



# Global Information Assurance Certification Paper

Copyright SANS Institute  
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

## Interested in learning more?

Check out the list of upcoming events offering  
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"  
at <http://www.giac.org/registration/gsec>

Even though you may have seen or heard advertisements proclaiming Microsoft's Windows NT security as being "C2" compliant (visit link <http://support.microsoft.com/support/kb/articles/Q137/0/18.asp> for explanations of various security levels), an 'out-of-the-box' installation with the default security/permissions set, is far from meeting these requirements. Depending on the requirements for security within an organization, the level of security can vary widely from institution to institution. Another major factor, in determining the level of security that can be achieved with NT, are the effects that some software/application packages may place on the system.

This document will cover some issues not covered in the 'NT Security' course and offer a couple of suggested 3<sup>rd</sup> party applications that may help to simplify the process of 'plugging holes,' so to speak.

To begin tightening the security of your NT installation it is recommended that you visit Microsoft's website and read the following document.

[www.microsoft.com/ntserver/security/exec/overview/Secure\\_NTInstall.asp](http://www.microsoft.com/ntserver/security/exec/overview/Secure_NTInstall.asp)

This document indicates the procedures on changing permissions and making entries/modifications to the registry to help increase the security level on your NT system. {Another good resource is Microsoft's TechNet/Knowledge base}

In most all documents you'll read on NT security one of the first instructions is to rename the Administrator account and disable the Guest account (which is disabled by default). I like to go one step further to create a 'honey-pot' (A trap of sorts for would-be intruders). I'll rename both accounts and then create two new accounts with the original names ('administrator' and 'guest') and disable both of these accounts and assign them the right "No Access" to root directories. In User Manager, Policies, Audit (NT's Administrative Tools) I'll make sure to turn on auditing for login attempts and failures. When someone attempts to login as one of these users it will write an event to NT's 'Event Viewer' log file. This will at least notify me that someone is trying to 'knock on doors' so to speak.

After you've tuned your registry and tightened up the permissions on your system, it's time to probe it to look for vulnerabilities that you were either unaware of or missed by accident. With all of the exploits on Microsoft's systems how can one possibly keep up with them all? That is easy, you don't! Let someone else. One of the best tools I've discovered to do this is Webtrend's Security Analyzer (which a 30-day trial version can be downloaded at the following link:

[http://webtrends.com/site\\_download/wsad.htm?product=security](http://webtrends.com/site_download/wsad.htm?product=security) ) It's an excellent tool that does everything from password vulnerability tests, port scans, to user/group permission analysis. It also probes for known NT vulnerabilities/holes that haven't been patched on your system. One of the most exciting features is the 'AutoSync' feature that allows you to download the latest vulnerabilities and applies them to your security

profile/policy (which is defined in the application). This way you don't have to spend hours of searching and reading about the latest threats that have been discovered. After they are detected, you will have to manually fix or patch any holes. The only negative is you are relying on the accuracy of Webtrends to find and disclose new vulnerabilities through their patch.

These are basically software procedures that can be performed to tighten security, however it would also be good to include some hardware configuration issues. Over the past several years I've heard the argument to load the NT file system on a hard drive using the FAT file system. The reasoning behind this is if there is a problem with the operating system, you can always use a DOS boot disk to access it and make necessary modifications. This may be good if security isn't a factor; however, if you are concerned about security it would be highly recommended to install using Microsoft's NTFS. As mentioned in the "A Survival Guide For Windows NT Security,"<sup>(1)</sup> there is now a 3<sup>rd</sup> party (by [www.sysinternals.com](http://www.sysinternals.com)) called NTFSDOS that allows NTFS partitions to be accessed from DOS. Ideally the operating system installation would be performed onto a separate hard drive (from your data) and an additional safeguard would be to mirror this drive. The data drive/drives should also be installed using NTFS.

Now that your server is more secure than it previously was you should be able to relax, right? Wrong. Depending on how the workstations are configured in your environment a threat exists that can totally undermine any security you have placed on your servers. In a Microsoft Windows environment, have you ever noticed that in Windows 95 upon the initial login to a domain, or when you are forced to change your domain password, it appears as though the login screen comes up twice? Well one is for the domain and the other is for Windows 95 itself. If you initially use the same password for both, it will only look like your logging in once. However, in actuality you are logging into two different systems. Once into the Domain and the second into Windows 95. This occurs when you have your Windows 95 system configured to use 'user profiles.' The danger here is that if the two passwords are not different, the Windows 95 password can be sniffed off of the network in cleartext thus revealing the NT domain password. There are two ways to create a blank password for Windows 95. One is from a command prompt type `cd c:\windows` (or the location of your windows installation) and type `"dir *.pwl"` (without the quotes) this will provide a list of users that have logged into that particular machine. At this point you can delete all of the pwl files (`del *.pwl`) or just a certain user's pwl file. This is removing/deleting the Windows 95 password file. The next time you login to the domain a "change password" window will appear with asterisks (which is your domain password being carried forward) in the first line. Highlight and delete them so it is blank. The other option is to go into "Control Panel/passwords" and make it blank through there. The recommended solution is to disable 'user profiles' altogether. Otherwise you will ultimately be reliant upon your users to remember not to fill in the Windows 95 password window with their domain password. A similar article can be found regarding Windows 95 and Microsoft's Internet Explorer {See <http://www.security.org.il/msnetbreak/>}.

<sup>(1)</sup> Sans Institute, “A Survival Guide For Windows NT Security,” Windows NT Security Step By Step Version 2.15 July 30, 1999.

© SANS Institute 2000 - 2005, Author retains full rights.