:41 PM - 1/26
2	ATTACK RESPONSES 403 Forbidden	attempted-recon	TCP	192.168.200.10:80	192.168.200.5:1481	dc1	5:39 PM - 1/26
-	spp: NMAP FINGERPRINT (stateful) detection	-	TCP	192.168.200.1:43735	192.168.200.5:25	dc1	5:35 PM - 1/26
2	SCAN nmap TCP	attempted-recon	TCP	192.168.200.1:43737	192.168.200.5:1	dc1	5:35 PM - 1/26
-	spp: STEALTH ACTIVITY (nmap XMAS scan) detection	-	TCP	192.168.200.1:43738	192.168.200.5:1	dc1	5:35 PM - 1/26
-	spp: NMAP FINGERPRINT (stateful) detection	-	TCP	192.168.200.1:43735	192.168.200.5:25	dc1	5:35 PM - 1/26
2	SCAN nmap TCP	attempted-recon	TCP	192.168.200.1:43737	192.168.200.5:1	dc1	5:35 PM - 1/26
-	spp: STEALTH ACTIVITY (nmap XMAS scan) detection	-	TCP	192.168.200.1:43738	192.168.200.5:1	dc1	5:35 PM - 1/26
2	SCAN Proxy (8080) attempt	attempted-recon	TCP	192.168.200.1:2580	192.168.200.5:8080	dc1	5:35 PM - 1/26
2	SCAN Squid Proxy attempt	attempted-recon	TCP	192.168.200.1:4998	192.168.200.5:3128	dc1	5:34 PM - 1/26
2	ATTACK RESPONSES 403 Forbidden	attempted-recon	TCP	192.168.200.10:80	192.168.200.5:1411	dc1	5:34 PM - 1/26
3	Virus - Possible MyRomeo Worm	misc-activity	TCP	xxx.x .223.43:110	192.168.200.5:1959	Squid	4:16 PM - 1/26
-	spp: possible EVASIVE RST detection	-	TCP	xxx.x .24.140:5190	192.168.200.34:1508	Squid	3:46 PM - 1/26

In the Events screen, accessed from the main menu under the PureSecure title bar, one can view the NIDS alerts as illustrated in Figure 14. Here, all the entries under Signature, Source, and Destination are all links to other screens. Clicking on a source link with a specific IP address results in a list of all collected events where the source IP matches. Likewise with the Destination links. The items in the Signature column, however, link to the "Signature Information" screen shown in Figure 15.

Figure 15. – Signature Information



Signature Information

Signature	Sensor	Event ID	Time Stamp
Virus - Possible QAZ Worm Calling Home More Info - Find in Rules	Squid (2)	32244	2003-01-26 15:33:56
Classification Description	**Priority**	**Classification**	**Time Since Event**
Misc activity	3	misc-activity	6 dy 5 hr 12 min 27 sec Ago

Basic Information

Src IP	Src Host	Src Port	Src Service	Dst IP	Dst Host	Dst Port	Dst Service
XXX.XX.175.192	localhost.mydomain.com	61039	-	XXX.XX.223.43	mail.ispdomain.com	25	smtp
Whois :: Trace :: Ping :: DNS				Whois :: Trace :: Ping :: DNS			

IP Information

Ver	Hlen	TOS	Length	ID	Flags	Offset	Chksum	TTL
4	5	-	673	16713	-	-	52295	127

TCP Information

Seq	Ack	Urp	Res	Win	Flags	Offset	Chksum
3126243973	1473114077	-	-	64231	AP	5	7295

Event Payload

Payload with Hex

```
46 72 6F 6D 3A 20 22 4A 61 73 6F 6E 20 4F 73 65   From: "Jason Ose
65 6E 22 20 3C 6F 73 65 65 6E 6A 40 78 78 78 78   en" <oseenj@xxxx
2E 63 61 3E 0D 0A 54 6F 3A 20 3C 61 64 6D 69 6E   .ca>.To: <admin
40 78 78 78 78 78 2E 63 6F 6D 3E 0D 0A 53 75 62   @xxxxx.com>.Sub
6A 65 63 74 3A 20 46 57 3A 20 74 65 73 74 0D 0A   ject: FW: test.
44 61 74 65 3A 20 53 75 6E 2C 20 32 36 20 4A 61   Date: Sun, 26 Ja
6E 20 32 30 30 33 20 31 35 3A 33 33 3A 35 36 20   n 2003 15:33:56
2D 30 37 30 30 0D 0A 4D 65 73 73 61 67 65 2D 49   -0700.Message-I
```

