Global Information Assurance Certification Paper

NT Security Todd Arnold

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 3rd party applications that may help to simplify the process of 'plugging holes,' so to speak.

To begin tightening the security of you 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
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) 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," [(1)] there is now a 3rd party (by 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/}.

[1] Sans Institute, "A Survival Guide For Windows NT Security," Windows NT Security Step By Step Version 2.15 July 30, 1999.

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event