SANS ANALYST PROGRAM

Sponsored by NIKSUN

NetDetector/NetVCR 2005 Traffic Analyzer

A SANS Whitepaper – August 2007

Written by: Jerry Shenk

Executive Overview

The NIKSUN NetDetector/NetVCR 2005 is like the "black box" on an aircraft. It collects all types of data, including packets, which can be analyzed later, when an organization suspects that some type of attack may have occurred. NIKSUN's approach to storing and making accessible all event and traffic data — all the way down to the packet level — is different from most network analysis appliances, which try to simplify the user interface and storage, but remove too much detail in the process. This leaves an experienced operator who needs packet-level detail at a disadvantage. Instead of being able to follow his own hunch by drilling deeper into the data, he's forced to trust a device's analysis instead of his own. While convenient for less experienced staff, this lack of detail presents a security risk in cases in which closer examination of traffic and events are required.

The NetDectector/NetVCR 2005 maintains the entire packet and all related network traffic so that the alert or incident can be reviewed in context. This is all done from a browser-based interface with a full complement of graphs, reporting capabilities and drill-down options. The NetDetector/NetVCR 2005 can also assist the operator in determining bandwidth usage and gathering very specific details about which machine, protocol or service the activity is occurring on.

Monitoring total bandwidth can be helpful in planning network usage around normal and peak traffic periods, as well as for setting a security baseline for normal user behavior. The ability to drill down and see how that bandwidth is or was being used can help track performance issues down to the device and services levels. More importantly, NetDetector/NetVCR, when configured correctly, can locate suspicious patterns of behavior that might indicate employee misuse or the existence of attack code inside the network. By detecting and alerting to the suspicious behaviors as they happen, this type of device goes beyond the reactive signature-based approach in which you must know the attack code before the system can look for and find it.

Because the NIKSUN appliance stores the traffic in its database, operators can access details on historical events in full context, to the level of detail that the analyst requires, including the bit level. Many other traffic analysis, IDS/IPS appliances and firewalls only log "important" information, such as traffic that matches a virus, worm or attack pattern. As a result, data that is considered "unimportant" in one case, such as a new, unknown attack — often called a 0-day attack — may not be detected. That seemingly unimportant data may be vitally needed once the attack is known and an organization realizes that they've fallen victim to it. This appliance stores all the traffic packets so that a high-level analyst can get the details required to determine the full extent of the damage, while a front-line analyst still has a simple user interface with graphs and charts with which to look for potential problems.

Another powerful feature of the NetDectector/NetVCR 2005 is the ability to reconstruct application data to re-create viewable e-mail messages, Web pages, chat sessions, ftp sessions and other traffic. This is particularly important when gathering information for litigation related to criminal hacking and employee misuse.

However, there are problems with reconstructing certain Telnet, FTP and e-mail sessions, as well as message data sets, which we cover at the end of this report.

NetDetector / NetVCR 2005 at-a-Glance

Licensing and pricing: Under $10,000 to over $100,000 depending on installation

System requirements: The NIKSUN NetDetector/NetVCR 2005 is a custom-made plug and play appliance.

Basic features:

- *Anomaly detection and real-time alerting on all events*
- *Unique data warehousing and mining for data storage and processing*
- *Archives relevant transactional details, including packet level data*
- *LAN, MAN and WAN interfaces for variety of access needs*
- *Identification of root-cause extends from user/host identification to applications and services including real-time trading, information warehousing, eCommerce, VoIP, Multicast, Instant Messaging, etc.*
- *NIKSUN's unique analytics to alert and identify activity as it happens*
- *Detailed security, performance, usage and other reports immediately validate the root-cause analysis*
- *Automated generation of management level reports*

Product Overview

The NetDetector/NetVCR 2005 is a custom-made network monitoring appliance that includes:

- *A packet capture device that stores packets that have been correlated to a proprietary statistical engine*
- *An embedded packet-viewer and protocol analyzer*
- *A proprietary database with custom applications for storing, parsing and correlating network event information*
- *A graphical interface and reporting center*

The appliance is rack-mountable and can be configured in a variety of ways to match data processing needs and interface requirements, including copper and serial interfaces such as T1 and T3, fiber optics for speeds up to OC48 and 10 Gigabit, SONET, ATM and almost any conceivable network interface. The appliance is based on a customized FreeBSD kernel and, in most cases, the disk space is configured as a RAID array. For even more storage, several SAN options are available.

The test unit was configured with 565 Gigabytes of drive space and two Gigabit monitoring interfaces. In addition there were two management interfaces. One of the management interfaces was connected to the lab network and the other was left unconnected. One of the monitoring interfaces was connected to the lab's core switch on a port that mirrored all the data to and from the firewall. The second monitoring interface was used for specific testing. The majority of the testing was done using the first monitoring interface. At one point, the unit was monitoring all the traffic to and from another lab switch in an effort to isolate specific traffic between specific hosts. The testing scenario is illustrated in Figure 1.