Alt-255 Decoded Payload

```
From: "Jason Oseen" <oseenj@xxxx.ca>
To: <admin@xxxxx.com>
Subject: FW: test
Date: Sun, 26 Jan 2003 15:33:56 -0700
Message-ID: <IOECLMPCCMFDNJMCMLBLCEFACNAA.oseenj@xxxx.ca>
MIME-Version: 1.0
Content-Type: text/plain;
.charset="iso-8859-1"
```

The Signature Information screen provides the contents of the data packet in its entirety for review. In addition, this screen provides the following utilities to gather more information on the source and destination hosts:

Whois - Contact information for a domain or IP address
Trace - Traces the route packets take to the host
Ping - Tests connectivity and the time it takes packets to get to the host
DNS - Resolves the IP address of the host

Also found on this screen are the links, "Find in Rules" and "More Info". Find in Rules takes the operator directly to the Snort rules for editing, and highlights the line containing the rule that triggered the event. This makes tweaking the rulesets for your environment a simple task. By using references in the Snort rules, the "More Info" link, if available, cross-links to databases of attack information found on Internet sites including "CVE" [12], "Bugtraq" [13], and "McAfee" [14], and provide more information on the vulnerability. In the PureSecure PERL script on Linux that's located by default at /usr/local/puresecure/console/cgi/", it appears that one could manually add an entire URL to the snort rule as well[15], although this isn't documented.

The "Monitor" screen, reached off the top menu, displays a list of all the hosts that are currently set up, and has icons that reflect their status. This resides on the upper part of the screen and is shown in Figure 16. The lower portion of this screen, not shown, displays a list of the most recent status changes.

Figure 16. – Service Monitoring Status

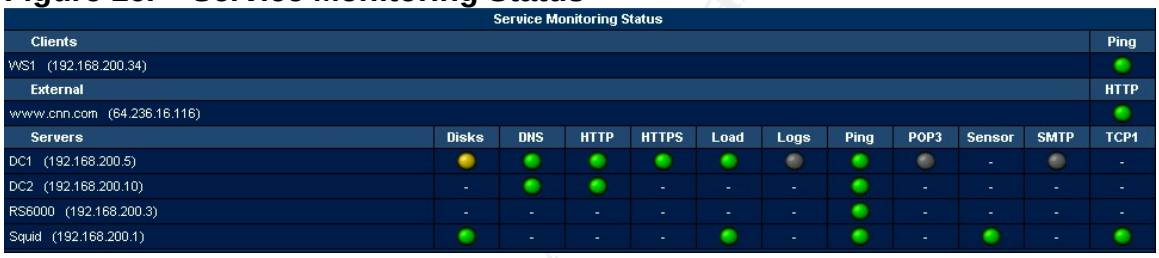
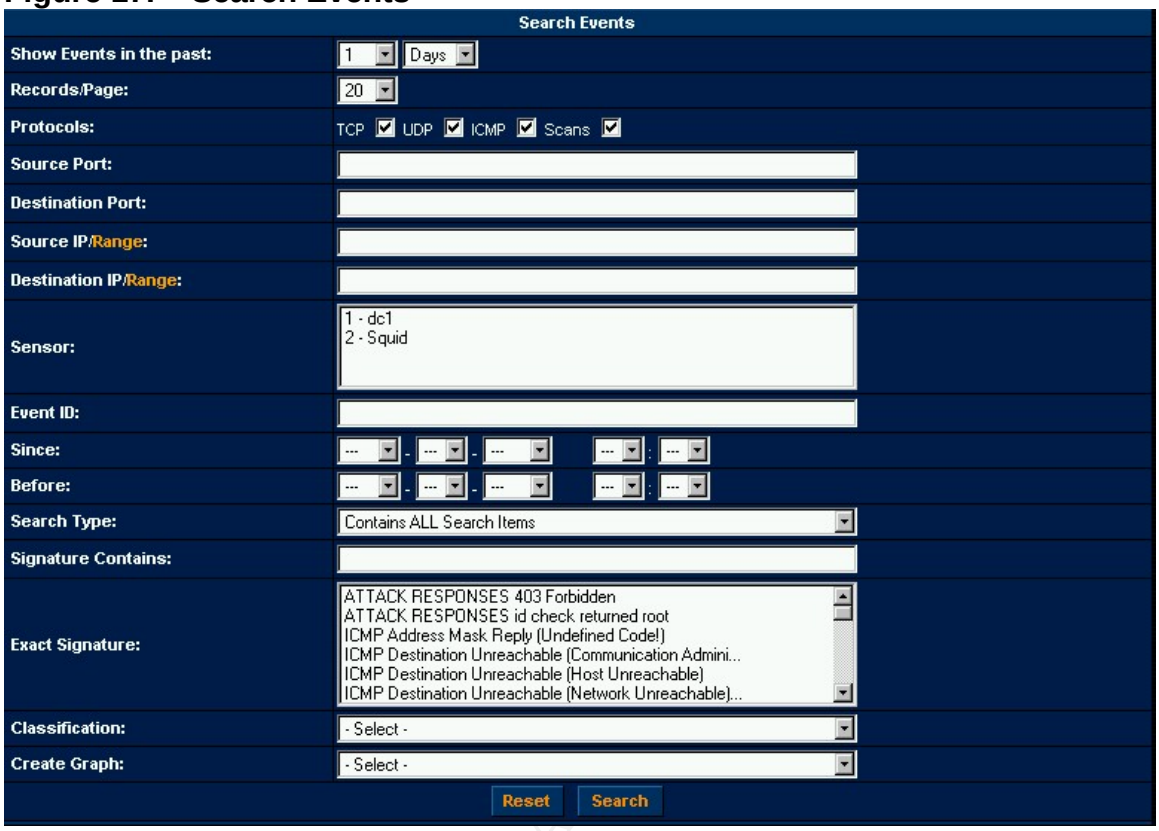


