Four Free Tools that every Administrator should Know About

2011-07-20 00:28:09 by Southern

Microsoft Network Monitor
Microsoft Network Monitor is a network protocol analyzer that lets you capture, view, and analyze network traffic. Version 3.3 of Network Monitor is available in 32- and 64-bit versions.

Microsoft Baseline Security Analyzer
The Microsoft Baseline Security Analyzer (MBSA) is an easy-to-use tool designed to help administrators of small and medium-sized businesses ensure that their Windows-based computers are secure. You can use MBSA to determine the security state of your computers in accordance with Microsoft security recommendations. MBSA also offers specific remediation guidance for security problems it detects, such as misconfigurations and missing security updates.
At the time of writing this, the current version was MBSA 2.1. This version is available in 32- and 64-bit versions, but it does not install on Windows 7. A new version that supports Windows 7 is due to be released sometime in the future. You can download the current version and get information regarding the a version for Windows 7 at microsoft.com/mbsa/.

Microsoft IPsec Diagnostic Tool
The Microsoft IPsec Diagnostic Tool helps network administrators troubleshoot network-related failures, focusing primarily on Internet Protocol security (IPsec).The tool checks for common network problems on the host machine and, if it finds any problems, it suggests re¬pair commands. The tool also collects IPsec policy information on the system and parses the IPsec logs to try to determine why the failure might have happened. The tool also provides trace collection for virtual private network (VPN) connections, the Network Ac¬cess Protection (NAP) client, Windows Firewall, Group Policy updates, and wireless and system events. The diagnostic report generated by the tool is derived from the system logs collected by the tool during its analysis phase.

Windows Sysinternals Suite
The Windows Sysinternals Suite is a set of advanced tools for troubleshooting issues with Windows-based computers. These tools were originally developed by Winternals Software LP, which Microsoft acquired in 2006. Some of the useful and popular tools included in this suite are:

Autoruns This tool lets you see what programs are configured to start up automati¬cally when your system boots. It also displays the full list of registry and file locations where applications can configure autostart settings.
BgInfo This tool automatically generates desktop backgrounds that include important information about the system, including IP addresses, computer name, network adapt¬ers, and more.
Process Explorer This tool lets you find out what files, registry keys, and other

objects that your processes have open, which dynamic-link libraries (DLLs) they have loaded, and who owns each process.

Process Monitor This tool lets you monitor the file system, registry, process, thread, and DLL activity on your computer in real time.

PsTools This set of command-line tools can be used for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and performing other tasks.

RootkitRevealer This tool lets you scan your system for rootkit-based malware.

ShellRunas This tool allows you to launch programs as a different user using a shell context-menu entry.

TCPView This tool lets you view active sockets on the computer in real time.

[Technet Microsoft]
http://www.southernwolf.net//modules.php?name=News&file=article&sid=3101