GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Security Configuration Wizard

GSEC Practical Assignment Option 1
Version

Kiosi Garfias

February 10, 2005

Abstract/Summery

Do you remember the last time a Windows Server was secure? Don't feel out
of place, neither do I. In reality, the most secure a Windows Server will ever be
is when it's shutdown, but don't tell that to Bill Gates. All joking aside, we have
all encountered unsecured Windows Servers since the early ages of Microsoft.
The challenge has been how to make it secure and keep it power on at the
same time. Unfortunately for us, leaving the server shutdown is not an option
we can afford to take, so we are faced with the monstrous task of securing a
"glass house".

When it comes to security, Microsoft took a little while to jump on the wagon. In
its latest release of the Windows 2003 server, Microsoft delayed the deployment
of a very promising security tool known as the Security Configuration Wizard
(SCW). To the benefits of the security community, Microsoft decided to deploy
this tool with the release of Service Pack 1. Even though Service Pack 1 is in
beta, the Security Configuration Wizard is promised as one of the new features
added to the Windows 2003 family of servers. Here is when I jump on the
wagon.

As a security professional, my intent is to educate other security professionals
on the capabilities, benefits, and limitations of the Security Configuration
Wizard. Before I jump directly into the tool, I will provide a quick overview of
Windows Security as well as briefly touch on some other useful tools that
complement the SCW. I will then jump into a system security policy
extravaganza that will emphasize how important Security Policies are to the

enterprise. Finally we will discuss the Security Configuration Wizard more in depth and provide some useful information that will help you determine how this tool will simplify your security needs.

As a former System Administrator, this document could not have been completed unless we actually play with the tool. So, I have created a section specifically dedicated for this task. I'll Install the tool, configure the tool, and create a security police that will be imported in to Active Directory.

Windows Security

Security is, and should be, the primary concern of every IT manager. Unfortunately, reality shows how this is not the case on many occasions. Security gets bypassed for the sake of convenience or to speed up a process that is broken. Due to these reasons, every year a virus comes and serves as a reminder to IT managers why security should be the primary concern and never be bypass.

With the deployment of the Security Configuration Wizard, security will be implemented in a more automated and manageable way. At this time, there are many processes to secure a server, but the most trusted way is with a manual checklist created by the organization who own the system. A few tools are out there that makes this process less painful. For example, Security Templates help configure certain security settings and can be used to deploy registry permissions throughout your organization; however, there are limitations to this tool. The SCW closes the gap between security, and some of the limitations of previous tools are eliminated. Like any other tool, its effectiveness is measured only by how well you use the tool to enhance the systems security. The SCW is not meant to fix all your security problems, or serve as a security policy for your organization, it is only a tool, and should be treated with caution.

Windows Security Overview

For the past generations of Windows operating systems, Microsoft has attempted to make its systems more secure and minimize the security risk associated with owning a Windows Operating System. The attempt has been made to simplify security, and make it more manageable for the systems administrator, as well as the security professionals. From the early ages of Windows NT, security has been slowly implemented in the Windows architecture. It all started with the centralization of account managements in the NT domain environment, and slowly moved to what it is today. The centralization of account managements was made possible with the release of Windows NT Server Primary Domain Controller technology. The domain architecture made it easier to manage account, and bumped security to a different level. Prior to this technology, account management was a nightmare and took face time away from security issues and not to mention how much of a

security risk it was on itself.

Many other security technologies have been developed since the release of Windows NT. Some were not very successful, and did nothing for security, while others were reengineered and became the backbone of Microsoft security tools. Let us take for example the Security Templates deployed with Windows 2000. Prior to their release, Administrator had to manually set every security setting in the registry and trust they will stay intact for the remaining life of the server. Security was a nightmare to manage in the server lever, now imagine the workstation lever. To our benefit, Security Templates were created and a wonderful tool known as the Security Configuration and Analysis Tool was deployed. This tool gave the administrator the flexibility to create a security template and apply it to all the windows systems in the organization. Automation and limited centralized security management capabilities were the reason security templates are still in use today.

The ultimate leap in security came about with the realization of Group Polices, which did the same thing as the security templates but in a grand scale. Centralize security management was now possible and the security management nightmare was over, at least we thought so. Even though Group Policies gave us the accessibility to manage the security in every domain, the domains were still not secure. A powerful tool able to implement most of the site security policy was in place, but it lacked a critical component, an effective site security policy. When Windows 2000 was deployed, the architecture was changed drastically from its predecessor and from one day to the next, the security policy did not quite fit in to place. Organization had to revise their security policy to work with the powerful tool at hand. So the romance between Group Policies and Security Polices flourished. Unfortunately, that relationship was not as strong in the beginning until the Administrators realize their security management nightmare was not over. The majority of early Group Policy deployments were done in a production environment by anxious administrators eager to play with the new technology, with the exceptions of those few that did it the right way. To make the story short, many organizations deployed Group Polices without any security policy backing them up. As you can see, the need for an effective security policy is crucial to maximize the benefits the security tools provide for your organization. With this in mind, let us now discuss the availability Microsoft security tools in place for a better understanding of Microsoft Security.

Microsoft Security Tools

Time and time again I have seen unsecured systems that had all the resources required to secure the system, but were not used properly or the Administrator was not familiar with the usage. As a security awareness effort, let us now discuss some of the tools that are deployed with the Windows Family of Operating Systems as well as provide a quick overview on each of them.

