Global Knowledge®

Expert Reference Series of White Papers

10 Network Security Tools and Tests Everyone Should Use

1-800-COURSES www.globalknowledge.com

10 Network Security Tools and Tests Everyone Should Use

James Michael Stewart, Global Knowledge Instructor, CISSP, CEHv3-8, CHFIv3-8, Security+

Introduction

At this point, everyone should be aware that security management is essential for everyone. Whether you are operating a home system, overseeing a small startup, or performing security governance for an enterprise, everyone can benefit from paying attention to security. I won't delve into the security basics here, such as:

- Always operate your computer as a regular user account, rather than an administrator
- Have a firewall on every system
- Keep your anti-malware and anti-spyware scanners up to date
- Avoid risky activities, such as opening attachments and downloading files from unknown sources

I assume that you have already addressed these concerns and want to know the next steps in the pursuit of a more secure computing system. To that end, I'm sharing a list of 10 security tools or security tests that everyone should know how to use. These are products and services that will assist you in confirming that your security is robust, checking out suspicious issues, and keeping ahead of new risks and threats.

Note: Most of the tools I recommend are Windows only. If you know of Mac or Linux solutions that offers similar functionality, please send me a message. Also, most of the items I list are free. Some have paid versions you might consider if you discover the free version is indispensible.

Nessus Home

Once a system has been updated, configured, and otherwise "secured," the next step is to test and evaluate the established security. There are a wide range of security scanners and vulnerability assessment tools available. One of the best is Tenable's Nessus. For personal use, Nessus Home is free to use to scan up to 16 systems. Nessus Home offers a thorough security scanner, which assesses configurations, patches, malware, mobile devices, and more. The commercial version of Nessus is suitable for scanning enterprise networks. The Nessus Home product is just as robust, but not overly complex. The scan reports from Nessus are amazingly detailed. By following up on each issue discovered by Nessus Home, you are sure to improve your overall security stance.

To check out Nessus Home for yourself, visit: http://www.tenable.com/products/nessus-home.

VirusTotal

Everyone encounters suspicious files from time to time. Files from unknown sources or that could be infected by malware. There are a number of online virus scanning services. Of these, VirusTotal is one of the best. To quote their own description, " VirusTotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans, and other kinds of malicious content detected by antivirus engines and website scanners."

VirusTotal maintains about 50 malware and spyware scanners, which you can use to check out files. You can either upload a file from your local system or provide a URL to a questionable file. In either case, VirusTotal will perform a real-time scan of the suspicious file and provide you with the results. You can use this free online service to keep your infection risk low. Since only a single real-time scanner can be run on your own local machine, having 50 scanners available for use is an invaluable asset. The range of different detection engines, scanning features, and custom definition databases amongst the wide range of anti-malware products can be brought to bear without having to maintain dozens of separate systems yourself.

If you have a file that you think might be infected, toss it up to https://www.virustotal.com/.

Secunia PSI

Keeping current with patches and updates across all of the software on a computer can be quite challenging. Your operating system typically will automatically download and install new updates (a few of your applications likely do this as well). But not every installed application is able to auto-update. Those that do often run an additional background service that periodically checks for updates, but having dozens of these background services eats up system performance. I recommend replacing the one-off updater services with one solution that will keep all products current across your entire computer. That tool is Secunia PSI.

Secunia PSI (personal software inspector) regularly scans your system for applications, and then checks those applications against their available versions. If a new or updated version is available, Secunia PSI can automatically download and install the update or just notify you of its availability.

To give Secunia PSI a try, visit: https://secunia.com/vulnerability_scanning/personal/.

Note: Secunia PSI does not automatically replace the per-app background checkers. You will need to manually uninstall or disable those. For that, check out Autoruns. Also, if you want a way to keep track of hardware drivers, consider Driver Booster at http://www.iobit.com/driver-booster.php. This tool can detect outdated drivers and assist in downloading and installing the latest versions.

Autoruns

The process task list on a typical computer includes dozens of applications and services. Many of these are not essential to your normal activities or the software products they are associated with. Background updaters, speed boosters, pre-loaders, etc., all get installed when you install or update applications, and then these little "helpers" launch at each system reboot. These unnecessary components slow boot time and consume system resources, often making your computer act far below optimum performance levels. The solution is to remove or disable the offending items. The tool I recommend for this is Autoruns.

Autoruns is a tool offered by Microsoft. It was created and is maintained by Mark Russinovich and Bryce Cogswell (formerly of Sysinternals, before being acquired). Autoruns scans your system for all of the things that get launched at bootup or login. You are presented with an organized list of items. You can select the disable any item or to completely remove an item. I recommend disabling items first, then test that the element isn't actually needed. In most cases, leaving items disabled is sufficient. If you determine that an item needs to be completely removed from your system, then you can opt to delete it. However, the deletion only removes the Registry elements that cause the auto-launching, it does not remove or uninstall the item from the system overall.

To start using Autoruns, visit: http://technet.microsoft.com/en-us/sysinternals/. Grab the Sysinternals Suite, which includes Autoruns plus many other excellent free utilities.

Keep in mind that blindly disabling items on your system can result in system failures or applications that fail to operate properly. So, take the time to research every element before you elect to disable it. You can gain some greater understanding of what is on your system and what is suspicious with any of the tools in the next section.

CrowdInspect, Should I Remove It?, and Soluto

Knowing what a program is that is running on your company can be a challenge. What is it? What does it do? Is it malicious? Do I even want it? Should I remove it? Answers to these questions are not too far away. There are many tools that can help in this regard, my favorites are: CrowdInspect, Should I Remove It?, and Soluto.

