Fighting Virus and Hack Attacks with a Network Analyzer
By Charles Thompson, Senior Systems Engineer for Network Instruments, LLC

Summary

This article shows how a network analyzer, historically used for network troubleshooting, can also be used to defend against the security threats. Certain features of a network analyzer can be set to monitor for virus and attack signatures and offer quick ways of isolating infected systems. For those organizations that are looking to invest in a network analyzer there are certain key features that should be considered.

Introduction

Chances are, your IT toolbox already contains a network analyzer. Historically, a network (or protocol) analyzer has been a great tool for troubleshooting network problems and monitoring for excessive bandwidth usage. But did you know a network analyzer can also fight virus and hack attacks? Along with keeping track of network devices and uptime, a network analyzer can also locate network security breaches and help identify and isolate virus-infected systems. It’s very easy to use your current analyzer to enhance your network security. But which analyzer features are essential for this task? The purpose of this article is to explain how an analyzer can augment firewalls and other perimeter defenses.

How Network Analyzers Work

A network analyzer shows you what is happening on your network by decoding the different protocols that devices on the network use to communicate, and presenting the results in human-readable form. Most mature analyzers also include some statistical reporting functionality. By watching network traffic, understanding bandwidth utilization, and reviewing connection dynamics, administrators can easily determine what station is causing the problem and why.

Protecting Against the Unknown

Every administrator of a corporate LAN of any size these days has already built strong defenses against hackers and virus attacks. But the viruses and hackers continue to get through. Why? Anti-virus and IDS systems are designed to prevent the incursion of known viruses and attacks. The hackers and “script kiddies” have the same access to all the threat bulletins and Windows patches that you have, and are always looking for the new vulnerabilities. In short, your firewalls and operating systems often won’t get a patch until the damage is already done. Imported disks, deliberate actions by employees, and visitors bringing infected laptops are some other weak spots in your security system that perimeter defenses alone cannot address.

Educational institutions are particularly vulnerable because of the tremendous variety of hardware and software platforms they must support. For example, systems and network administrator Nellie Shelton at the Presbyterian College in Clinton, South Carolina, uses a network analyzer to monitor and troubleshoot over 15 different VLANs. Over 90% of students live on-campus within 15 different residence halls. Students bring in a variety of computer hardware and software to connect to the campus network. As a result, University campuses offer large security concerns.

“Educational institutions offer very different challenges to a network administrator,” explains Shelton. “At most places of business, the hardware and software systems offered to an employee are already agreed upon by the IT department. Here, we have no control over what systems, devices or applications are brought into the network. It’s a unique situation.”

Using a Network Analyzer to Find and Isolate Infected Systems
In the case of a security breach, a network analyzer can save valuable amounts of time in locating a virus. How does this work? Viruses and hacker attacks typically generate a recognizable pattern or "signature" of packets. A network analyzer can identify these packets and alert the administrator to their presence on the network via email or page. Most analyzers let you set alarms to be triggered when a particular pattern is seen. Some analyzers can be programmed to send an email or page when these conditions are met. Of course, this assumes that the virus and its signature have been seen before and incorporated the analyzer’s list of packet filters. (A filter specifies the set of criteria under which an analyzer will capture packets or trigger an alarm or some other action.)

New viruses and worms have different signatures depending on the vulnerabilities they are trying to exploit, but once systems have been successfully breached, there are a relatively small number of things that hackers actually want to do with your network, the top ones being:

- Use your systems in a Denial of Service (DoS) on a third party. A good network analyzer can easily identify such systems by the traffic they generate.

- Use your system as an FTP server to distribute “warez” and other illegal files. You can configure an analyzer to look for FTP traffic or traffic volume where it is unexpected.

The very nature of viruses and worms is to produce unusual levels of network traffic. High frequency of broadcast packets or specific servers generating an unusual number of packets are logged in the analyzer’s record of longer term traffic, allowing the administrator to follow up on suspicious traffic patterns. The analyzer can also help in identifying inappropriate traffic which may leave your network open to attack, or may signify potential weaknesses. This would vary with the particular network or corporate policy, but could include automatic notification of traffic such as MSN, NNTP or outbound telnet.
Which Analyzer Is Right for Your Network?

