

Hardening Windows 2000 Computers

Elliot Gingold, LAN Server Group, Client Services

There is always a trade-off between security and usability of computer systems. Features which make computers easy to use are always very popular with users; unfortunately however they also may increase the opportunities for breaking in and compromising that system. Those who produce computer systems and software want to impress users with a range of bedazzling (and often not fully tested) features and Microsoft is certainly a leader in this regard. Unfortunately, this means that computer systems straight out of the box present an easy target for hackers, virus writers and the like. It is the job of administrators to shut as many of the open doors as in possible before they can get in. Most of this session will concentrate on this aspect of computer security.

It is probably appropriate, however, to have a look at the range of security related tasks which face a Windows 2000 administrator. These include:

- 1 Hardening the various settings that can compromise security and activating secure procedures.
- 2 Keeping the machines up to date with respect to service packs and patches, including those for the OS, but also for applications.
- 3 Installing and maintaining anti-virus and other scanning programmes.
- 4 Monitoring the state of the systems (log monitoring etc).
- 5 Ensuring that recoverable backups of all important data is available.

Before moving on to look at the first point, the major emphasis of this seminar, I will briefly examine the question of updates. Recent events (the Slapper worm for example) show the importance of this issue.

Keeping your Systems Up-to-date

Whenever an event such a Slapper occurs, everyone is quick to blame administrators for not applying patches in a timely manner. However, this is clearly not a case of thoughtless negligence. It has become very hard to keep up with the continual flow of hotfixes and the like, especially when one is responsible for a large number of machines each with differing configurations. In addition, it is well known that applying patches without testing can lead to unforeseen incompatibility problems. Nonetheless, this is clearly an area in which everyone has to lift their game.

We will have a brief look at four different methods that Microsoft makes available at no additional cost to aid in this task. Unfortunately, comparison of the results obtained using each illustrates the mess the area is in. It is almost inevitable that the different scanning tools

will list different critical patches as missing. Microsoft has a long way to go before it is on top of this field!

Windows Update Service (SUS)

This is Microsoft's attempt to make mass compliance with patching possible. The feature is built into w2k sp3 and XP. We have established a SUS server on campus to which computers can be pointed. For information see: <\\dc5\Windows 2000\Utilities\Windows Update Client>.

This service can be configured, either on individual machines, or by local group policy, to apply all approved updates to client machines automatically. This eliminates the difficulties caused by the restrictions preventing normal users applying such updates manually. Such automatic updates would be scheduled for night hours.

This tool has, however, a number of serious limitations in its present form. It does not apply service packs and only looks after the core operating system (plus IE). Furthermore, I have found it to be the worst tool at missing updates. There is also no possibility of updates being tested on a range of machines before approval. Thus I would conclude that it is better than nothing for keeping workstations reasonably up-to-date, but that further versions are anxiously awaited.

Windows Update (Web based - on Start Menu)

Easy to use, but administrator privileges required. Presents a wider range of updates than SUS (not just critical updates), but still OS based. At least it checks for updates when you want to!!

HfNetChk

A command line utility which scans for missing updates but does not patch. Can be run remotely (provided you have the necessary permissions). Available from: www.microsoft.com/technet/security/tools/tools/hfnetchk.asp.

Checks a number of applications (SQL/Exchange) as well as the OS. Generally regarded as being the most reliable, but options can be confusing. We have used this combined with script based application of patches on our servers.

Microsoft Baseline Security Analyzer (MBSA)

A GUI based tool, apparently related to HfNetChk. Nice to use for administrators, but again only for analysis, does not apply updates.

<http://download.microsoft.com/download/e/5/7/e57f498f-2468-4905-aa5f-369252f8b15c/mbsasetup.msi>

With so many options, all with limitations, it is not surprising that many organisations have purchased tools to aid in the update process. The most popular of these (which at least one University Department has purchased) is St Bernards Update Expert.

