Baselining with Security Templates
by Derek Melber - WindowSecurity.com - Monday, 4 October 2004.

The solution to creating and implementing security baselines on computers in your network is to “just do it.” Security baselines establish the foundation for the overall security of a computer. If a computer has no foundation, the chances of it being compromised are very high.

One of the most common complaints about creating and implementing security baselines is that they are hard to establish for the different computers on the network and they are almost impossible to implement. Couple this complaint with keeping the computers up to date with the security baselines causes computers to go without any baseline or security foundation.

What is a security baseline?

I am sure that you have all heard about security baselines or have a preconceived definition of them. However, I just want to make sure that my definition and your definition is the same for this article. The security baseline is a suite of security settings that are established for each type of computer in your organization. The security baseline is established in such a way that the computer performs it duties, but nothing else.

The reason for this “limited” approach is that if the computer can’t perform anything but its predetermined duties, the possibility for it being attacked successfully is much smaller.

Windows computers need security baselines more than about any other type of computer for a couple of reasons. First, Microsoft is notorious for allowing the default installation of their operating systems to be insecure. I don’t think I need to defend this statement much, considering the issues with Internet Information Services and Internet Explorer over the past couple of years.

The security baseline will consist of more than just securing services and applications; it will go to the core of the computer security settings. A typical security baseline will include control over services, permissions on files, Registry permissions, authentication protocols, and more. There will be a security baseline established for each type of computer in your organization. This will include domain controllers, file servers, print servers, application servers, clients, etc.

Security Templates for Baselining

In the last article I wrote, Understanding Security Templates (LINK!!!), you were introduced to the contents of a security template. There we saw that a security template included settings for the following areas:

- Account Policies
- User Rights
- Event Log settings
- Restricted Groups
- System Services
- File Permissions
- Registry Permissions

As you can see from this list to the list we just unveiled in the baselining section above, they are virtually encompass the same security settings. Although a typical security baseline needs to include a few areas outside of a default security template, it includes so many of the settings it can't be ignored as a solution for implementing your security baselines.

Configuring Security Templates

The first step to implementing the security baseline on your computers is to determine what the baselines will be for each type of computer. The next step is to create an environment that makes it easy and efficient to implement these settings. The solution to step two is to develop security templates for each type of computer.

To complete this security template creation you will use the Security Templates snap-in. The Security Templates snap-in is included in the Microsoft Management Console (MMC). To access the MMC and include the snap-in, follow these steps:

1. Click the Start button.
2. Select the Run menu option.
3. Type MMC into the text box and click the OK button.
4. Select Console from the Toolbar to get the menu options.
5. Select the Add-Remove snap-in menu option.
6. Click the Add button.
7. Select Security Templates from the Snap-ins list, then click the Add button.
8. Click the Close button, then click the OK button.
9. Expand the Security Templates node, then expand the C:\Winnt\Security\Templates node to see the list of security templates, as

shown in Figure 1.

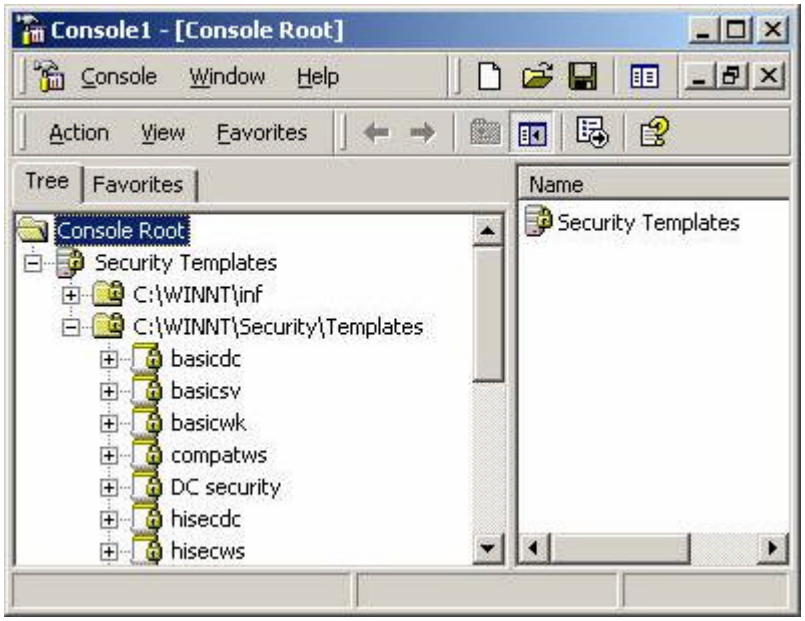

Fig 1: Security templates snap-in provides access to the default templates, as well as the ability to create new templates

You can either start with one of the preconfigured security templates, or you can create your own. If one of the preconfigured templates has 90% of the settings that you prefer you can just copy it as a starting place.

If you want to create your own security template, just right-click on the security template folder (C:\Winnt\Security\Templates) and select New Template.

This will create a new template that has not configurations in it to begin with. As a suggestion, make sure you name the security template according to what it will be controlling, because they can be hard to track down when there are numerous templates created.

After you create the template, you will just delve into the different topical areas of the security template, making the settings that match the security baseline settings that you have established.

To make the process of creating all of your security template more

To make the process of creating all of your security template more efficient, you can create a matrix that includes all security baselines and their settings. Start by creating the security template that has the fewest baseline settings. Then, copy this template to create the additional templates, which will just need to be configured for the differences from the original security template.

Deploying the Security Templates

After the security template is created, you now need to deploy it. If you only need to deploy the security settings to a few computers, you might want to choose a manual method, which allows tighter control over establishing the security on the computers. If you are up against deploying the security templates to thousands of computers, you will want to choose an automated solution, which provides persistent affects. There are three primary methods to deploy security templates to establish the security baseline on your computers: manual, command line tool, using a GPO.

