Expert Guide to the Top Windows Security Tools

Businesses often lack the proper security tools essential for managing the myriad of security challenges associated with their Windows systems. In this expert E-Guide, brought to you by SearchEnterpriseDesktop.com and BeyondTrust, you will discover the security tools essential for effectively managing your Windows systems. Explore the critical role Microsoft Baseline Security Analyzer plays in security scanning measures. Learn why Sysinternal tools are essential for any organization's security initiatives and how they can be used in various security management scenarios. Gain insight into four pivotal Internet Explorer 8 Group Policy security settings.

TechTarget
The Technology Media ROI Experts

SearchEnterpriseDesktop.com E-Guide

Expert Guide to the Top Windows Security Tools

Table of Contents:

Why should Windows shops use Microsoft Baseline Security Analyzer?

Kevin Beaver, CISSP

We've all heard the adage, "something is better than nothing," and know how it holds true to information security. When I hear this saying, Microsoft's Baseline Security Analyzer (MBSA), a barebones security configuration scanner, comes to mind. Sure this tool may be best suited for small and medium-sized businesses, but it can help enterprises with necessary security scanning measures.

MBSA, now in version 2.1 is actually pretty decent. It not only tests for missing patches (what it's well-known for) but also uncovers other weaknesses in your Windows-based systems such as:

- Users in the Administrator group
- Open file shares
- Null sessions enabled
- Automatic Update status
- IIS lockdown status
- Login auditing status
- Blank or weak Windows and SQL Server passwords
- Weak Internet Explorer zone and Microsoft Office macros security settings

MBSA is free and relatively painless to run. You can download and run it on your local computer or, if you have administrative rights and are currently connected, run it against a single networked system or your entire network for that matter. To show you how MSBA works, I ran it against my network (Figure 1). As it turns out, it found some missing updates on my test system that I assumed were up-to-date -- after all, Automatic Updates were enabled.

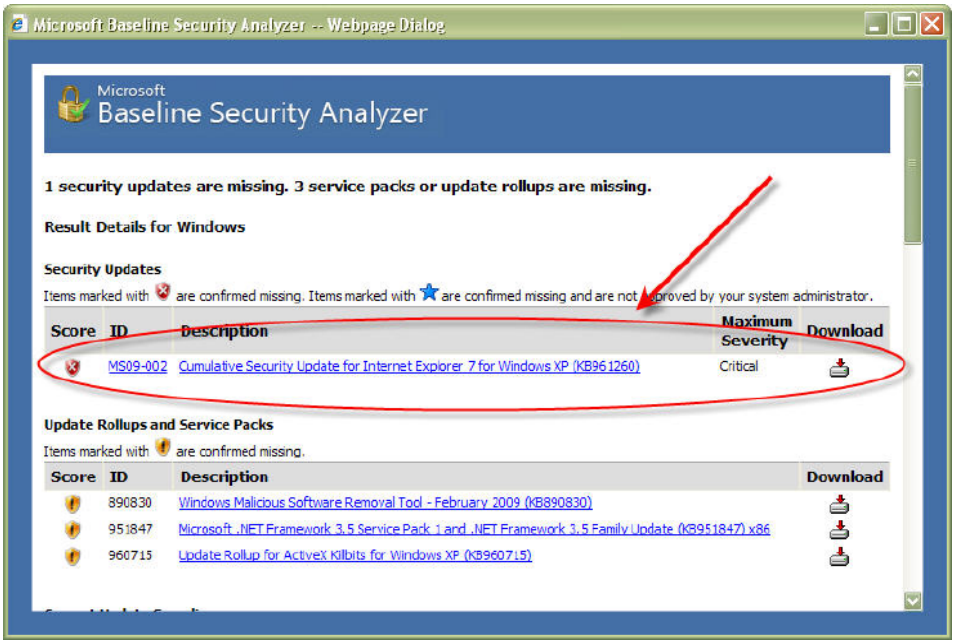

Figure 1 MBSA can highlight missing patches assumed to have been taken care of elsewhere.

This is a perfect example of how assuming your patches are current simply because you use WSUS, Automatic Updates, or third-party tool can really come back to bite you.

Yet, even with all of MBSA's positive traits, I have found some downsides:

1. MBSA is not a full-fledged vulnerability scanner that you can rely on to detect everything (never assume that just because MBSA has checked for the basics that you're in the clear).

2. MBSA is not a vulnerability scanner that's going to check for third-party software weaknesses, Web application flaws, or really anything outside of the out-of-the-box Microsoft-delivered realm (the source of many vulnerabilities in Windows).