<http://www.stbernard.com/products/updateexpert>

Tools for Hardening Windows 2000 Systems

In previous versions of Windows NT, instructions for hardening systems invariably included the need to make direct alterations to the registry using tools such as *regedit* (so-called registry hacks). While such operations were gist to the mill of experienced administrators, they were approached with trepidation by less experienced users. One of the major advances in Windows 2000 was the provision of tools that make similar operations less intimidating. In addition, there has been a considerable extension in options available to the system hardener.

While it is always possible to make changes to the configuration of a system on an individual basis, in real situations it is far more practical to first put together a complete set of desired configuration settings and to apply these to individual computers as a whole. Such sets of configuration settings are referred to as *Security Templates*. When you install Windows 2000 a number of such templates are included in the c:\winnt\security\templates folder. Here you will find templates for basic workstation, basic server and basic domain controller installations as well as for higher security versions of the templates. It is, in fact, the basic templates which are used when the system is first installed (except when an upgrade has been performed from an earlier OS – here a lower security compatibility template is applied).

Note that security templates can be used cumulatively – you may have a template which adds further application-related settings to computers using that application.

Few would claim that Microsoft is the leading expert on computer security so it is unsurprising that a number of other organisations have produced their own security templates and made these widely available. In this seminar we will be looking at templates that have been made available by the Centre for Internet Security (CIS). We will, in fact be concentrating on one such template for Windows 2000 Professional, the so-called “Gold Standard” or “Consensus Baseline” template, drawn up by CIS in conjunction with a number of other security organisations and US Government agencies. This template can be downloaded from <http://www.cisecurity.org/>. Following links to Windows 2000 Professional Level 2, register and download the installation file **CIS-Win.exe**. Running this file on your computer will install a range of templates, the CIS Scoring tool, and most importantly, a number of pdf files which cover in some detail the procedures that will be demonstrated in this seminar and also document the system changes introduced by the application of the key templates. As it is assumed that any participants in this seminar serious about taking this process further will download this information the detailed instructions will not be repeated here!

It should be made very clear that you should NOT simply obtain a template from another organisation and apply it to your systems, whatever the credentials of the organisation involved. Hardening security always has usability consequences and some of these will not be acceptable in your situation. Some, in fact, might break critical applications or prevent client machines from taking part in your network. It is thus necessary to test proposed changes thoroughly before applying them to working machines. The first stage in this is to familiarise yourself with the changes that are being introduced and the justification offered for them. The documentation provided with third party templates is invaluable for this purpose, alongside the system tools which allow you to analyse the current configuration of your system and compare this to the settings in a given template.

I will be demonstrating this process with respect to the CIS Gold Standard template. We will, of course, only have time to look at a very small proportion of the settings covered. Determining the suitability of a various settings to our particular environment would make an excellent topic for discussion either on our web based discussion form (liteco), flite or indeed follow-up seminars. The aim of the process should be to produce templates of our own which can then be applied to systems at this University.

The following demonstrations will be included in the seminar:

Local Security Policy

This mmc based console is provided as part of all Windows 2000 installations. Experienced administrators will recognise it as (for the most part) a sub-set of the Group Policy tool. However, it has one major difference – it reports on the actual setting on the machine at a given time rather than on a policy. It should be noted that when a system is part of a domain structure it reports both the *local setting* and *effective setting*. This is because any local setting will be overruled by settings introduced as part of site, domain, or OU based Group Policies. More on this later!

Individual security settings on a local machine can be set using this tool. We will introduce this aspect with a look at the Restrict Anonymous setting. However, the main use of this tool is gaining a quick insight into the setting in operation on a given machine. It is not possible to determine which Group Policy is responsible for a particular effective setting. With Windows 2003 based domains this will become possible with a new Resultant Set of Policies tool.

CIS Scoring tool

This tool examines the overall state of security on a system and awards a score between 0 and 10. Actually, due to some recognised bugs in the scoring system, a score of 10 cannot be reached even by following all recommendations. However, a score of 0 is possible, and I have seen this result in some local systems!

The tool uses HfNetChk to measure hotfix up-to dateness, and a security template of your choosing to access whether the tested machine is conforming to your security policy. Its produces a useful first indicator of the state of a particular system and can provide an excellent incentive for digging deeper!