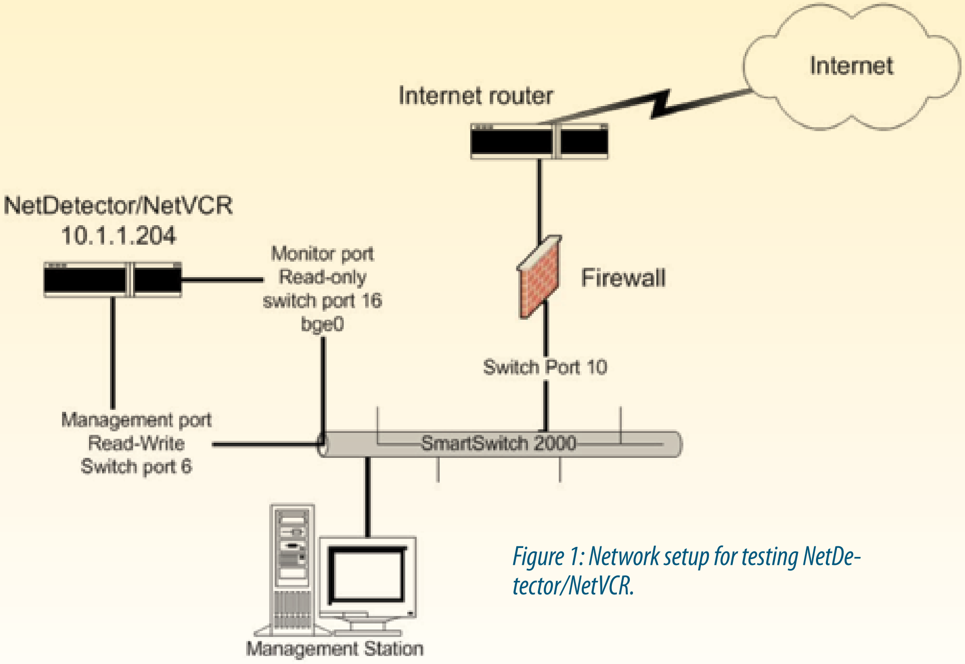


Figure 1: Network setup for testing NetDetector/NetVCR.

Initial System Setup

The appliance arrived well packaged with drive rails, network cables and a serial cable that could be used for setup if needed. It also came with some printed documentation, additional documentation on a CD-ROM and a CD that could be used to install the application. To protect the drives during shipping, they were packed separately within the shipping carton and were clearly labeled as to which drives should be installed into which drive bays.

There was some discrepancy in the documentation about how to initially get access and do the site-specific installation. Part of this was due to a corrupt PDF file on the documentation CD. NIKSUN had shipped the wrong version of instructions, and after a call to NIKSUN support, I received an e-mail with the correct documentation and instructions about running /etc/sys_config.pl.

This script was fairly straightforward. One question in the script asks about the type of firewall. I found out from NIKSUN tech support that this refers to the firewall configuration of the appliance, not the network firewall (i.e. PIX, Checkpoint, iptables, etc.). Tech support recommended that I use "open" as the firewall type in order to get into the Web interface with a cross-over cable to configure the firewall. During setup steps, that might leave your network open to attack, so at this point it's best to follow the installation guide and not put the unit on the production network until it's fully set up and tested.

After a reboot, the appliance was up and running so I could connect to the graphical screen and log in, as shown in Figure 2.

