Global Information Assurance Certification Paper

Matthew Connors

Introduction

This report will cover the topic of System Policies and the System Policy Editor (SPE) for Microsoft Windows operating systems. This is a fairly simple implementation in an NT network environment and a commonly overlooked way to reduce the number of security compromises by users. Recent studies suggest that the majority of system compromises were of an internal nature; either the misunderstandings of an employee, the ravings of a disgruntled employee or the tinkering of a tech wannabe. In any case, the implementation of system policies will reduce the number of incidents the security or network analyst will have to respond to.

To gain a better understanding of System Policies this report will look at: a) what a system policy is, b) System Policy Editor, c) Creating policies and d) implementing policies.

What is a system policy?

A system policy is a set of registry edits designed to create a consistent environment that controls what a user can do to the workstation across a domain. The registry edits are accomplished through a file created by the System Policy Editor (SPE). This will be discussed in-depth in the next section. Registry edits are OS specific due to Microsoft's inconsistent implementation of their OSs with respect to the registry. This requires a system policy for WinNT systems and a policy for Win9x systems. Further, the Win9x policy needs to be created on a Win9x computer and the WinNT policy needs to be created on a WinNT system.

There are three (3) tiers of system policy: the machine, user, and group. When looking at the hierarchy of the three policies, the machine policy has the highest priority followed by the user and then the group. Policies are loaded in the lowest to highest order. All registry edits are over-written by the higher priority changes to the system.

It should be noted that all policies take priority over Profile settings, which are not covered in this report. Also, all tiers do not have to be implemented.

The system policy gives you control over the following:

- Control panel
- Desktop
- Disk access
- Network access
- Shell access
- System access

System Policy Editor (SPE)

The System Policy Editor (SPE) is a Microsoft program that will allow for the creation of system policies. The program is shipped with Win9x and WinNT Server or may be downloaded from www.microsoft.com. The SPE must be downloaded to a Win9x computer from the server before being run on the workstation.

The SPE is not loaded by default on Win9x systems and it is not even shipped with WinNT Workstation. It is a default on WinNT Server systems. For Win9x systems the program can be install from the \Admin\Apptools\Poledit\ directory on the CD-ROM. You will want to install the SPE as well as the Group policies. To install SPE on WinNT Workstation you will need to either download it from the NT Server or obtain the Server CD-ROM. When using the CD-ROM you will need to run the SETUP.BAT file from the \CLIENTS\SVRTOOLS\WINNT directory. Be aware that SETUP.BAT will not create icon and program groups on the Start Menu.

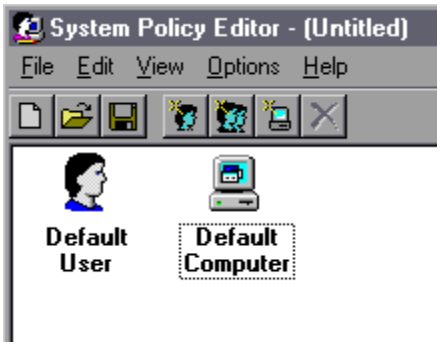
As previously stated a policy on a Win9x machine will not work on a WinNT machine and vice-versa. In addition to this the naming convention used on system policies differs, Win9X machines will look for a file called CONFIG.POL and WinNT computers will look for a file called NTCONFIG.POL. After the policy has been created in must then be placed in the NETLOGON share of the PDC. If file replication is not running the files must also be placed in the NETLOGON share of the BDCs. Shipped will SPE are several templates. Among these are COMMON.ADM, WINDOWS.ADM and WINNT.ADM. The COMMON.ADM template has information for both NT and 9x while the other two templates only have information for their respective systems.

Creating Policies

As stated before, policies for Win9x and WinNT differ slightly. As we have already identified the majority of the differences between the two, this section will outline the process of creating a policy for both of the OSs and then we will highlight the remaining differences.

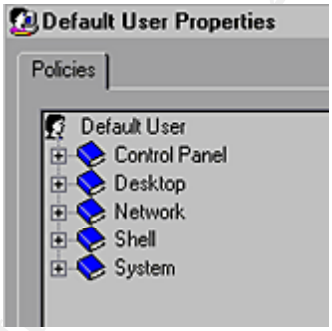
To create a system policy:

1. Open the SPE.
2. Choose New File from the File menu. Default User and Default Computer icons will be displayed in the window. The Default User settings are used to configure the typical setup that will be needed for every user. The Default Computer settings are used to configure the typical setup that will be needed for every computer. Either setting can be used to affect every User and Computer located on the domain.



- From the Default selection we will be modifying the settings for the desired result.

