Global Information Assurance Certification Paper

Abstract

Security is an important requirement of multi-user client/server environments. When you have a multi-user environment you don't want someone being able to modify someone else's files or log in as them. And you certainly don't want a user to be able to log in as the Administrator or make use of Administrator features. Whether their intentions are malicious is inconsequential, even mistakes can be devastating.

Security Overview

Physical security is maintaining the network's servers in a locked, secured room or building. Physical security also covers every aspect of the computer network, not just the servers. Cables, hubs, routers, client machines, etc. are all important to consider, and need to be protected from people who don't need to have access to them.

Password security is an extremely important aspect of security. Think of it like this: you could have the most secure server in the world being protected behind a bank vault with a network firewall surrounding it, but all of that may be worthless if a user's password is easy to guess (e.g., their username, name, a common word etc.).

User security is also extremely important. User security means keeping the user in their own little virtual world. If a user is kept within these confines they will probably not cause as many problems on the system as they would if they had free reign of the server. It is all too common to hear of stories where Joe in Marketing started browsing around the network and read some private letters that Judy over in Accounting wrote. For reasons like these, it is critical that you are aware and careful of who is added to the Administrators group. For that matter you also need to assure that the "everyone" group is not where it shouldn't be.

Network security is one of the biggest threats. Due to the wild growth of the Internet, network security has become a growing issue of system administers. With the popularity of the Internet, and the ease of getting on the 'Net, any sufficiently talented sixteen year old can break into a computer on the other side of the world from his bedroom.

Network security involves protecting the network from remote attacks by setting up firewalls, packet filtering methods, intrusion detection systems, and constantly checking the network for leaks.

NTFS offers many security related advantages over FAT. The FAT File system is used by DOS and is supported by all the other operating systems. It is simple, reliable, and uses little storage. NTFS provides everything. It supports long file names, large volumes, data security, and universal file sharing. If you choose to use NTFS over FAT be careful when using the convert utility when converting from FAT to NTFS. The "Everyone" group will have been given Full Control rights to all files and directories. You can use the *fixacls* utility available on the NT Resource Kit to restore the default permissions on the NTFS system files.

Protecting Your Windows NT Installation

It is very important to stay current with any security related Service Packs and Hot fixes released by Microsoft. There are several mailing lists that deal with Windows vulnerabilities and their associated fixes. Microsoft maintains a Product Security Notification Service mailing list for security related issues in their products. NTBugtraq also maintains a mailing list to discuss bugs in various products (these are not exclusively Microsoft bugs). You can also subscribe to ITSO-ALERTS mailing list.

Ensure Guest Is Disabled

The Guest account in NT can provide unauthenticated access to NT, and can open the door for a cracker trying to elevate his/her authority once logged on to the system. You should ensure that this account remains disabled.

Rename Administrator

"Administrator" is shipped as the default system administrator account on all NT systems and is the target of the majority of attacks against NT. By renaming this account, you are increasing the amount of information a person needs to know to brute force the administrator's password. Though it is relatively easy for a skilled cracker to find out the new username, this should help. It's also a good idea to create a "fake" Administrator account that is disabled and has no privileges just to see if someone is attempting a logon.

Renaming process

- **Rename** "Administrator" to "Your New Admin"
- Copy "Your New Admin" to "Administrator" (this will save the unusually long description of the original administrator account)
- give "Administrator" a complex 14-character password
- make "Administrator" disabled
- remove full name and description from "Your New Admin"
- give "Your New Admin" a complex password

Strongly Encrypt Security Database

The SAM database contains all your user account information (i.e. User name, password etc). To ensure that your SAM database is protected you may want to consider the following. These procedures illustrate how you can enhance the security of account password data by using SYSKEY.

Understand the options to store encryption keys using SYSKEY.

SYSKEY provides three ways by which to manage the SAM password data encryption key:

1. Store Startup Key Locally
   SYSKEY generates a random encryption key and stores it locally on the system SYSKEY generates a random encryption key and stores it locally on the system

2. Store Startup Key on Floppy Disk
   SYSKEY generates a random encryption key and stores it on a floppy disk that you provide. This key disk must be inserted every time the system is started.

3. Password startup

   With the password startup the "Administrator" selects the password whenever the system is started. The password is used to transmit the encryption key. There are many considerations to turning on the SYSKEY option. If you do choose to enable the SYSKEY option, make sure that have an up-to-date Emergency Repair Disk available. If you need to repair your system, you will need the ERD that corresponds to whether or not password data encryption was enabled using SYSKEY at the time repairs became necessary.

Account policy

Account policy settings control password and account restrictions. There are many recommended settings here is an example:

Maximum password age (60 days) means that the user will be required to change their password every sixty days. Minimum password age (1 day) means that the user will be required to keep their new password for at least one day before they can change it again. Minimum password length (7 characters) will require the user to have a password with no less than seven characters in length.