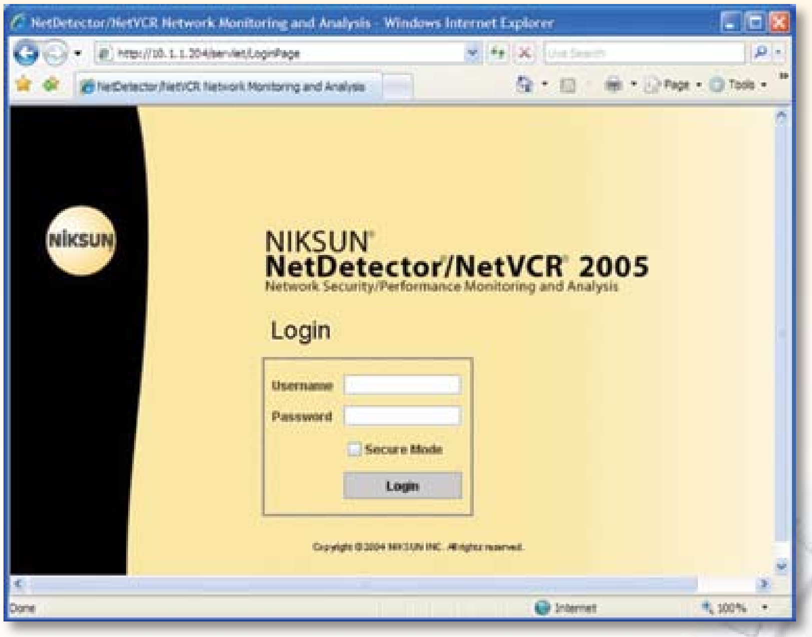
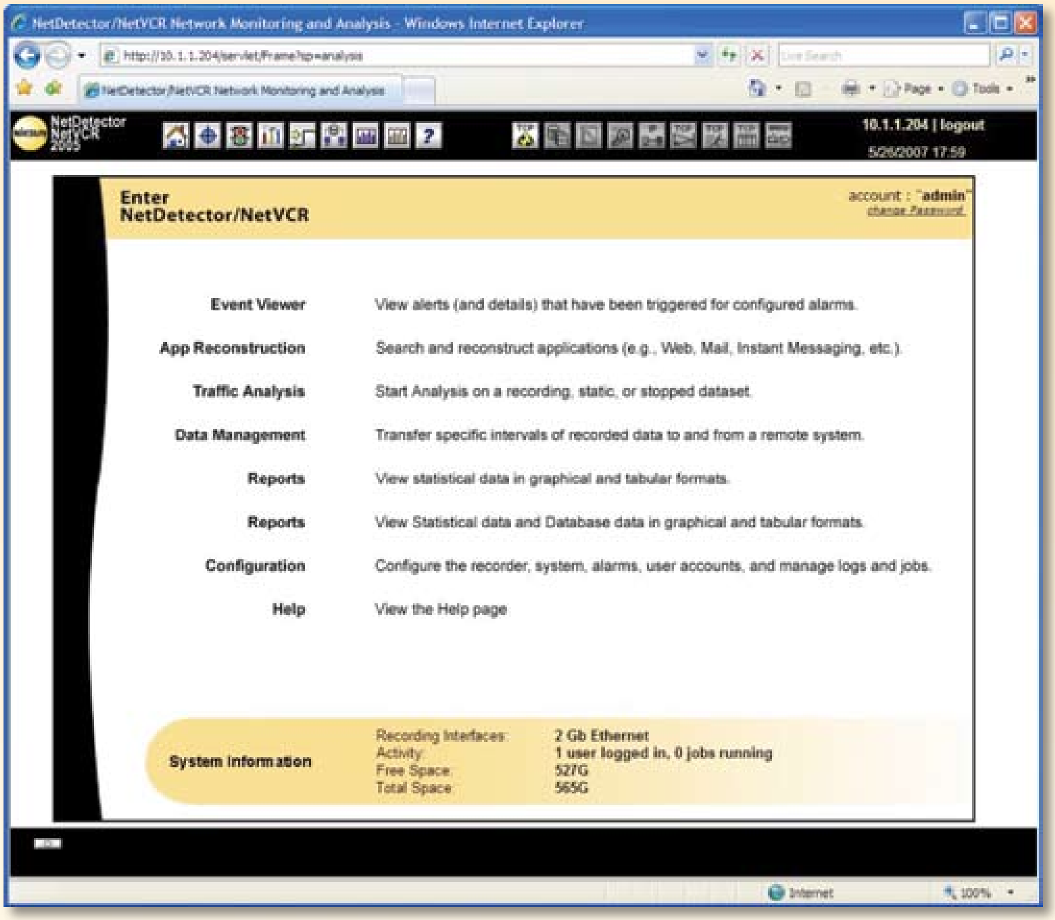

NetDetector/NetVCR Network Monitoring and Analysis - Windows Internet Explorer
http://10.1.1.204/servlet/LoginPage
NetDetector/NetVCR Network Monitoring and Analysis
Page
Tools
NIKSUN
NIKSUN
NetDetector/NetVCR 2005
Network Security/Performance Monitoring and Analysis
Login
Username
Password
Secure Mode
Login
Copyright ©2004 NIKSUN INC. All rights reserved.
Done
Internet
100%

Figure 2. NetDetector/NetVCR 2005 login screen.

You can change the interface from the configuration menu by clicking on the firewall link under the “Management Interface” section in the left frame. The other options for firewall types are explained in Chapter 2 of the Customer Installation Guide, which came as a pdf. If the IP information, domain name or host name needs to be changed, this script can be re-run, although this will have some ramifications related to previously stored data. The most obvious of these issues is that data that was collected with the original appliance name will not be stored with the current dataset. The appliance stores traffic data in datasets with names related to the hostname and the interface the data was collected from. Data with the old appliance name is, however, available if analysis of that data is required.

The default username and password are recorded in Appendix A of the user’s guide, a fact that was not clear in the initial setup documentation. This appliance contains full data captures from the network, so changing this password is critical, as it will soon be collecting confidential data. Because default passwords are one of the first things attackers look for when they get inside a network, instructions to change the passwords should be included prominently in setup instructions.

The main menu (see Figure 3) lists the primary features of the appliance, but it is not necessary to return to the main menu while doing data analysis. In most places throughout the system there is a menu bar at the top of the screen that enables quick access to the primary functions. Matching most menu items to their icons was intuitive, but some took a little guessing, hardly a major issue.