3. Double click on the Default User or highlight the Default User, choose Edit and then Properties from the menu.
4. Under the Default User Properties you will be presented with a tree from which changes can be made from the following categories:
    a. Control Panel
    b. Desktop
    c. Network
    d. Shell
    e. System



5. By expanding each of the branches you will be able to see the different options allowed. Then the process of determining what edits should be made begins. Through the use of editing you will be able to restrict access and limit liability to such items as:
    a. Restricting user access to the Control Panel settings
    b. Restricting user access to changing file or printer sharing settings
    c. Removing options from the Start menu
    d. Restricting user access to the command prompt or REGEDIT
6. Changes are made to the policy through the use of check boxes. A control is enabled when the box is checked, disabled when the box is blank and left out of the policy when the box is grayed out.
7. Special care should be taken when making policy edits. Thoroughly read each option before making edits, as some of the options are not worded clearly.
8. After you are satisfied with the Default User edits it is time to make the Default

Computer edits. Double click on the Default Computer or choose Edit and Properties from the menu.

9. Under the Default Computer Properties you will be presented with a tree from which changes can be made from the Network and System categories.
10. By expanding the branches you will be able to see the different options allowed. Then the process of determining what edits should be made begins again. Through the use of editing you will be able to restrict access and limit liability to such items as:
    a. Forcing a computer to log on to a NT Domain
    b. Disabling password caching
    c. Turning file and print sharing off and on
    d. Enabling user profiles
11. After all of the Default User and Default Computer settings have been edited you will want create customized policies for users, groups or computers. This can be done by selecting add users, groups or computers, choosing the respective item and adding it to the policy.
    a. Add to the policy by clicking on the icon with one head, two heads or a computer, or selecting Edit and Add User, Group or Computer from the Menu. The Add User function will allow you to select usernames as found in the User Manager and bring them into the policy. The Add Group works in the same manner. The Add Computer function will allow you to select computer names as found in the Network Neighborhood. Then edits to the policy can be accomplished, as done in the default edits.
12. You will not be allowed to randomly create a name for the user, group or computer. It must correspond to an actual name located in the NT domain. A special condition exists when creating group policies. You must assign a group priority, or the order in which group policies are loaded.
13. A special group policy should be created for the Administrators. This policy should effectively remove all of the restrictions that where placed in the other policies. The Administrator policy should then be placed with the highest priority.
14. When you are satisfied with your policies save them with the appropriate name. CONFIG.POL for Win9x systems and NTCONFIG.POL for WinNT systems.
15. Copy the Files into the NETLOGON shared directory on the domains PDC.
16. WinNT will automatically look for policies but Win9x will not. To fix this problem every Win9x computer will have to have support for group policies added and some registry settings checked. Adding support for policies was reviewed in the SPE section. The settings that need to be checked are:
    a. In the Control Panel go to Passwords and select the option that Users Can Customize under the User Profiles tab.
    b. Then Run Regedit and go to the key titled HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Control\ Update. Verify that the value is set to 01. This will tell the computer to check the server for information on system policies at logon
17. You should then test the policies. This is accomplished by randomly selecting

five (5%) to ten percent (10%) of your user, group and computer policies and logging on the systems. Then verify that the policies are performing as necessary. If any changes need to be made, make the adjustment and retest.

18. Keep a journal of all changes made to the policies. This will help in troubleshooting and making future changes.

The majority of the differences between SPE for Win9x and WinNT are in the options for Users, Groups and Computers. This is due to the different registries of the two OSs. You will also be able to load more templates as well as create your own templates.

Implementing Policies

The last step in the System Policy is implementation. There are several steps necessary to implement system policies successfully on your NT domain. The most important of which is homework. It is far easier to find a mistake and fix the policy before it has been implemented than to try to fix the policies with an entire department looking to hunt you down because they cannot do their job. Determine what groups will need access to system resources and plan accordingly. Your security policy will help you with this. If your company does not have a security policy get ready to do a lot of talking and leg work.

The next step is to run a pilot on a test network. The test network will allow you to double-check any issues that may arise unexpectedly. When the policies have been fine-tuned to the point they are ready to go live it is time to check all of the networks Win9x machines for the correct settings. The company's inventory will help you a great deal in this matter. If you don't have an inventory, again, get ready to do a lot of walking.

The last step is to go live.

It should be mentioned that before any implementation of system policies are made management should be behind you and the security policy should be updated to reflect the proposed changes.

Conclusion

System Policies are a fairly simple way to protect NT networks from internal user security compromises. Be the compromise from a curious user, a disgruntled employee or a self-proclaimed techie, system policies will reduce the number of incidents the security or network analyst will have to respond to and make everyone's life a little simpler.

Bibliography

Techrepublic.com "Creation of Windows System Policies: Using the System Policy

Editor" www.chaminade.org/MIS/Tutorials/SystemPolicies.htm January 30, 2001.

Microsoft. "Guide to Microsoft Windows NT 4.0 Profiles and Policies" www.microsoft.com January 30, 2001.

Globetrotting.com "User Profiles and System Policies: Windows NT and Windows 95" www.globetrotting.com/win95/pol.html January 18, 2001.

Microsoft. *Windows 95 Resource Kit,* "System Policies." CD-ROM. Seattle, WA: 1997.

Security-tips.com "Enabling System Policies on a stand-alone computer" www.security-tips.com/010.htm February 5, 2001.