Password uniqueness (3 different passwords) means that the user is forced to change from a favorite password, and is not allowed to have that same password until they have used three unique passwords first, and even then when the age has expired they will have to change the password again. This ensures that the User is not using the same password over and over again. Account lockout after (4 attempts) means the account will automatically lock on the fourth bad logon attempt. This prevents brute force logon attempts. Reset count after (60 minutes) means the login failure count will be reset if the time between two login failures is more than sixty minutes and the account has not been locked. Lockout duration (forever) means unless an authorized administrator unlocks the account, the account will remain locked indefinitely.

Again these are only one choice of recommendations. You will have to analyze your network and decide what works best for your and their clients.

Audit policy

With NT, by default auditing is not enabled. Auditing is extremely important to have enabled. It adds the ability to track what the user is doing, and offers information for troubleshooting.

Minimal Recommended Settings

Both, success and failure should be logged for "Logon and Logoff," "User and Group Management," "Security Policy Changes," and "Restart, Shutdown, and System" events. The "Logon and Logoff" event is triggered when a user logs on or off, or makes a network connection. "User and Group Management" events occur when a user account or group is created, changed, or deleted; a user account is renamed, disabled, or enabled; or a password is set or changed. "Security Policy Changes" are represented by changes to the "User Rights", "Audit", or "Trust Relationships" policies. Finally, "Restart, Shutdown, and System" events mean occurrences where a user restarted or shut down the computer, or an event has occurred that affects system security or the security log.

Failures should be logged for "File and Object Access," and "Use of User Rights." "File and Object Access" events are generated when a user opens a directory or file or the user sends a print job to a printer. "Use of User Rights" events are logged when a user uses a user right other than those related to logon and logoff.

Disable Unnecessary Services, Protocols and Features

If you're not using a particular protocol on a server, like IPX/SPX or Net BIOS, unbind it from the network adapters it's bound to. This prevents denial-of-

service attacks against that protocol, improves your overall server performance, and safeguards you against protocol-specific exploits

The services that run under the "System" account are very powerful. It is recommended that you investigate all services running and eliminate all that are not needed. There are many services that need to be looked at with a critical security eye. The more you are able to eliminate the better your security is.

There are several optional components available when installing NT, like Internet Information Server (IIS). Refrain from installing anything that is not essential so that you are not vulnerable to unnecessary threats. Checking your software periodically and removing what is not needed is also a good idea.

Protecting your File system

Use NTFS

NTFS is far superior and offers security advantages over FAT. While FAT is simple and reliable, NTFS provides control over how you want your data secured. NTFS also supports long file names, large volumes, and most importantly SECURITY. If you have converted from FAT to NTFS you need to be aware of the default permissions, and change to what is appropriate for network.

NT creates a couple of hidden shares by default for remote administration (normally C$ and Admin$). Microsoft recommends disabling these shares if you can, but the reality of everyday administration and the requirements of various software packages will probably cause you to disregard this recommendation.

Below are a few of the common, default, NTFS permissions that you need to be aware of:\

C:\ Administrator-full control, Creator/owner-full control, Everyone-change, Server operators-change, System-full control

C:\%SystemRoot% Administrator-full control, Creator/owner-full control, Everyone-change, Server operators-change, System-full control

C:\%SystemRoot%\repair, Everyone-full control

There is a long list and as you can see these permissions are wide open. This does not apply to a drive that has been converted using the Convert utility. A converted NTFS drive opens files and directories with Everyone-full control as the default permissions. These examples above are only a few that show how

vulnerable you are without going back and setting up strict permissions that fit your security needs.

The Next Step

These are just a few of the things to consider when securing your NT 4.0 server. Implementing these steps would be a good start, but by no means should you consider your server secure by only following this overview. Entire books and courses address NT security and provide the necessary detail to secure your servers. Hopefully, this overview gets you started thinking about what makes an NT 4.0 server secure and will motivate you to pursue the information that will allow you to complete the job.

References:

"Default NTFS Permissions in Windows NT" Microsoft (December 6, 2000) www.Support.Microsoft.com/support/kb/articles/q148/4/37.asp

Randy Franklin Smith" Windows IT Security" (December 21, 2000) URL: http://www.windowsitsecurity.com/Articles/Index.cfm?ArticleID=16363

"The Sans Institute Windows NT Security Step by Step" Author (too many names to list) (version 2.15 July 30 1999)

Carnegie Mellon University "Selecting Audit Policy Settings on Windows NT 4.0 Servers revised: (March 17, 1999) URL://http://www.cert.org/securityimprovement/implementations/i041.05.html

Craig S. Wright "NT Security Issues" (January 15, 1999) http://www.demorgan.com.au/documents/nt-doco-index.html

"File permissions on the NTFS file system (June 7, 2000) http://www.Support.Microsoft.com/support/ServiceWare/NTServer/Nts40/371ILIOB.asp

"Directory Permissions (June 7, 2000) http://www.Support.Microsoft.com/support/ServiceWare/NTServer/Nts40/371ILJ9G.asp

Last Updated: May 29th, 2017

Upcoming Training

SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
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
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
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 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
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
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 Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event