Manual

Of the three methods, you can probably guess that this is the least used method. The reason seems fairly obvious: you don't want to manually configure thousands of computers to establish the security on them. However, manually deploying security templates is common. You will most likely see this when the computer is not part of a Windows Active Directory domain and when the administrator of the computer does not have Active Directory administrative rights, but does have administrative privilege over the computer.

This method includes using the Security Configuration and Analysis (SCA) snap-in. The snap-in is accessed just like we accessed the Security Templates snap-in from above.

SCA only works on the computer where the MMC is running. The tool can't configure computers remotely, which is where the limitations are evident. To configure the computer with the security template, follow these steps within the SCA snap-in:

1. Right-click on the SCA node and select Open Database
2. Select a name for the database
3. Select the security template you want to use
4. After the database is created, right-click on the SCA node and select the Configure Computer Now option

Command line

If you have more than just a few computers that you need to configure, but you don't have access or control over the GPOs in Active Directory, you can deploy security templates using a command line option. The command line tool is named SECEDIT.EXE and is the command line version of the SCA. Almost anything that you can do in the SCA you can also do with the SECEDIT tool.

SECEDIT can either be run on each computer, or it can be scripted to run automatically on many computers. The command that would deploy a security template on a computer is:

SECEDIT /configure /db db1.sdb cfg sectemplatename.inf /log logname.log

This will configure the local computer using a database name of db1.sdb, a security template name of sectplatename.inf, and a log file of logname.log. These names can be anything that you want. If you are scripting the command, you will want to place the security template file on a network share and use a network path to point the computer to the file.

GPOs

The most efficient and easy way to deploy security templates is by using GPOs. The GPO provides a scalable and persistent solution. The solution does require and Active Directory domain and access to the GPOs. Using GPOs to implement your security templates are more efficient than the other two solutions because the other two solutions just don't scale to an entire domain of computers. GPOs provide a method to implement the security templates within the Active Directory structure where the computer accounts are located and organized within organizational units (OUs).

GPOs are easier to implement security templates because the templates can be imported directly into a GPO. Since the GPOs are linked to the OUs which typically are created to house computer object types, it is a perfect solution.

The first step to using GPOs for security template implementation is to have an OU structure in place, which is the case in most Active Directory domains. Next, there needs to be a unique GPO linked to each of the OUs which contain different computer types, for example file servers, print servers, application servers, and clients. In essence, there should be at

least one OU and GPO for each security baseline.

To get the security templates into the GPOs, you will need to edit the GPOs using either the ADUC interface or the GPMC. Once the GPO is being edited, you will expand the Computer Configuration node, as shown in Figure 2.

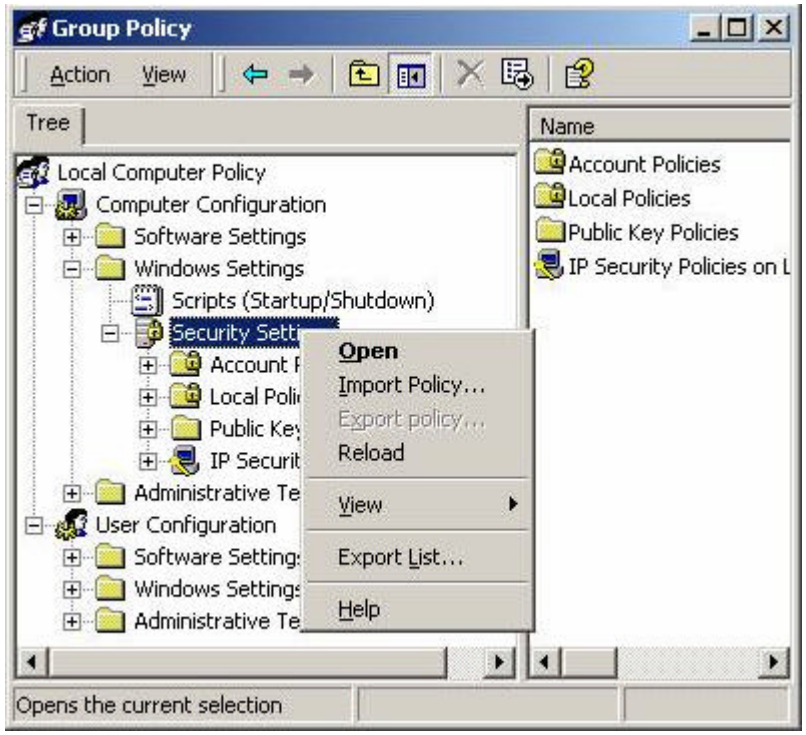

Fig 2: Typical GPO opened to import a security template

After right-clicking on the Security Settings node, you can select the option to Import Policy. This will open up a browse window, allowing you to select the security template for each GPO that you should contain a security template. Then, just close the GPO and the settings are in place.

Once the security template is imported and the GPO saved, the computers within the OU will automatically have the security template settings configured on them within about 90 minutes. This provides an easy way to deploy the security templates, affect all of the computes in the domain easily, and persistent.

Summary

Security baselines will help both IT and auditors if they are correctly designed and implemented. The baseline should include all security settings that are essential to locking down the computers, but still allowing them to perform their function. There should be security templates created for each type of client and server that requires different security settings. Once the security templates are created for each type of computer, there are three different options to implement them on the computers. The most efficient and easiest option to deploy the security templates is to use GPOs. The GPOs will be linked to OUs containing the computer accounts. The GPOs will apply the security template settings automatically to the computers within the domain.