



NI-LAN Network Monitoring System

Overview

The NI-LAN system is a high performance and logic intensive network monitoring system that has been hardened over the years.

The default setting of the NI-LAN system is to capture every IP packet (headers and content) and write all packets to a Session Content File associated with the local address referenced within the IP header.

To sustain real-time and background processing without any packet loss the system uses up to one hundred and twenty eight (128) megabytes of memory packet buffer space. This large memory buffer space is necessary during period of high packet transient spikes and is used extensively during the overnight archiving of all session files.

The NI-LAN software is highly customizable to meet specific monitoring applications. Within your environment the emphasis may be on providing the information required for detailed network forensic analysis and for Information Assurance purposes as an extension to the intrusion detection services provided within your group. The emphasis may be on turning over complete session content files for review by law enforcement authorities.

Because the NI-LAN was designed to monitor everything, the system is particularly good at identifying unusual patterns of activity. A cumulative filtering mechanism, encompassing five filter classes, isolates those session files that should be further reviewed.

NI-LAN background search operations (in distinction to real-time auditing) have high value when the need arises to identify specific session activity that occurred within completed sessions. The background search directs the system to scan completed session files and report all session files that contain a match to the search arguments. The full forces of the five filter classes are used to select which completed session files are searched.

Search operations are extremely flexible. For example, a background search for a new overnight virus will be initiated by simply specifying the virus (Hex or ASCII) signature. The Search Report identifies all session files containing matches to the virus signature. These session files may then be reviewed packet by packet to cull necessary detail on transmittal or reception of the new virus.

The real-time NI-LAN system will search in background mode the last 250,000 online session files at a rate of up to one million packets per minute. This background search rate will double as faster processors are deployed.

On the real-time NI-LAN system all operational activity, including background search operations, occurs within "spare" processing cycles with no impact on critical real-time packet capture, auditing and disk writes.

An NI-LAN Surrogate system is available to provide the full functionality of the real-time NI-LAN system (exclusive of real-time processing) for review of archived session files.

The largest NI-LAN configuration is four systems within a single rack-mounted enclosure. The largest NI-LAN configuration within the 2U chassis is one system.

The NI-LAN system can be used for quite varied monitoring applications. Setting up a monitoring application requires defining what to look for then defining where and how to look. What to look for is defined by setting up simple string arguments, complex string arguments, and scenarios within the auditing structure. Where and how to look is defined by setting twenty five (25) switch values and fifteen (15) configuration functions.

Auditing within the NI-LAN system can be quite simple or very complex depending on the subtleties of the information being sought. NI-LAN system auditing is much more than simply looking for string arguments and includes identification of various combinations of events and a mechanism for real-time alerting. The NI-LAN auditing structure contains ten audit sets each with twenty audit elements. Elements within an audit set may be simple string arguments, complex arguments (where multiple strings must evaluate true within a given packet for the argument to be true) or scenario arguments. Scenario arguments consist of simple or complex elements or other scenarios defined in a logical relation. Scenarios are evaluated as true or false.

Audit sets are best ordered by purpose. One audit set might define virus signatures. Another set might be a "nasty" set to identify inappropriate network usage. A third set might be used to identify hacking attempts with an archive and red alert attribute set if hacking is determined to be successful. A set might be established to monitor for espionage or hints of terror. An ad hoc set is quickly defined depending on a purpose shaped by current events. When an audit element is defined, the setup of that element within the audit set, within the auditing structure, is completed in seconds with no disruption of monitoring.

Depending on the setting of the Operational Mode switch the NI-LAN system will monitor either local-to-local or local to remote (e.g., Internet) packet activity. In either mode of monitoring it is necessary to set the master :FILTER: function to define the address range of local addresses. The master :FILTER: function is generally set to the first two octets of all local class B addresses to be monitored and the first three octets of all local class C addresses to be monitored. When monitoring local to remote it is necessary to define all local proxy addresses to the :EXCEPT: function to override the local to remote monitoring default of discarding packets that are transmitted from one local node to another local node. Once defined, the addresses within the :EXCEPT: function list are considered to be remote addresses and packets will not be discarded when coming from a "local address" proxy. All other Switch and Function settings default to capturing all packets on all protocols on all ports and writing all packets to specific individual session content files associated with the local address.

