InfoWorld®
July 14, 2003 ■ ISSUE 27
GET TECHNOLOGY RIGHT

NIKSUN Wins InfoWorld's
2004 Technology of the Year Award
NIKSUN NetDetector: Best Network Security Product

NetDetector Captures Intrusions

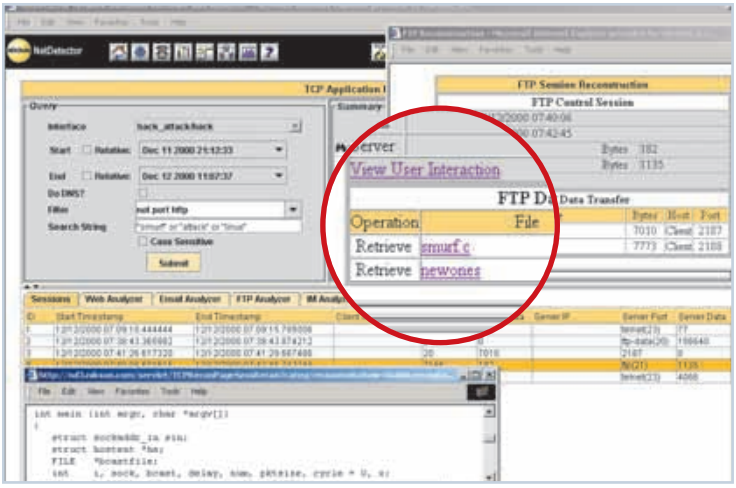
Niksun appliance combines complete event recording with powerful reporting and analysis

PAUL VENEZIA

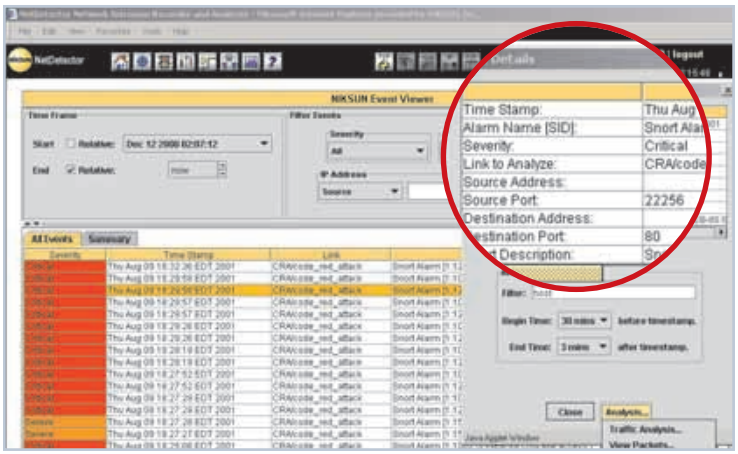
IT'S NOT OFTEN that I bear witness to a perfect match of innovation and execution, but Niksun's NetDetector is as close as I've seen. To the casual observer, the NetDetector appears to be simply another IDS (intrusion-detection system), but it actually goes much further than that.

Rather than simply capturing the packet headers of monitored data streams, and examining them for possible attacks, the NetDetector stores every packet, from header to payload, in an indexed database. This not only permits an administrator to be notified when an attack has occurred but also to reconstruct the attack, keystroke by keystroke, packet by packet, and determine the exact commands issued by the attacker, in addition to any files or other data that was transmitted to or from the compromised system.

Further, the NetDetector's packet-capture and playback capabilities are accompanied by a truly intuitive management console, and full standards-based reporting tools. While working with the NetDetector, I found that nearly every option I could have asked for was available, from importing and exporting packet captures in a variety of formats to exporting reports and graphs. In short, the NetDetector is simply done right.



NetDetector dissects attacks and allows administrators to reconstruct them. Here we see that an attacker used FTP to pull the files 'smurf.c' and 'newones' to a compromised server. By clicking on the file names, we can even view the contents of the transmitted files.



NetDetector uses the Snort IDS to analyze attacks and provides a great deal of flexibility in viewing the data. Here Niksun's Event Viewer organizes detected attacks by severity, filtering on a single host.

Built for Speed

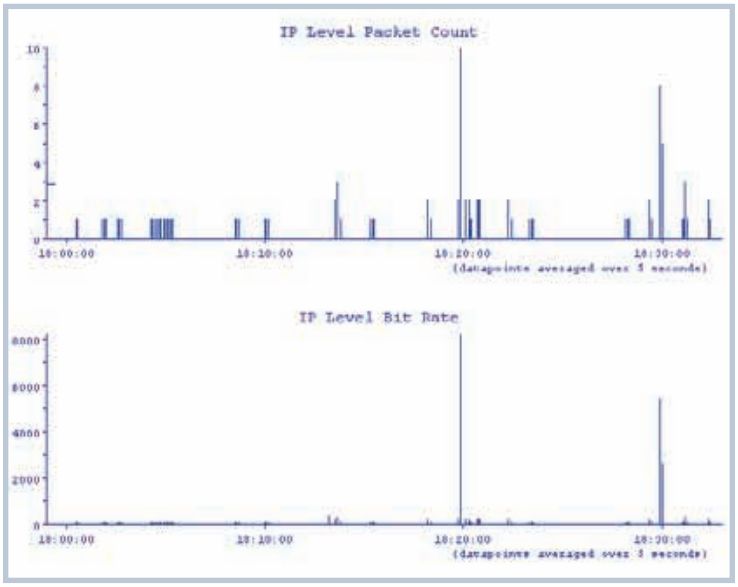
The hardware foundation of the NetDetector unit I tested is a SuperMicro SuperServer 6022L-6 with two 2.8GHz P4 processors, 2GB RAM, and six 72GB SCSI drives. The OS is tried-and-true FreeBSD with a custom kernel. The system can utilize any number of interfaces, from standard Ethernet to ATM, Packet-over-SONet (Synchronous Optical Network), and HSSI (High-Speed Serial Interface). My test unit came with four 100Mbps Ethernet interfaces (one for management). Each interface is treated as a separate entity, allowing them to monitor completely different networks and