3. MBSA is not a penetration testing tool that's actually going to exploit the weaknesses it uncovers (this requires higher-end commercial tools and, in many cases, some hacking know-how).

4. MBSA is not a tool that's going to generate fancy and easily-customized security assessment reports (they may be good enough for you but probably not enough for your managers, auditors, and business partners).

Despite these downsides, MBSA does provide a general security snapshot of your Microsoft systems. It highlights the low-hanging fruit and shows you where you're not following sound security practice – at least in the eyes of Microsoft. But, again, it's still better than nothing and a good starting point that I highly recommend if you've yet to test your systems for security vulnerabilities.

Mitigate 92% of critical Microsoft vulnerabilities

It's easy – eliminate admin rights with BeyondTrust

Increase Security, Reduce Cost

A review of all vulnerabilities documented in last year's Microsoft Security Bulletins shows that configuring users to operate without administrator rights can mitigate the effects of 92 percent of critical Microsoft vulnerabilities[1]. This increased protection comes with the added benefit of a 24% decrease in IT labor cost per desktop[2]. Achieve all this in one simple step — adopt a strategy of Least Privilege security with BeyondTrust.

Least Privilege Management

BeyondTrust enables enterprises to easily move beyond the need to trust users with administrator rights by elevating privileges for authorized applications, system tasks, and approved software and ActiveX installations without end user input, pop-ups or consent dialogues. Empower your network administrators to manage this security policy from within Microsoft Group Policy. Secure your Active Directory network today!

For a free pilot installation contact us at 1.603.610.4250 or visit www.beyondtrust.com.

[1] Obtain a copy of the free report at www.beyondtrust.com/mitigatevulnerabilities
[2] "New Report Shows 92 Percent of Critical Microsoft Vulnerabilities are Mitigated by Eliminating Admin Rights", February 3, 2009, http://www.businesswire.com/news/home/20090203005227/en

Sysinternals tools: A must-have for every Windows security toolbox

Kevin Beaver, CISSP

I love cool software tools. They not only satisfy my gadget fixation, but also help me in my work. While I have used many tools over the years, the one that stands out as my favorite is the Sysinternals toolset.

Originally a standalone toolset, written and hosted by Mark Russinovich and Bryce Cogswell, Sysinternals was acquired by Microsoft nearly three years ago. I shuddered at the thought of the acquisition. I even hurried to do a quick download of the tools in case they were suddenly unavailable. Fortunately, Microsoft has mostly left things alone, and in many cases, they have made them better.

The Sysinternals tools are broken down into four major categories: File and disk, networking, security and miscellaneous. There's hardly anything you can't do with these programs to manage, hack or otherwise probe a Windows-based PC. Having worked on assembly language programming early in my career to control PCs in every way imaginable, I have an innate need to delve into the system innards of Windows quite often. These tools allow the user to do things that Microsoft doesn't build into the operating system by default, and you can't really get their functionality anywhere else.

A note of warning: With the power Sysinternals tools bring to the table, they're not for everyone. In fact, used incorrectly, these tools can really jam up a system -- so proceed with confidence and caution.

The specific Sysinternals tools that have helped me over the years are:

- **AccessChk and AccessEnum:** Used to enumerate Windows user rights and privileges
- **Process Explorer (the most popular of them all):** Used for probing Windows processes and killing hung ones that Windows Task Manager can't seem to handle
- **Process Monitor:** For monitoring real-time file, registry, etc. activity
- **PsTools:** To control remote Windows systems
- **RootkitRevealer:** For finding Windows-based rootkits
- **ShareEnum:** For enumerating Windows shares on the network
- **TCPView:** To determine what's using specific TCP connections

And here are a couple of other gadgety-type tools that may help you:

- **DiskMon:** A hard disk activity light which comes in handy for troubleshooting things on computers that don't have one
- **ZoomIt:** For zooming in and marking up presentations

Don't want to mess with downloading and unzipping the entire Sysinternals suite to your system? Visit live.sysinternals.com where you can download individual tools quickly and easily. I especially like the Sysinternals Utilities Index that describes the purpose of each tool (which I sometimes forget) as well as provides a link to the download and usage page for each tool.

If you take Windows administration and security seriously, you must familiarize yourself with the Sysinternals tools. I'm still amazed at how many IT professionals haven't heard of or use them in their daily work. So go ahead, download these tools and explore what they have to offer. Once you see what they can do for your day-to-day management and troubleshooting duties in Windows, you'll realize you can't function without them.

Using Sysinternals tools in security management scenarios

Kevin Beaver, CISSP

By now most Windows shops understand how using Sysinternals tools can help streamline daily management tasks. To further demonstrate the power and benefits of these tools, let's explore three security management scenarios you're likely to come across when administering Windows systems, and show how Sysinternals can work for you.