Figure 17. – Search Events



With the results from a search, most any event function is available. You are able to get more detail on a single event, the source and destination IP addresses, create special summary reports, or delete the events completely.

Conclusion

With the abundance of products available on the market, it can be a difficult task to choose an Intrusion Detection System that is full-featured, and still remains simple to set up and use. Demarc's PureSecure has an abundant range of abilities that makes the developer confident that it is one of a kind. Although there is a similar, free product called the Analysis Console for Intrusion Databases, or "ACID", one author states "PureSecure is much more polished, more complete, and more full-featured than its free software counterpart".[16]

This document attempts to illustrate the majority of the features available within the product, however, to fully appreciate how the functionality of PureSecure can save time and frustration in any environment, one must install it on a few machines and give it a complete evaluation. Although PureSecure is simple enough to install and use for those that are relatively new to intrusion detection, it can be tuned to be powerful enough for even some of the most complex scenarios.

References and Endnotes

[1] Kirsner, Scott. "The Legend of Bob Metcalfe." Wired Magazine. Issue 6.11. Nov. 1988. URL: http://www.wired.com/wired/archive/6.11/metcalfe_pr.html (26 Jan 2003).

[2] Sans Institute, The. "Host-Based Intrusion Detection." Security Essentials. Revision v1.8a (2002): p4

[3] Demarc Security. URL: http://www.demarc.com (26 Jan 2003)

[4] Caswell, Brian & Roesch, Marty. "What is Snort?" Jan. 2003. URL: http://www.snort.org/about.html (26 Jan 2003)

[5] "The Tcpdump Group", URL: http://www.tcpdump.org (26 Jan 2003)

[6] "Windows Packet Capture Library", URL: http://winpcap.mirror.ethereal.com/ (26 Jan 2003)

[7] "MySQL: The World's Most Popular Open Source Database", URL: http//www.mysql.com (27 Jan 2003)

[8] "GNU General Public License", URL: http://www.gnu.org/copyleft/gpl.html (27 Jan 2003)

[9] Demarc Security. "Demarc PureSecure 1.6 Personal Edition License Agreement". URL: http://www.demarc.com/license/puresecure16_personal.html (27 Jan 2003).

[10] Demarc Security. "Demarc PureSecure 1.6 Professional Evaluation License Agreement". URL: http://www.demarc.com/license/puresecure16_professional.html (27 Jan 2003).

[11] Demarc Security. "PS 1.6 User Guide". URL: http://www.demarc.com/support/documentation/ps1.6-userguide.pdf (27 Jan 2003).

[12] "Common Vulnerabilities and Exposures". URL: http://cve.mitre.org (02 Feb 2003)

[13] "SecurityFocus". URL: http://www.securityfocus.com (02 Feb 2003)

[14] "McAfee Virus Information Library". URL: http://vil.nai.com/vil (02 Feb 2003)

[15] Demarc Security. "PureSecure 1.6" Application for UNIX-type machines" PERL script, Lines 11328 – 11345 (2002)

[16] Barr, Joe. "How to Install PureSecure, the painless IDS". LinuxWorld. Apr. 2002 URL: http://www.linuxworld.com/site-stories/2002/0430.puresecure.html (02 Feb 2003)