group all captured data accordingly. In fact, every data set represented within the management UI is considered an interface, whether an actual physical interface or a finite data set captured manually.

The internal storage of the unit I received is a JBOD (just a bunch of disks) array, since the proprietary Stream database is file system-based. Packet captures can be stored across physical and logical partitions, and the NetDetector can be configured with FC (Fibre Channel) host bus adapters to integrate with an existing SAN environment to augment its internal storage capabilities.

For intrusion detection, the NetDetector relies on Snort, the open source IDS. As with any IDS unit, the Snort IDS engine can be enabled to monitor all traffic or a selected segment (based on filtering rules) on any given interface. Additionally, it's possible to select a specific time frame or capture and reprocess that traffic stream through the IDS engine. The NetDetector also has extensive event reporting and notification capabilities, and can send e-mail notifications and SNMP traps when an event is triggered.

The management interface is a Java-based console, accessible by Web browser. The main menu is well-organized and cleanly presented. Selecting "Start Analysis" brings you to a selection of monitoring interfaces. Once the appropriate interface is selected, an abundance of data is presented, but it's extremely simple to drill down into that data to pull out the relevant data set. Data presentation can be sorted by protocol, date, source, destination, attack or signature type, and so on. As data is presented in a frame on the left, graphs can be plotted from that data in the mainframe. These graphs are interactive; you simply drag the mouse over the graph to select a time frame for closer inspection. As the graph detail expands, the hosts referenced by the newly drawn graphs are presented on the right, and all data related to those hosts change to match the time frame selected.



NetDetector also provides graphical views of events, such as this CodeRed attack measured over 30 minutes. The graphs are interactive; to select the timeframe, you simply click and drag the mouse over the graph, and the data set changes accordingly.

Network Forensics

Once a particular attack or signature has been identified, every packet comprising that event is available, both in raw packet form or presented in an HTML rendering of its original format. For example, in the lab, I passed an AIM chat session by the monitor; later, I was able to reconstruct the entire session and view it (in an HTML mock-up) from either user's perspective. Another option is to replay the session, just as it was recorded.

You can export any capture in standard pcap (packet capture) format for importing into protocol analyzation applications such as Ethereal. You can also view the raw packet data through the NetDetector's internal packet viewer.

The NetDetector doesn't stop there, however. Rather than using a proprietary filtering language, you enter all filtering commands in standard bpf (Berkeley Packet Filter) format, easing the curve for anyone familiar with tcpdump, Ethereal, or other bpf-based applications. After relevant data has been selected, generating reports with charts and graphs is easy. The reports can be exported in HTML, PDF, and CSV (Comma-Separated Values) format, or e-mailed directly from the interface. Also, it's simple to have reports run at scheduled intervals and e-mailed to administrators.

On June 18, the North American Association of Securities Dealers (NASD) mandated that brokerage houses must store all instant messages sent or received by their brokers for a period of three years. This is only the first such requirement placed on instant messaging in the enterprise, but it's certain that more will follow. The technological side of these requirements is usually vague, but the function must be performed. Niksun's NetDetector can be easily adapted to this purpose, given its powerful searching, storage, and filtering capabilities. In fact, it's easy to implement filters on the monitoring interfaces to watch only traffic from certain IP addresses, IP subnets, protocols, protocol families, and so on.

While truly an impressive tool, NetDetector comes with a few caveats. Obviously, encrypted traffic cannot be viewed, so HTTPS and SSH (Secure Shell) traffic remains obscured. Another caveat is liability. If the NetDetector has captured and archived sensitive data, that data could be retrieved by anyone with administrative access to the system or potentially by subpoena. Niksun can build a NetDetector with filtering rules hard-coded to prevent even administrators from capturing data from sensitive hosts. Other than that, it's a best practice only to retain captured streams for a defined length of time.

Niksun has produced an impressive product in the NetDetector, both in the interface and the back end. If you need to go further, add-on products such as NetVoice can expand the capabilities of the NetDetector to permit decoding and analysis of VoIP data. In any case, the NetDetector will give you more information about your network than you would have thought possible.

— *Paul Venezia*

Niksun NetDetector

Niksun niksun.com

EXCELLENT 9.3

Performance (30%)	10
Security (30%)	9
Management (20%)	9
Configuration (10%)	9
Scalability (10%)	9

COST: $28,000 as tested, with four 10/100 interfaces

BOTTOM LINE: Niksun hits the mark with a well-designed and well-implemented network forensics tool. From the intuitive UI to the extremely responsive database, the NetDetector is a stellar blend of innovation and execution.

BEST NETWORK SECURITY PRODUCT

Niksun NetDetector is a near perfect match of innovation and execution. It not only detects but records and replays intrusions.