1. Scanning for open network shares that users have haphazardly enabled
2. Monitoring system activity during a suspected intrusion or malware infection
3. Analyzing TCP sessions to determine who's talking to what and vice versa

Be forewarned that you shouldn't jump in head first with Sysinternals tools. I suggest you read the documentation that comes with each tool and proceed with cautious enthusiasm. These tools are not for the faint of heart. They aren't difficult to use, but you may end up making Windows do more than you intended and crash your system or lose important data.

Scenario 1: Scanning for open network shares that users have haphazardly enabled

I've noticed that users often take advantage of the power of networked computers and file sharing. While this function can serve a legitimate purpose, it can be easily exploited by users with malicious intent. By using the ShareEnum tool, you can put a stop to this unnecessary sharing out of directories and files to those who don't need access. Proceed as follows:

1. Load the program
2. Enter an IP address range or Windows domain to scan
3. Click "refresh"

This tool will uncover open shares that everyone and every group has access to, similar to my findings in Figure 1.

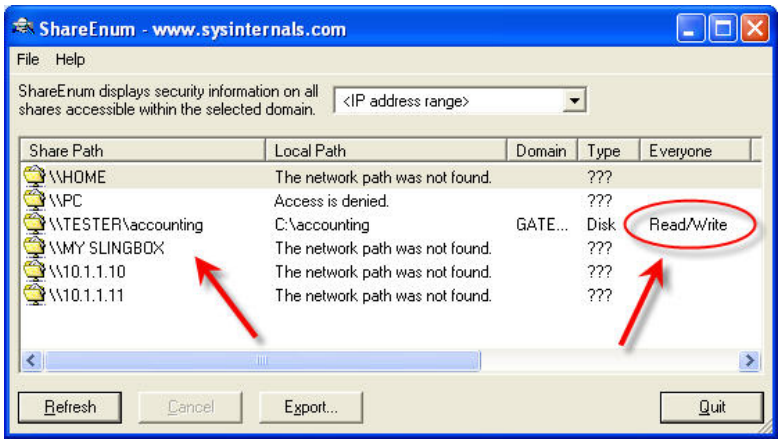

Figure 1 Using Sysinternals' ShareEnum to enumerate open and exposed network shares

Armed with this information, you can revoke unnecessary rights and lock down your sensitive files. If you would like to check access rights to directories, files or even registry keys on a specific system, then check out the similar AccessEnum tool.

Has someone or something compromised one of your Windows systems and you want to see the activity under the hood? Formal forensics methodologies aside, you can download and run Sysinternals Process Monitor, which shows you anything and everything taking place on Windows systems from registry access to file writes to network connections and beyond as shown in Figure 2.

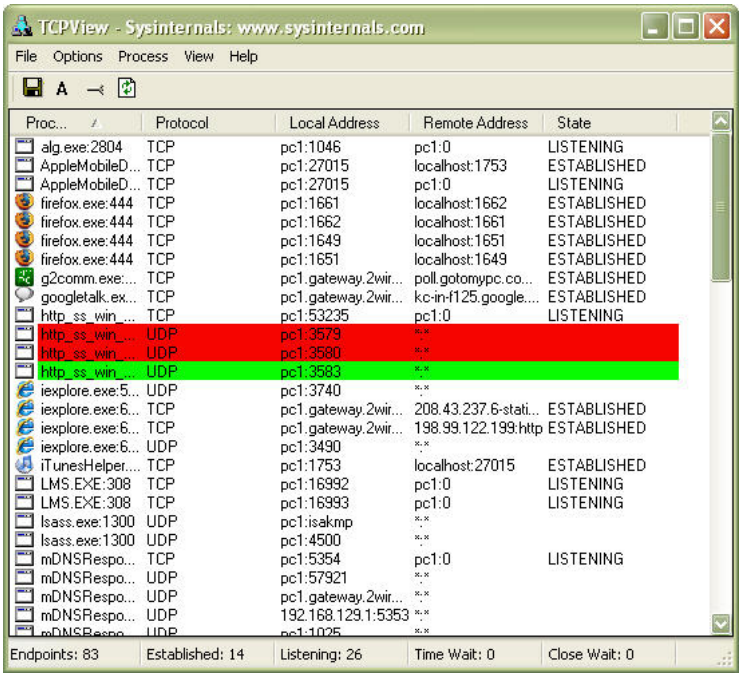

Figure 2 Using Sysinternals' ProcessMonitor shows exactly what's going on in Windows at any given time.