NetDetector/NetVCR Network Monitoring and Analysis - Windows Internet Explorer
http://10.1.1.204/servlet/Frame?sp=analysis
Live Search
NetDetector/NetVCR Network Monitoring and Analysis
Page
Tools
NetDetector
NetVCR
2005
10.1.1.204 | logout
5/26/2007 17:59
Internet
100%

Enter
NetDetector/NetVCR

account : "admin"
change Password

Event Viewer	View alerts (and details) that have been triggered for configured alarms.
App Reconstruction	Search and reconstruct applications (e.g., Web, Mail, Instant Messaging, etc.).
Traffic Analysis	Start Analysis on a recording, static, or stopped dataset.
Data Management	Transfer specific intervals of recorded data to and from a remote system.
Reports	View statistical data in graphical and tabular formats.
Reports	View Statistical data and Database data in graphical and tabular formats.
Configuration	Configure the recorder, system, alarms, user accounts, and manage logs and jobs.
Help	View the Help page

System Information

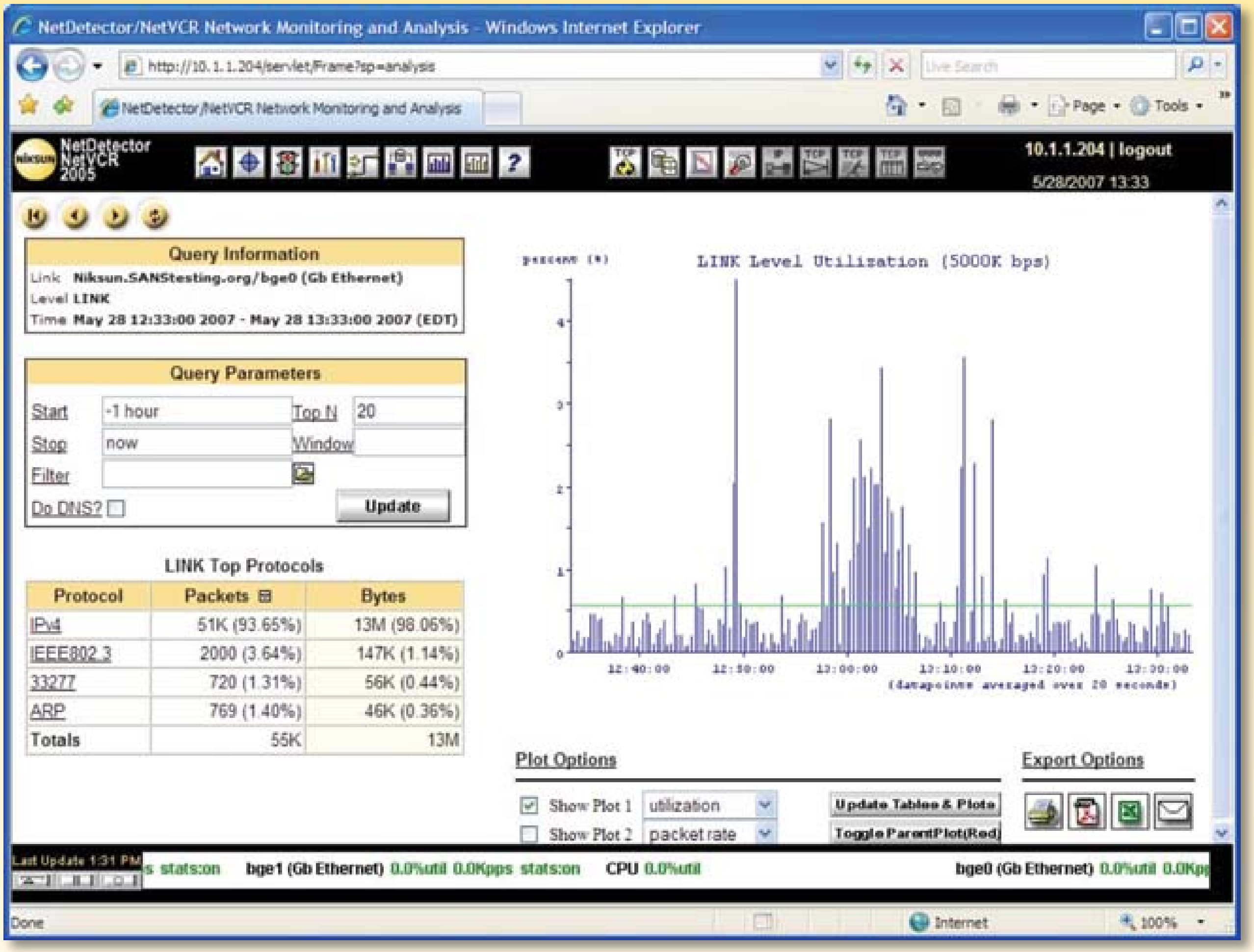
Recording Interfaces:	2 Gb Ethernet
Activity:	1 user logged in, 0 jobs running
Free Space	527G
Total Space	565G

Figure 3. NetDetector/NetVCR 2005 main menu options.

