ENTERPRISE NETWORKING

Windows NT Security Tips and Tricks

BY JOHN E. JOHNSTON

Many network administrators don't take the time to adequately address the security of their Windows NT servers. This can leave their network vulnerable to hackers and can also leave their data and programs exposed to accidental deletion by the end users. When Windows NT Server is installed, very few security measures are installed by the default installation. Security must be imposed by the network administrator.

More and more companies are connecting their internal networks to the Internet. Most of these companies will install a firewall to help prevent hackers from accessing their internal network from the outside. However, how sure can they be that the firewall is protecting their Windows NT file servers from being attacked by hackers?

This month's column will present several techniques that will help you gain control of the security of your Windows NT servers.

1. Don't install a service on your Windows NT Server if you aren't going to use it.

Certain services actually open holes that hackers can use to find information about your NT servers. For example, the SNMP service opens holes for SNMP probes to discover TCP/IP addresses of the critical components on your network. Do not install any service on your NT servers that you do not plan to use.

2. Use the SHOWACLS.EXE utility.

The SHOWACLS.EXE shareware utility from Somarsoft is a security auditing program for Windows NT servers. This utility produces easy-to-read reports that show the permissions established for your NT Server's file system, registry, printers and shares. These reports allow you to easily spot holes in your security setup. SHOWACLS.EXE can be obtained from www.somarsoft.com

3. Do not implement FAT disk partitions.

With Windows NT you can either implement FAT or NTFS disk partitions. NTFS partitions provide a much more robust security architecture for your file system. Unless you have a compelling reason to implement FAT partitions, you should opt to utilize NTFS partitions for all of your Windows NT disk partitions.

> When Windows NT Server is installed, very few security measures are installed by the default installation. Security must be imposed by the network administrator.

4. Utilize the Window NT auditing facility.

Learn how to enable and use the Windows NT Auditing facility. At a minimum, you should audit the following events:

- failed logon attempts
- repeated denied accesses to a resource
- system re-boots

5. Apply Service Pack 3 to your Windows NT 4.0 Servers.

Service Pack 3 for Windows NT Server 4.0 corrects several security exposures. If you have not already done so, you should implement Service Pack 3 on all of your Windows NT 4.0 file servers.

6. Rename the Administrator account.

Hackers love to gain access to your Windows NT Administrator account. Prevent hackers from attempting to gain access to your network by changing the name of your Administrator account.

7. Restrict physical access to your servers.

Restricting physical access to your file servers is one of the most important security measures you can take. If a hacker has physical access to your file servers, you are in trouble.

8. Remove the floppy drives from your servers.

There are two good reasons to remove the diskette drives from your file servers:

- There are utilities that a hacker can use to access your NTFS partitions. To use these utilities, the hacker must boot the file server from a diskette. If you remove the diskette drive, this attack is thwarted.

- If you accidentally boot your file server from a virus infected floppy, you may not be able to remove the virus without damaging the Windows NT software. By removing the diskette drive from your Windows NT servers, this exposure is eliminated. If you do find yourself in the awkward position of contracting a boot sector virus on your NT server, you can search the Microsoft Knowledge Base using the keywords "boot, sector and virus" for tips on removing the virus.

9. Apply post Service Pack 3 hotfixes if you have been attacked.

There are several security related hotfixes that were released after Service Pack 3. Most of these hotfixes address holes that hackers can use to cripple your Windows NT servers. The following Microsoft Knowledge Base articles describe these attacks and the corresponding hotfix:

```
Q179129
Q165005
Q143478
Q154174
A147706
```

A word of warning on applying hotfixes: If you apply a hotfix, Microsoft will not provide support for the Windows NT operating system on your server. Because of this dilemma, you should only apply hotfixes to your servers if you experience one of the hacker attacks that is corrected by the hotfix. All post SP3 hotfixes will be supplied in Service Pack 4 in the very near future. Microsoft will support these fixes when applied using Service Pack 4.

10. Use the Administrator account as a decoy.

If you suspect that someone is trying to hack into your system using the Administrator account, you can use this account as a decoy to attempt to track the hacker. Rename the original Administrator account, then create a new account named Administrator. Remove all access privileges and group memberships from the decoy Administrator account. You should then audit every action and all login attempts for the decoy account.

11. Try hacking your own system.

One of the best ways to find security holes in your network is to try to hack into it. Many computer hackers are bored, male high school students. Some companies will seek out and hire these students over their summer vacation specifically to have them attempt to hack into their computer networks in order to reveal any security exposures.

CONCLUSION

You can never completely secure any network but you can take steps to deter all but the most knowledgeable and persistent hackers. While the techniques presented will help you, this list is by no means all-inclusive. You should perform the measures that meet your security objectives, then review and audit your network to determine if more security measure are necessary.

If you have any questions or comments on this material, or have suggestions for future topics, please feel free to email me at johnj@fast.net.

NaSPA member John E. Johnston is manager of technical support and communications for a major hospital in Pennsylvania. He designs and maintains cross-platform local and wide area networks utilizing NetWare, OS/2, DOS, and Windows.