CrowdInspect pulls data from VirusTotal, the Malware Hash Registry (MHR) (https://www.team-cymru.org/Services/MHR/), WOT (Web Of Trust) services (https://www.mywot.com/), and from its own monitoring of malicious injection activities. With this range of detail, you can quickly discover unwanted operators on your system. Visit: http://www.crowdstrike.com/crowdinspect/.

Should I Remove It? focuses on detecting unwanted software, such as adware, spyware, toolbars, malware, and unwanted applications. In the pursuit of removing bloatware and crapware, this tool quickly identifies those applications you want of your system fast. Visit: http://www.shouldiremoveit.com/

Soluto is a utility that assists in a wide range of system improving operations. This includes update and patch management, identifying unwanted software items, tracking crashes and unresponsive applications, delaying auto-launching applications in order to improve boot time, adjusting which programs launch automatically vs. launch only when requested, monitoring of Web browser add-ons, and more. Visit: https://www.soluto.com/

ShieldsUp

ShieldsUp is a free online service for testing your firewall and how exposed you are online. ShieldsUp operates from the Gibson Research Corporation's website (https://www.grc.com/), and offers a quick assessment of your attack surface as exposed online. Go test your system and find out what hackers can see when they network scan your IP address. Follow the recommendations to improve your security and lock down your vulnerabilities. The ShieldsUp service is found at https://www.grc.com in the Services menu.

While at GRC, you might want to explore the other amazing tools and services, such as DNS benchmark, HTTPS Fingerprinting, and SpinRite.

Malwarebytes and HijackThis

Often your anti-malware scanner just isn't enough. Using advanced supplemental tools to detect and remove malicious code is an essential part of being an Internet user. Two great tools to have on hand are Malwarebytes and HijackThis. These tools can usually operate on your system concurrently with an existing real-time anti-malware scanner present, a feature which is not true of many malware products. Whenever you suspect an infection or if you think you have inadvertently performed a risky activity, and your anti-malware scanner is staying suspiciously quiet, run one of these tools to discover if your fear is justified. Malwarebytes can be found at: https://www.malwarebytes.org/. HijackThis is available from: http://www.hijackthis.com/.

NoScript and ScriptSafe

Surfing the Internet has become a dangerous activity. If you are using a Web browser with default configuration, you are vulnerable to a wide range of exploitations and attacks. Most of these issues are due to the fact that most Web sites transmit mobile code to Web browsers for client side execution. While most of this code is safe and benign, there is no way for an end user to know when malicious mobile code is being offered until it is too late (i.e., it is already running on the user's system). The only way to mitigate this risk is to disable client-side execution of scripts and mobile code. While this can be done in most browsers directly, it can be difficult and it usually applies universally. A better solution is to use a browser extension that adds quick access to a range of features including being able to target the settings on a per site basis. For Chrome users, the tool ScriptSafe is a great choice. For Firefox users, the tool NoScript (http://noscript.net/) is the clear leader. These tools can be quickly located in their respective browser's extension/add-on marketplace.

Note: If you are using a different browser, switch to Chrome or Firefox.

CCleaner

Just using your computer will cause a plethora of detritus to build up over time. This includes temporary files, histories, cached content, cookies, downloads, MRU (most recently used) listings, orphaned files, and stray registry entries. Some of this stuff is left over when uninstalling legitimate or malicious software. From time to time, performing a deep cleaning of your OS will result in improved performance. Try out this tool from: https://www.piriform.com/ccleaner

Pandora Recovery

Sometimes files get deleted by mistake. Important files. Files that you don't have backed up (you have a backup, right?). Fortunately, the standard delete function removes the directly listing and pointers to storage clusters, while leaving the actual file data in place. If subsequent write activities overwrite these "available" clusters, the data is lost. However, if you can attempt a reclamation of the lost file before the data is actually lost, the act of undelete may be possible. I've used Pandora Recovery several times to recover files. Try it yourself: http://www.pandorarecovery.com/

Bonus Tool: WDO

Sometimes your system will become infected by something that your native or standard detection and removal tools are unable to address. When you think you are in this situation, before giving up and low-level formatting or replacing hardware, try an offline scanner. Microsoft's Windows Defender Offline (WDO) is used to scan your system while the OS is not active. This can give the security scanner the boost it needs to detect and remove some of the nastiest forms of malware. Download WDO and install it on a spare USB drive, so you can be prepared: http://windows.microsoft.com/en-us/windows/what-is-windows-defender-offline.

Conclusion

It is everyone's responsibility to be more secure. Having the right tools helps you achieve better security. Be the IT expert for yourself on your home systems by using these tools to get a better handle on the security of your systems. And be on the lookout for other great tools to expand your security toolbox.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge through training.

Foundstone Ultimate Hacking: Web

CEH v8

Network+ Prep Course (N10-005)

Visit **www.globalknowledge.com** or call **1-800-COURSES (1-800-268-7737)** to speak with a Global Knowledge training advisor.

About the Author

James Michael Stewart has been working with computers and technology for over thirty years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and Security+. He is the primary author of *CISSP Study Guide 6th Edition*, *CompTIA Security+ Review Guide: SY0-401* (to be released Q2 2014), *Security+ Review Guide 2nd Edition* (SY0-301), *CompTIA Security+ Training Kit (Exam SY0-301),* and *Network Security, Firewalls, and VPNs*. Michael has also contributed to many other security focused materials including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds a variety of certifications, including: CISSP, CEH, CHFI, and Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in Philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants hands-on "street smarts" experience. You can reach Michael by email at michael@impactonline.com.