The configuration option from the main menu (system properties icon) allowed for the manipulation of the interfaces. The only tuning that I did initially was to tailor the link speed to coincide with the lab's Internet speed so that I could get a good picture of network utilization relative to Internet activity. I also gave the port "bge0" the name "Firewall port" to make it a little clearer what traffic was being monitored. In the lab, this is almost silly; but, in a large environment with a half-dozen or more interfaces, having meaningful interface names would be helpful. These interface names are also included in reports, and hence would be much more meaningful to management and other non-technical audiences if the names reflected the interface's function.

Functionality: Network Monitoring and Analysis

Traffic Analysis is the core feature of the NetDetector/NetVCR 2005 appliance. By default, all packets are collected and stored. After the data has been stored, the traffic can be analyzed (see Figure 4). By storing all the traffic, the network analyst does not have to project what will be analyzed prior to an incident occurring. Because of this feature, the data would still be there to analyze if an enterprise thought they needed one piece of information, such as traffic to their critical servers, but later found out that they needed something different, such as data on a normally inconsequential test server that was compromised.


NetDetector/NetVCR Network Monitoring and Analysis - Windows Internet Explorer
http://10.1.1.204/servlet/Frame?sp=analysis
Live Search
NetDetector/NetVCR Network Monitoring and Analysis
Page
Tools
NetDetector
NetVCR
2005
10.1.1.204 | logout
5/28/2007 13:33

Query Information

Link Niksun.SANStesting.org/bge0 (Gb Ethernet)
Level LINK
Time May 28 12:33:00 2007 - May 28 13:33:00 2007 (EDT)

Query Parameters

Start -1 hour Top N 20
Stop now Window
Filter
Do DNS? □ Update

LINK Top Protocols

Protocol	Packets	Bytes
IPv4	51K (93.65%)	13M (98.06%)
IEEE802.3	2000 (3.64%)	147K (1.14%)
33277	720 (1.31%)	56K (0.44%)
ARP	769 (1.40%)	46K (0.36%)
Totals	55K	13M

percent (%)
LINK Level Utilization (5000K bps)
4
3
2
1
0
12:40:00
12:50:00
13:00:00
13:10:00
13:20:00
13:30:00
(datapoints averaged over 20 seconds)

Plot Options

☑ Show Plot 1 utilization
□ Show Plot 2 packet rate

Last Update 1:31 PM s stats:on bge1 (Gb Ethernet) 0.0%util 0.0Kpps stats:on CPU 0.0%util bge0 (Gb Ethernet) 0.0%util 0.0Kp

Figure 4. NetDetector/NetVCR Graphical interface showing network utilization for the prior hour.

Data storage space is managed by the appliance and historical data is stored as long as possible. NIKSUN has benchmarked many customers with 8+ TB of active storage and a couple with 12+ TB of active storage per device. The largest of these have plans to grow to 40+ TB.

Space is configured as a RAID array. As the storage space becomes full, old data is deleted. Depending on the size of the organization and its regulatory requirements, it may need to maintain specific types of data for a year, three, even more. So, for even more storage, several SAN options are available.

To lighten the storage requirement, there is a configuration option within the system properties icon that allows the analyst to specify what traffic to collect. For example "host 10.1.1.116" will collect only traffic to or from the host 10.1.1.116. This filter and other filters on the appliance must be configured in Berkeley Packet Filter (bpf) syntax. The bpf syntax is a powerful filtering syntax that's also used with TCPdump, and many other traffic analysis tools (see sidebar).

One handy feature of the traffic analysis screen is that you have the option to automatically update the screen. There are times you would want to turn this feature off. For example, during a specific analysis, like researching traffic patterns for a specific time frame, the default option of not updating is handy. For general purpose monitoring, being able to have the screen update on a regular basis is helpful for delivering regular reviews and visual status updates to the system operator.

Berkeley Packet Filters

One of the key mechanisms for tuning the NetDetector/NetVCR 2005 is applying a Berkeley Packet Filter (bpf) syntax filter. The basic construction of these filters is very simple, but they can also be very powerful. This appliance can use basic bpf filters.

When doing network forensics, two of the most used selection criteria for packets are the host IP address and the port. If we already know that we are looking for traffic from a particular host, we can specify only that host with the bpf "host 10.1.1.116." That would restrict the displayed traffic to the host 10.1.1.116.

If, however, we had one host that we knew was generating a lot of legitimate traffic and we wanted to analyze all traffic EXCEPT that one host, we could use the filter "not host 10.1.1.116."

We can also include or exclude traffic based on the port, as in "port 80" to limit the display of traffic to port 80 traffic only. Conversely, "not port 80" would exclude port 80 traffic.

It's also possible to combine filters into a longer statement such as "port 80 and not host 10.1.1.116." This filter would result in displaying only port 80 traffic from all hosts EXCEPT the specified host.

By default the appliance collects all data, with options to drill down to more specific information as desired. If there is a need to analyze some particular traffic, that can be done from the GUI menu by entering a time in the start and stop fields, entering a bpf filter, or drilling down on the various protocols, ports and hosts. At any time during the drill-down, the option to view raw traffic is available from the "View Decoded Dump of Traffic Data Packets" icon (🔍) in the menu bar. Selecting this icon brings up the "View packets" screen, from which data can be exported to the local machine in pcap format, if further analysis is needed, using packet analyzers or a variety of other traffic diagnostic tools available as products or freeware.