(Based on switch and function settings, the NIC driver code and the associated Interrupt Service Routine (ISR) processing is optimized to eliminate packets at "first glance" that do not meet the application requirements. For example, there might be no need to retain packets that only have the "ack" flag set within the IP header if there is no data content within the packet. These packets are discarded at first glance if the No Content switch so specifies. If the Operational Mode switch is set to monitor local to remote (e.g., Internet activity) then packets traveling local node to local node are discarded at first glance. This ability to make first

glance decisions without forwarding irrelevant packets into the reduction process SIGNIFICANTLY enhances the performance of NI-LAN systems. There are seven switches and five functions which adjust the "first glance" analysis to make sure that only packets that meet application monitoring requirements are forwarded.

Both online and archival disk storage is conserved by the setting of the Session Retain switch. A backward look is done at the time the session is closed out. If no alerts were generated or no critical audits matched or scenarios evaluated true then the Session Retain switch determines if the session should be retained or immediately deleted. If immediately deleted then no entry is made to the system master file. Similarly, the Session Size switch determines the minimum session content file size that is to be retained. The default for both the Session Retain switch and the Session Size switch specifies that no session content files are to be deleted at session completion.)

Possible NI-LAN applications within your environment include:

1) Monitor all network activity to develop a dynamic profile of the use of network resources. The monitoring and reporting of network activity based on actual packet content auditing provides a quite different view of activity from what may be culled from server logs, firewall logs, profiling software or from intrusion detection systems. Unexpected and suspicious patterns of activity are often revealed through packet content auditing that otherwise would go undetected.

2) Monitor for network forensics and investigative purposes to establish a complete and permanent record of all activity on all addresses, an address range, or specific addresses. Once an investigation is initiated, it is essential to preserve as much evidence as possible. Monitoring and the preservation of evidence is an essential part of any specific investigative process and a requirement for network forensics.

3) Monitor outside the firewall to evaluate activity on known or unknown "holes" as defined within firewall control lists. Alternatively, specify the firewall address to the :BYPASS: function to discard all packets to or from the address of the firewall. Use of the :BYPASS: function in this manner outside the firewall would then highlight capricious or intrusive activity.

4) Use the :TRACK: function to monitor any Dial-In Point-to-Point Protocol usage. The tracking screen would then detail time of last activity, byte counts and peak concurrency associated with PPP usage. The tracking screen would highlight if any users are unnecessarily maintaining connection but doing nothing and thereby distorting capacity requirements. Tracking PPP sessions frequently reveals unusual and unauthorized usage.

5) Monitor local servers that are externally accessed using the NI-LAN :TRACK: function list to select specific IP addresses or an address range and monitor these servers with the Open switch set to open one session content file for each remote address.

(The Open switch determines when to open a session content file. Generally the Open switch is set to open a session content file upon the first reference to a local address and to keep one local session content file open until no packets are received for a period of time. The timeout period is specified by the setting of the TimeOut switch and is generally set to 5 or 10 minutes.

To emphasize remote address activity and to conveniently order the Report screen by time of remote address activity, the Open switch could be set to open a new session content file each time a new remote address references a server. With this Open switch setting a master file record and a session content file would be created for each exchange of packets between any server and each remote address. Because the Report screen displays record information from the time sequenced master file, any unusual remote address activity crossing servers is spotted. Filtering the Report screen to a suspect remote address would then provide a clear cross server time sequenced profile on the complete activity of that remote address. Moreover, all session content files reported out by setting a remote address filter would contain all packets exchanged between the remote address and the specific servers and only packets exchanged between that remote address and that specific server.)

Many monitoring applications become apparent once an initial NI-LAN system is installed and as system capabilities become known. NI-LAN systems are serious and highly evolved information hunter-gatherer systems. What is hunted for and what is actually gathered and retained is dependent on the setting of the twenty five (25) switches, the fifteen (15) configuration functions and the auditing or search information structure. This approach allows for quite efficient, specific and varied monitoring applications to be quickly defined.

Awareness Is Important

NI-LAN systems provide cognizance of what really happens on networks. Network activity is often different from what is considered possible, expected, or authorized.

The NI-LAN systems will be directly supportive of network security operations. Examples are outlined below:

The NI-LAN system software will assist security operations in identifying, understanding, and documenting attempted and successful access to root. When any intrusion event occurs, the NI-LAN system can filter to session files associated with targeted nodes. The packet-by-packet replay and review of the "method" of intrusion can then be understood and documented with subsequent implementation of an effective defense.