With its filtering and logging capabilities, as well as process tree exploration (similar to that in Process Explorer), Process Monitor allows you to do things that typically only very advanced people would dare to try or advanced tools would allow. The best part: Process Monitor is free. After running Process Monitor and experiencing first-hand the benefits this tool provides, you'll understand why Microsoft acquired Sysinternals.

Let's say you have a system acting up, transmitting and receiving a lot of network packets but you don't know where they're headed or coming from. You may also be curious about what application or process is generating the traffic. This would be a perfect scenario in which the Sysinternals TCPView tool would be useful. As shown in Figure 3, TCPView can drill down to help you monitor and troubleshoot both TCP and UDP connections in a happy-clicky-GUI fashion without having to do it the archaic way by using netstat –an from a command line.

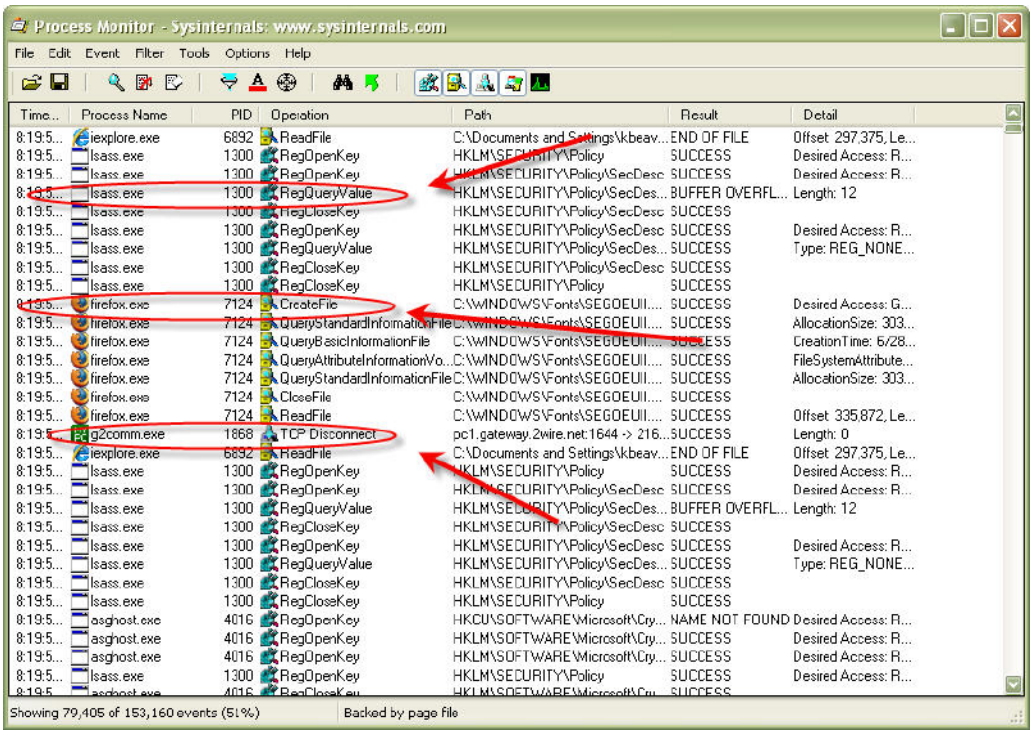

Figure 3 Using Systinternals' TCPView to analyze Windows-based network communications.

The possibilities for using the Sysinternals tools are unlimited, so check out what Microsoft has to offer in this gem of a toolset. The tools mentioned in this tip are, most often, my personal choice in security-related scenarios. However, you won't want to overlook the value of PsTools and the utility of BgInfo. (On a side note: The humor of BlueScreen -- what a clever prank for April Fools' Day. We've got to have fun to take the edge off, right?)

Four Internet Explorer 8 Group Policy security settings

Brien M. Posey

For many years, Microsoft has given us the ability to lock down Internet Explorer using Group Policy settings. With more than 1,300 Group Policy settings that can be applied to Internet Explorer 8, I can't possibly cover all of them, so here are four security settings that I think are worthy of highlighting.

Note: I only list partial paths for the Group Policy settings because most of these policies can be applied at both the user and machine levels of the Group Policy hierarchy. To find the policy settings that I will be discussing, look under either *Computer Configuration* \ *Administrative Templates or User Configuration* \ *Administrative Templates* within the Group Policy Object Editor.)

The SmartScreen Filter

The biggest new Internet Explorer 8 (IE8) security feature is the SmartScreen Filter. The SmartScreen Filter is essentially an enhanced version of the phishing filter that debuted in Internet Explorer 7.