From a forensic standpoint, this handy little traffic packet analysis icon is a critical feature because it allows for an independent audit of the same traffic without having to drag down menus. Many traffic analysis solutions only report summary data, without providing any access to the raw data. As a result, independent analysis is impossible to do after the fact.

One example of using the device's network monitoring capabilities took place in the lab. While testing the appliance, an anomaly alarm was generated when I had a spike in utilization. Utilization on the test lab typically runs around two to five percent overnight. The NIKSUN appliance generated the alert that utilization was over 40 percent. I was able to review the entire day and see a large utilization spike at around 8 p.m. I entered start and stop times of "Jun 5 19:38:30" and "Jun 5 19:56:30," respectively, to quickly narrow down the exact time of the spike. Entering the month as June would also have worked. The results of my analysis are included in the Appendix.

Being able to use easily understood syntax for this search eliminated the need to pull up the NIKSUN documentation for valid search criteria. I was able to see that there were two spikes of a couple minutes' duration by typing the time and date information into the GUI. The traffic was over 99% IPv4 traffic, so I clicked on that link to start drilling down to find the source of the traffic.

Before going any further, I wanted to document what I'd found so far. I did that by exporting the information to a PDF. The next step was to either highlight the TCP protocol that was responsible for 98 percent of the traffic or highlight the IP address that was responsible for 91 percent of the traffic (10.1.1.195). I selected the IP address and could then see that the two spikes were each related to different public IP addresses. By this time, I also knew that this was not anything malicious. The 10.1.1.195 IP address is a new Microsoft Windows Software Update Services (WSUS) server that was being tested in the lab. The two spikes were 100% Web traffic that matched WSUS-related traffic. I also clicked on the "View Decoded Dump of Traffic Data Packets" icon and could see the WSUS server requesting the file `v3-19990518/cabpool/mpas-fe_65169cfff3d8acd897cdd18d1a4d06f1edd1ed0b.exe`. That's a pretty clear picture of exactly what happened.

It took about 10 minutes to get the information I needed to classify this as a non-issue. To be sure this process worked in an historic context, I went back a week later and reproduced my initial findings through analysis of the stored data. Often, when dealing with a security event, we don't find out about things until after the fact, so being able to reconstruct the event from the full packet information stored in a searchable database is valuable.

Event Viewer

The Event Viewer is the Intrusion Detection System (IDS) part of the appliance. Events can be defined as IDS signatures, Anomalies, Real Time Xperts, NetSLM/Threshold, and Content. The test appliance is licensed for IDS and Anomaly alarms.

The IDS is based on Snort® and has a lot of potential. It is a rather simple task to store and view alerts. There is, however, no function to automatically update signatures. In many cases, administrators may want to update signatures manually to maintain tighter control over their network signature files. In most cases administrators would like to at least have the option of automating that function.

NIKSUN says it plans to have that level of automation available in first quarter of 2008. In the meantime, Nikun does have an option to manually connect to NIKSUN's SupportNet portal to download new signatures. The URL for the signature updates comes pre-loaded into the appliance and new signatures are posted for update the last Friday of every month (with signatures for critical, zero-day vulnerabilities being updated on an emergency, as-needed basis, in compliance with standard industry practice). On more than six occasions between early April and mid-July when I went to the URL to upload signatures, I was given a message indicating a successful upload, but each time was told there were no new signatures for my machine. After several calls and e-mails back and forth, NIKSUN product managers determined that the signature update URL loaded into the test system was not aligned with the version of Snort® on the test device. This is a common enough problem that mitigation information is automatically e-mailed to their new clients through their SupportNet newsletter.

This is an unacceptably messy and risky process that we hope NIKSUN won't repeat in its upcoming automatic updates. Intrusion and monitoring systems like these must absolutely ship with current, up-to-date IDS signature information and make it easy to get those signatures. Furthermore, troubleshooting information should be included in the information documentation itself instead of an external newsletter. Otherwise, NIKSUN leaves enterprises vulnerable to new malicious code getting past out-of-date defenses.

GUI Options and Settings

The GUI options from within the graphical environment allow the administrator to configure a filter for the IDS system, apply the IDS to a single interface, configure a Syslog server, and enable or disable individual rules. However, there is no option in the GUI to create or modify individual rules. Detailed rule manipulation requires hands-on familiarity with FreeBSD and Snort® from the command-line on the console. For a system administrator with those skills, this should not be a major problem. However, it is an inconvenience and makes it more difficult to make changes as security policies, application types and usage requirements dictate them. A lot of work is required if a new network attack occurs or if you need to tune the IDS to modify the "$HOME_NET" variable.