The NI-LAN will measure compliance to security requirements and regulations. Non-compliance and poor security practices can be culled and appropriate remedies applied. The NI-LAN identifies port probes. A tally of byte and packet counts by port since midnight, the time of last reference to each port and the source and destination address of the last packet to reference each port is displayed on the port activity screens. Unusual port activity associated with port probes are easily spotted on these screens.

Denial of Service attacks are identified. The NI-LAN tallies the number of flows that never complete the "three way handshake" within sixty seconds. The various real-time FAP (flow address pair) screens and the real-time Network screen alert to a denial of service attack. The completed session

Report screen reports all denial of service "sessions" to provide detail on the timing and address range of the attack. The various detailed packet replay and timing screens provide additional details required for criminal investigation.

The impact of an overnight virus can be evaluated. If a virus signature is entered as a search argument the NI-LAN will initiate a background search to identify local addresses that potentially received or transmitted the virus.

Securing Networks is a continuing multi-layered Process

It is expected that most large installations have an effective network security policy in place with multiple security mechanisms deployed. The subtle objective of monitoring is really to reveal surprises. In a perfectly ordered world where everything works as planned there is no reason to monitor. It is no surprise that surprises occur.

Perspective

Access through a network provides an economical method of connecting users with information they require.

The ubiquity of Internet access goes further to provide anyone a chance to access sensitive information from anywhere in the world. As a result, the potential for malicious, illegal or non-appropriate network activity has been substantially raised.

The use of networked resources has traditionally been controlled by access methods designed to balance risks to benefits. Many of these methods are sophisticated, some are effective, and a few are both usable and effective. However, all methods used to control access are prefaced on trust and assumptions. The trust is that "keys" are not shared inadvertently or otherwise. Trust is also extended that users only perform application functions that are authorized and appropriate to their duties. Assumptions are made about the risk associated with any remote connection and the impact of stolen or shared access keys.

Security managers have reluctantly adopted a modified access control approach to protect against the Internet. Firewalls, software and hardware encryption, and various sophisticated Internet access schemes are being implemented. However, this emphasis on access restriction as the cornerstone of network security policy is most incomplete and assumes that if unauthorized access is eliminated then the job is done. This is not the case and security violations continue to most frequently occur by someone that is known, someone that is trusted and someone that has a complete set of "Keys to the Kingdom" in hand.

Access rights and what people do are distinct issues.

Malicious, illegal or non-appropriate network activity using all the correct keys is still malicious, illegal or non-appropriate. Network security policy that concentrates on qualifying and restricting access to the exclusion of detection and review of potential security violations is most incomplete.

Something besides keys, assumptions and trust is required.

The NI-LAN system assists security managers in establishing and measuring compliance to an Internet use policy which promotes network security while

encouraging responsible and productive use of the Internet. Mark Twain quipped "Conscience may just be concern that somewhere, someplace, somebody may be watching". If he was right then the best deterrence to inappropriate network usage is probably to make personnel aware that monitoring does really occur and that tools are in place to measure compliance to network usage policy.

Where do you think they will go tomorrow?

NI-LAN System Salients

The Network Intelligence System model NI-LAN is designed to provide an integrated approach toward securing, planning for and managing inter-networking communication routers and gateways. The NI-LAN provides the following functions or features:

- 1) 10/100 mbps connection to an Ethernet segment.
- 2) real-time monitoring on up to 1000 concurrent sessions.
- 3) complete data capture of all packets on all sessions.
- 4) five classes of cumulative session file filtering.
- 5) real-time session security auditing.
- 6) real-time security alerting and reporting.
- 7) real-time identification of server access.
- 8) real-time display of remote and local IP address.
- 9) NIC address associated to all local IP addresses.
- 10) real-time display of active sessions.
- 11) replay display of active sessions.
- 12) replay display of completed session.
- 13) background session security auditing and searching.
- 14) account reporting by IP address.
- 15) automatic IP address naming.
- 16) audit reporting by IP address.
- 17) capacity planning measurement and reporting.
- 18) Ethernet Protocol Type accounting and reporting.
- 19) IP Port accounting and reporting.
- 20) Historical trend information on Port and Protocol Usage
- 21) Removable disk drive.
- 22) Surrogate System processing.
- 23) Archival/Retrieval.