

NetworkComputing

Securing your network with in-depth analysis?

Network analysers are designed to observe the network, identify issues and alert administrators of problem scenarios. James Dunn, of Network Instruments, explains why these features make it an excellent security tool.

With the challenge mounting to secure an ever-expansive network, is it possible that the defences themselves become a source of vulnerability to the determined intruder? Perhaps there is help on hand from tools already available to the network manager. One such example is the network analyser, more commonly associated with analysis and troubleshooting.

Administrators already build strong defences against hackers and virus attacks on their (e.g.) wired networks, but many of their wireless networks are vulnerable, providing hackers with easy access to potentially wreak havoc. It is possible that an analyser can augment firewalls and other perimeter defences, keeping hackers at bay, thus adding a new and powerful line of defence.

Anti-virus and Intrusion Detector systems are designed to prevent the incursion of known viruses and attacks. However, hackers create thousands of new viruses and attempts to threaten networks, and if they have access to threat bulletins and Windows patches, they can easily find new vulnerabilities. Therefore, your firewalls and operating systems often won't get a patch until the damage from a hacker is done.

Imported disks, deliberate actions by employees and visitors bringing in infected laptops, can also harbour threats. The very nature of viruses and worms is to produce unusually high levels of network traffic. Viruses and hacker attacks typically generate a recognisable pattern or "signature" of packets. Network analysers can detect high frequencies of broadcast packets or specific servers generating an unusual number of packets, allowing the administrator to follow-up on the suspicious traffic patterns. Some analysers can even be programmed to send an email or page to an administrator when these conditions exist, so it can be acted upon immediately.

An analyser can also help in identifying inappropriate traffic that leaves 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.

To be a useful corporate security tool, the analyser must be "distributed" so that it covers your wired to wireless network. A distributed system includes consoles and probes to offer complete visibility. It must also be able to capture and decode all protocols and have flexible filtering that allows triggered notification.

Often in wireless networks,

companies will install an access point (AP), which is typically intended to give employees access to the network. However, depending on permissions and the level of encryption, some wireless networks may be providing access to everyone, including hackers, who may have a wireless NIC on their computer and be within range. If access is not limited, it's critical to use your network analyser to run a wireless site survey to understand who is accessing the network.

Wireless networking is prevalent in both corporate and domestic markets and its deployment is growing. A network analyser will never replace your firewall, anti-virus software or intrusion detection system. However, because it is not possible for these precautions to work as effectively on wireless networks as they do on wired networks, you cannot maintain the security of your network without a network analyser. A good analyser alerts you when the other defences have failed and takes much of the pain out of identifying, isolating, and cleaning up compromised machines.

Considering the general troubleshooting and monitoring features included "for free" in such tools, the decision to purchase a comprehensive analyser with network security features could be easily justified. **NC**

www.networkinstruments.com