To make detailed modifications of the IDS ruleset, including adding custom rules, it's necessary to use ssh to connect to the appliance and make those changes at the command-line. One word of warning: Using ssh to make changes at the command line is a multi-step process that should only be done by personnel who are familiar with Snort® and Linux-type system administration. It involves connecting a keyboard directly to the appliance or using ssh to connect to the appliance. By default, the user root is not permitted to ssh to the appliance, so it's necessary to connect using the account vcr. The password for vcr can be changed by the root user from a keyboard connected directly to the appliance with the command "passwd vcr". Then an administrator can use ssh to connect to the appliance and elevate his access with the command "su –". At this point, he'll be asked for root's password. Once the administrator is at the console prompt on the appliance, the snort rules are located at `/usr/local/niksun/snort/rules/`. This directory also contains the `snort.conf` file. As with most Snort® installations, the local.rules file is normally not updated automatically and is a good place for custom rules. After adding custom rules you have to restart the IDS. To do this from the graphical screen, select the configuration option from the main menu screen. In the left frame, under the Alarms section, click on the IDS Signature link and then on the "submit" button to apply your changes.

The Event Viewer menu also contains a number of pre-configured "Anomaly Alarms." These alarms can be configured to alert based on the breaching of a predetermined threshold based a number of metrics including server response and utilization. As with most features of the NetDetector/NetVCR 2005, these alarms can be applied or not applied based on the appliance's configurable bpf filters.

One use for applying filters to an alarm would be to track outbound ftp traffic. In many companies, ftp traffic is allowed and commonly used by IT staff, art departments and other business units with legitimate purposes for moving large files around. Even in those instances, a sudden increase in outbound ftp traffic could signal an insider data breach or a misconfiguration that demands further examination.

Traffic Reconstruction

The Application Reconstruction option is a useful feature that's made simple on this appliance. In this context, "Application" refers to specific types of network traffic like HTTP (Web traffic on port 80), SMTP (e-mail traffic on port 25), Telnet (port 23 traffic), etc. In many traffic sniffers, it's possible to select a particular data stream and extract data files, for example, files in an ftp data stream or individual messages in an SMTP data stream. There are also programs to extract specific types of data, such as driftnet[1] that will extract images from Web traffic.

The NIKSUN appliance does a reasonable job of providing application reconstruction for a wide range of application data types. However, there were some problems with reconstruction. In lab testing, we ran into irregularities with Telnet data reconstruction. Telnet sessions to BSD–and Linux-based hosts often showed up if the login was completed. Telnet connections to a variety of Cisco devices were never correctly reconstructed as Telnet sessions. They were recognized as a completed session, but the system did not identify the kind of completed session. There were similar discrepancies with SMTP traffic. Most mail was correctly defined as mail, but some sessions, particularly odd sessions that would be more representative of spamming or attempts at reconnaissance, were not correctly identified as e-mail sessions. In all cases, the traffic was successfully captured and extracted into sessions for manual review.

As useful as it is, relying solely on the Application Reconstruction feature could cause crucial data to be missed. Manual review of the session data is warranted in cases of importance.

In every case I tested, the data was all there. It just wasn't correctly identified. One possible work-around for dealing with specific application traffic is to use the session tab instead of the individual application breakdown tabs. To accomplish this, right-click on a session and then select ASCII to see the entire ASCII session. To replace the functionality of the "telnet tab," an analyst could enter "port 23" in the filter field and then view sessions under the session tab. Such an approach would restrict the traffic to port 23, which normally runs Telnet traffic. With the NIKSUN appliance, this work-around produced consistently accurate results.

[1] http://freshmeat.net/projects/driftnet/

Summary

NetDetector/NetVCR 2005 is a network traffic analysis appliance that fills a need in many organizations to monitor and analyze traffic for security events, policy violations, and general network health and well-being. This device has a lot of functionality that helps analyze network traffic and look for anomalies. If I were forced to pick a single feature to highlight, it would be the fact that full packet data is archived. This provides the experienced analyst with the raw data needed to do an in-depth investigation. Other positives include the fact that the appliance also has a wide range of configuration options that allow it to monitor traffic from a number of different interfaces simultaneously. The option for importing and exporting raw data is another feature that enables the verification of evidence. Even with all the detailed functionality, the appliance is simple enough that an entry-level analyst can get it up and running quickly.

The setup documentation is a little spotty, so the installation should be done by someone who is knowledgeable about networking, network monitoring and Linux-type operating systems. The personnel assigned to operate this appliance should be given ample time to work with the appliance prior to an going live in a production environment so they are familiar with its capabilities. That familiarity will make it possible to get the needed data quickly when there is a need for a serious investigation. The Application Reconstruction feature could be used for first level analysis, but verification using the Traffic Analysis feature should be performed prior to making critical determinations.

Because of my work in forensics, I'd love to have one of these appliances sitting on every network I work on because I could get to the data I need faster using intuitive syntax. I would, however, advise users to set it up carefully, replacing all default passwords with strong unique passwords in initial setup. Another area to pay attention to is your Snort® signature updates. Even as the new automatic update features roll out, continue to confirm that new signatures are updating on a monthly and as-needed, zero-day basis. Potential buyers should also be aware that not all session data is treated equally, so there will be instances in which their data doesn't render right. When that happens, they will need to drill down on the data manually. In future versions, I'd like to see NIKSUN get a more consistent rendering of all data formats.