Security Template and Security Analysis and Configuration (SAC) Tools

Microsoft does not provide a ready made console for these tools but an mmc containing both of these is easily constructed as will be demonstrated.

The *security template* add-in has a single purpose: it provides an easy to follow view of the settings in each template. Initially it only points to the Microsoft templates but can easy be pointed to other template containing folders (as will be demonstrated). Template settings can also be modified within this tool though it is more usual to construct custom templates with the SAC tool.

Security templates themselves are simply text files (as will be shown). In fact, knowledge of the fairly basic syntax of these files allows changes in templates to be made with a text editor. This route, however, is more likely to be error prone!

The *security analysis and configuration* tool is rather more powerful (and complex). Operation of the tool proceeds by the following steps.

- 1 A security template is loaded into a new 'database', or merged into an existing 'database'. In fact, I found the term 'database' somewhat confusing in this context. It is really only a working copy of the template you are examining, or modifying.
- 2 The tool can then analyse the current setting and reveal inconsistencies with the settings in the template.
- 3 You can then apply the template settings, bringing the computer up to the level required by the template.
- 4 Alternatively, you may decide to alter template settings if you consider some of these are unsuitable for your purposes. Building a custom template in this way is probably the main application of this tool. The modified database can then be exported to a new template file.

We will examine the various types of settings which are found in a Security Template (and hence in a local security or group policy). These are

- Password policies (only apply to local passwords!)
- Account lockout policies (as previous)
- Audit settings
- User right assignments (these bear careful examination)
- Security options (these are in fact registry settings)
- Settings for Event logs
- Restricted groups (membership of which cannot be easily altered)
- System services (start up state and security)
- Registry (security of keys/values and auditing)
- File system (allows ntfs permissions/auditing setting to be controlled)

Finally, it must be made clear that it is possible to add settings manually to security templates which are not covered in the standard consoles. The CIS Gold template in fact adds a number of security options (i.e. registry keys) which do not appear in the tools we have looked at. This is because the tools are designed to display only what was considered at the time of creation the most important parameters – a tool would showed every possible registry key would not be feasible. The configuration file for these tools, however, uses a simple syntax and it is not difficult to add display of extra items. While this is beyond the scope of this seminar, I can give help if requested.

secedit

This is the command line partner to the tools in the last section. In fact, simply typing secedit into a command line produces an excellent GUI based help screen. The tool can be used for analysing or configuring security setting on a machine in the same way as is done with SAC

(above). It can also validate the syntax of a security template. Probably its best known use is with the refresh switch which will refresh current settings from Group Policy – a far more effective method than waiting for automatic refreshing or rebooting the computer!!

Applying Security Templates

The final stage in use of security templates is, in fact, applying them to the machines. We have already seen how this can be done using the SAC tool. In fact, if application of a template is all that is required, the `secedit` command line option is more convenient (and can of course be used in scripts). For applying the security template to a large number of workstations the following options are available.

Use of Group Policy

Once a security template has been designed and tested it can be imported into a GPO. This should be linked to the OUs containing the w2k computers. This should be the most effective way of installing security policies and will prevent permanent overwriting of settings by users..

However, there are two elements in security templates that do not appear in Group Policies. These are the Registry permission and file system permissions/auditing settings. Although I have not examined this exhaustively at this time, these settings do not appear to be transmitted via the Group policy mechanism.

Use of start-up scripts

It would be perfectly feasible to set up w2k start up scripts to apply the required security template each time a computer boots up. (Or, if you trust your lockdown, on installation of the system only). It would be necessary to ensure that the settings, which would be applied locally, would not be overridden by GPO settings from the domain structure.

This method would have the disadvantage that settings would be permanent “tattooed” into the registry. If the computer was moved to another area and some different settings were needed, the original settings would have to be explicitly removed. The anti-tattooing mechanism of GPO application is one of its strongest (if incomplete) features.

Finally, it should be emphasised that the templates we have been discussing are referred to as baseline because they are designed for hardening normal day to day use computers. If computers require higher levels of security it would be appropriate to lockdown additional features. Such features are often included in incremental templates which are applied in addition to the baseline template.

1/2/2003