The SmartScreen Filter is a reputation-based anti-malware component that is designed to complement traditional anti-malware software. As you may be aware, more and more cases are emerging in which malicious files are being posted on otherwise safe sites, such as social networking sites. As such, Microsoft designed the SmartScreen Filter to identify and completely block websites that are known to be malicious or to block only the malicious portion of an otherwise safe site. The SmartScreen Filter can be used to monitor file downloads as well.

The Group Policy settings that control the SmartScreen Filter are as follows:

Policy Name	Location
Prevent Bypassing SmartScreen Filter Warnings	Windows Components\Internet Explorer
Turn Off Managing SmartScreen Filter	Windows Components\Internet Explorer
Use SmartScreen Filter	Windows Components\Internet Explorer\Internet Control Panel\Security Page\ (There is a separate SmartScreen Filter setting for each Internet Explorer zone).

Data Execution Prevention

One of the most common types of attacks against Windows, over the last several years, has been a buffer overflow attack. Generally speaking, this type of attack works by inserting malicious code into an unchecked buffer, causing that buffer to overflow into other memory space, where the malicious code can then be executed.

Windows Vista protects against this type of attack by using Data Execution Prevention. Using this feature, Windows knows which memory areas code should and should not be executed in and takes steps to prevent code from running in memory locations that should be off limits.

Data Execution Prevention has been used by 64-bit versions of Windows Vista from the beginning, but Internet Explorer 7 was somehow exempt because of compatibility issues. Internet Explorer 8 resolves these problems and adds Data Execution Prevention capabilities to the browser.

Data Execution Prevention is enabled by default and enabling it at the higher levels of the Group Policy hierarchy may prevent future malware from disabling it at the local computer level. The following Group Policy setting controls it:

Policy Name	Location
Turn Off Data Execution Prevention	Windows Components \ Internet Explorer \ Security Features

InPrivate Browsing and InPrivate Filtering

InPrivate Browsing is a new feature that protects the user's privacy. When the user enables InPrivate Browsing, Internet Explorer opens a new browser window and does not record the Web pages that are viewed or any searches that are performed during that session.

InPrivate Filtering is a similar feature. It gives users a choice as to the types of information that websites can use to track the user's browsing habits. Like InPrivate Browsing, InPrivate Filtering must be enabled and only applies to the current session. The Group Policy settings that are related to InPrivate Browsing and InPrivate Filtering are as follows:

Policy Name	Location
Prevent Deleting InPrivate Blocking Data	Windows Components \ Internet Explorer \ Delete Browsing History
Turn Off InPrivate Filtering	Windows Components \ Internet Explorer \ InPrivate
Do Not Collect InPrivate Filtering Data	Windows Components \ Internet Explorer \ InPrivate
InPrivate Filtering Threshold	Windows Components \ Internet Explorer \ InPrivate
Disable Toolbars and Extensions When InPrivate Filtering Starts	Windows Components \ Internet Explorer \ InPrivate
Turn Off InPrivate Browsing	Windows Components \ Internet Explorer \ InPrivate

Suggested Sites

The Suggested Sites feature isn't a security feature, but I felt I should address it anyway. When you enable the Suggested Sites feature, Internet Explorer suggests other websites that the user might enjoy based on the sites that they have visited.

Several websites have raised privacy concerns over this feature because of the way it transmits your browsing history and your IP address to Microsoft for analysis. There have also been allegations that this feature might someday be used to serve targeted advertising, although Microsoft denies these claims. The following Group Policy setting controls the Suggested Sites feature:

Policy Name	Location
Turn On Suggested Sites	Windows Components \ Internet Explorer (This setting only applies to the user configuration.)

If you would like to see a more comprehensive list of the policy settings that are available, check out the Microsoft TechNet article Group Policy and Internet Explorer 8.

Resources from BeyondTrust Corporation

Eliminate Admin Rights - Learn more about BeyondTrust Privilege Manager

Locking Down Desktops by Applying the Security Best Practice of Least Privilege

How to Build a Secure and Compliant Windows Desktop

About BeyondTrust Corporation:
BeyondTrust Corporation, a pioneer in Least Privilege Management, enables enterprises to move beyond the need to trust users with excess privileges or administrator passwords. BeyondTrust solutions provide protection from zero-day threats, data theft, and malicious use.

BeyondTrust Privilege Manager was the first product to enable the security best practice of Least Privilege in Windows environments by allowing administrators to assign end users permissions to required or selected applications. Least Privilege strengthens security by limiting users to the permissions they need to do their jobs. Hundreds of organizations worldwide in industries such as financial, healthcare, government and military rely on BeyondTrust Privilege Manager to secure their enterprises. BeyondTrust is a Microsoft Gold Partner.