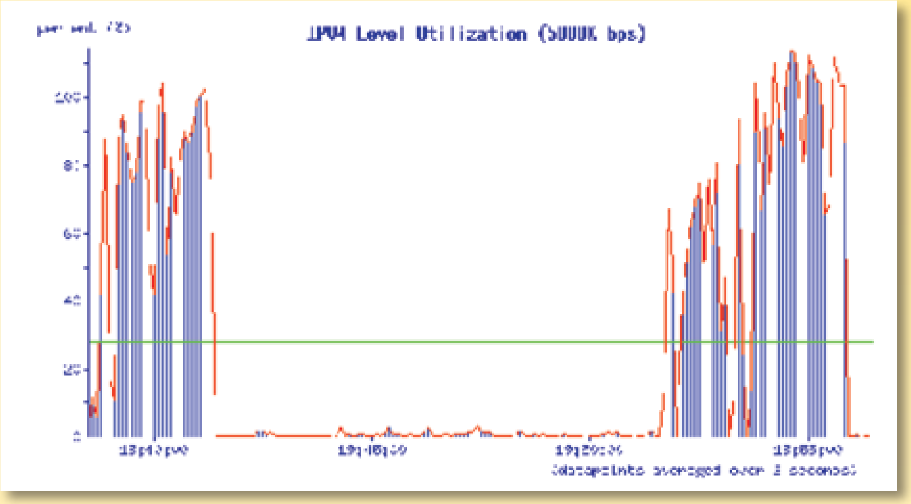
About the Author

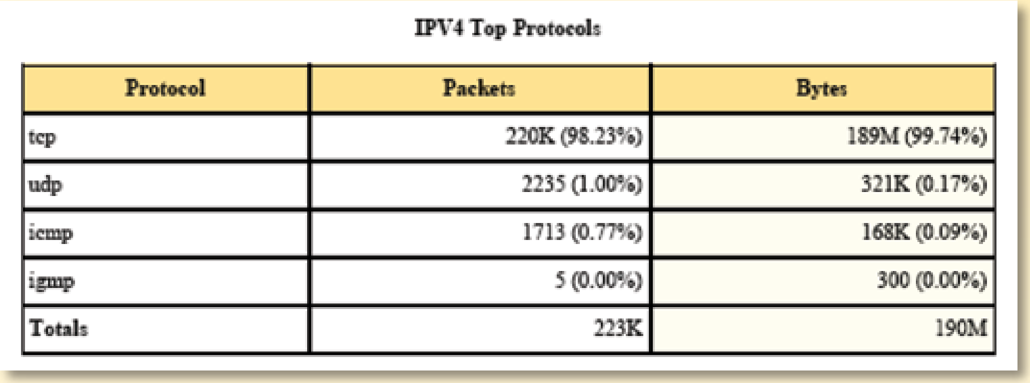
Jerry Shenk *currently serves as Senior Analyst for the SANS Institute and is the Senior Security Analyst for D&E Communications in Ephrata, PA. Since 1984, he has consulted with companies and a variety of financial and educational institutions on issues of network design, security, forensic analysis and penetration testing. His experience spans from small home-office systems to global networks. Along with some vendor-specific certification and a CISSP certification, Jerry holds five GIAC GOLD certifications: GCIA, GCIH, GCFW, GSNA and GCFA, all completed with honors.*

SANS would like to thank

NIKSUN®

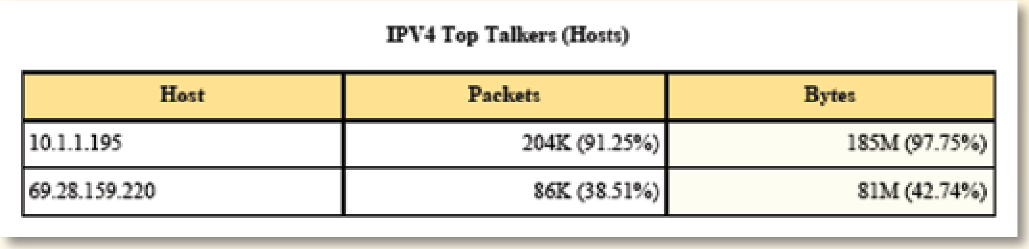
Appendix: Traffic Analysis





IPV4 Top Protocols

Protocol	Packets	Bytes
tcp	220K (98.23%)	189M (99.74%)
udp	2235 (1.00%)	321K (0.17%)
icmp	1713 (0.77%)	168K (0.09%)
igmp	5 (0.00%)	300 (0.00%)
Totals	223K	190M



IPV4 Top Talkers (Hosts)

Host	Packets	Bytes
10.1.1.195	204K (91.25%)	185M (97.75%)
69.28.159.220	86K (38.51%)	81M (42.74%)