To be useful as a corporate security tool, the analyzer must be “distributed” so that it covers all the areas of your network. It must also be able to capture and decode all of the protocols from all of the media (Ethernet, WAN, 802.11, etc.) on which your corporate data flows. The other crucial feature is flexible filtering that allows triggered notification. A network analyzer can only capture and decode the information that it can “see.” In a switched network environment, an analyzer is only able to see traffic local to the switch. To overcome this, most modern analyzers are supplied with multiple agents or probes that are installed on each switch in the LAN. An analyzer console can then query the probe for either raw packets or statistical traffic reports. When an analyzer is used in a general troubleshooting or monitoring mode, it is nice to have as much visibility as possible. When used in a protection mode, the visibility is vital. So – the more distributed the analyzer, the better. The distribution needs to be reviewed in both qualitative as well as quantitative terms. Look for an analyzer that can install probes or agents on the topologies present within both your existing network, and any planned enhancements. Look not only for Ethernet capabilities, but WAN and wireless capabilities if these are either present or possible additions.

Application analysis is important because a rapid increase in volumes of email is one of the obvious signs of many viruses. A final consideration would be the method of data transfer between the probe and the analyzer’s console or management station. The transfer of data must be minimal (to prevent unnecessary load on the network) and as secure as possible. Probe functionality is another important factor. They should be able to perform all the functions required by the organization – the capture and decode of packets, analysis of traffic levels both in terms of stations active as well as applications being used.

For example, when the Presbyterian College was attacked with a virus, Shelton turned to her probes to locate the infected devices on her VLANs. Her analyzer saved her valuable amounts of time in locating the network threat.

“Every year, before the dorms officially open, our football team moves in to begin training. One year, our network was severely impacted,” explains Shelton. “We had a virus. I had to then go into every dorm and manually look for the infected system. I spent all of August and September searching for a worm. It was a process of burning CDs, going back to my office and looking through the information. With my network analyzer it would never have taken that long.”
Using Network Probes for Increased Visibility

Probes need to be placed where they can see the critical points of the network. These would include the network’s default gateway (since all broadcast packets and all packets with unknown destination addresses will be sent here), the E-Mail server(s) and any other servers deemed as critical or likely to be attacked. In order for a probe to detect a certain device it will ideally be located on a hub onto which the device is also directly connected. If this is not possible – and the device to be protected is connected directly to a switch port, then the switch should be configured to mirror (or SPAN) all traffic from that switch port onto a separate switch port on which the probe is located. For continuous monitoring of viruses and attacks, probes must be implemented. More probes may need to be deployed if some are to be used for general monitoring, and some to be used for protection. Alternatively some analyzers are supplied with multi-function probes that can perform both tasks simultaneously. If you want to analyze WAN, WLAN, or gigabit traffic, you must choose a vendor with solutions for those media as well. Look for a solution that offers the ability to create your own traffic pattern filters as well as offering packaged filters for known viruses and hacker threats. Another thing to look for is the vendor’s willingness to offer timely updates as new security threats are discovered. A quick response to a breach can mean the difference between an inconvenience for a few users and a disaster for your company. Look for an analyzer that can be configured to email or page you when the virus or hacker attack is sensed. Most analyzers can tell you what machines are generating the most traffic, what protocols are taking up the most bandwidth, and other such useful information allowing you to detect attacks and infected systems. The most powerful analyzers have “expert” functionality available that looks at conversation threads and identifies more subtle problems (missing ACKs, high wireless re-association counts being two examples) automatically.

A Fresh Benefit for a Trusted Tool

As IT security becomes a larger concern for every organization, it’s imperative that IT departments are using every tool in their toolbox to fight the latest network threats. A network analyzer will never replace your firewall, anti-virus software or intrusion detection system, but it can certainly add to your line of defense. In choosing an analyzer, look for a comprehensive solution that covers multiple-topologies with distributed probes for visibility into all areas of your network. When used to its full capability a heavy-duty network analyzer is a trusted tool that can also offer additional protection for your organization.

About the Author

Charles Thompson, Senior Systems Engineer for Network Instruments, LLC, works with the Network Instruments Sales Organization to provide technical expertise and in-depth product information to enterprise accounts. Network Instruments is the industry leading developer of superior, user-friendly and affordable network management, analysis and troubleshooting solutions.