Please note that this section was not intended as an Administrative Manual for each of the tools discussed, but as an educational tool for the benefit of new security professionals.

Some of the tools discuss here are:

- Security Configuration and Analysis
- Security Configuration Wizard
- Group Policy Objects

Security Configuration and Analysis

The Security Configuration and Analysis (SC&A) function as a scanner and deployment tool of multiple security options with the use of security templates. The tool allows for the creation of security templates, also known as local security policies, which can later be integrated in to other similar system. The concept is simple and usability ranges from setting registry permissions to account management. The SC&A tool allow for more security options than the Security Configuration Wizard; however, it lacks certain options available only on the SCW.

Security Configuration Wizard

Security Configuration Wizard is the latest security tool deployed by Microsoft in SP1 for Windows 2003 Servers. It functions very similar to the Security Configuration and Analysis tool discuss earlier. The SCW scans the system and determine what services are running and associates all detected services to roles. It then creates a security policy and saves it as an xml file which can later be deployed to other similar servers using Group Policy Objects. The strengths of the Security Configuration Wizard are services management and port security. "All detected services that are not used by the functional roles will be disabled and ports that are not in use will be blocked." (SCW Help Pages)

Group Policy Objects

Group Policy Objects are use to force uniform setting to user and computer within Active Directory. We will later discuss how Group Policy Objects can be use to deploy SCW security polices to all server in the domain.

Systems Security Policy

Systems security policy is to security, as the skeleton is to the body. Many organizations don not seem to understand this concept and are satisfied knowing that the Administrator will keep all their systems secure by applying the latest Microsoft security patch. Security is more than just patching systems with

the latest patch, it consist of careful planning and effective security policies dictating what can and cannot be done in your organization's network. With this concept established, let us now discus how your Systems Security Policy can be implemented with the help of Group Policies Objects and SCW policies.

Group Polices

Our primary focus would be the effective user of Group Policies to meet our security needs. Prior to Group Policies, Administrators had to manually configure each machine, or ghost from an "at one time secure image". Security is dynamic and unless you update your secure image every time a patch comes out and manually implements the latest security setting on you current network, you organization will be vulnerable to viruses and other exploits. Clearly this scenario depicts an unmanageable security environment, which can lead to the loss of company assets and in many cases, the loss of human life.

NOTE: Group Polices can be a little complex at times, and in some cases dangerous, so before you start implementing group polices make sure you have taken the time necessary to test and evaluate your GPO in a lab environment.

One of the benefits of Group Polices is that it can deploy SCW security polices to all the servers in the enterprise. This process of deploying SCW polices can be a little dangerous if not familiar with the tools capabilities. For example, if a server is configured as a File server/Telnet server/FTP server and it is placed in an OU with a GPO that was created with the SCW to support only a file server then the GPO would lock down the ftp and telnet service crippling your server. To our good luck, SCW has the capability to perform role backs. We will dedicate more time to role back at a later time.

SCW Deployment

There are two ways to implement a SCW policy to the enterprise. One would be running the tool on the server we wish to configure and implement the policy with either the command-line or GUI interface. This method works best but it takes away from the centralize management of security. The second method would involve the use of Group Polices Object to deploy the policy. Unfortunately, this method requires a little more work than just a few clicks on the button.   Group Policy does not provide native support for the Security Configuration Wizard policies. Here is where the command-line tool comes in to place.

The SCW command-line tool transformation function, "scwcmd transform", allows for the transformation of SCW polices in to native files that are supported by Group Policy. The command tool is very simple, yet powerful.   Once the command transforms the policy, it will create a Group Policy Object in Active Directory, which will have to be linked to an OU for it to take effect. (scwcmd

transform /h)

There are a few security issues with following this route. "IIS settings can not be deployed via group policies." Major issue if you tell me. It is a risk that must be evaluated and addressed in the Security Policy. It might be better to not deploy SCW policies using GPOs if a server is running IIS. Best practice would be to use the SCW tool to implement the policy locally rather than using GPOs.

Security Configuration Wizard

Overview

The Security Configuration Wizard was not intended to solve all of you security needs. Microsoft clearly indicated in its help pages, how SCW is not a security panacea, but only a tool. As a security tool, the SCW offers the capabilities to configure your server for a specific function and deploy the same setting to other servers performing similar organizational functions. Similar to Security Templates, SCW generates an xml file that houses all the settings require for the servers configurations. One of the benefits for the SCW is that Security Templates can be imported in the SCW security policy. This will create a more powerful security policy.

Roles

The Security Configuration Wizard is heavily guided towards functional roles for performing its security needs. It is easier to implement security, if system security policies are implemented for each role the system plays in your organization, rather than having one single security policy for all the servers. The Security Configuration Wizard does this for you; it first determines what services are being provided by the server with the use of an internal scanner. The scanner is guided by the Security Configuration Database, which contains all the information required for each role. Functional roles will be assigned base on what services are running and what ports are open. Once the role is assigned, the server will be configured to meet the security needs stated in the Security Configuration Database. (SCW Help Pages)

Capabilities

The SCW can be used to apply multiple security settings depending on what functional role is perform by the server. A server can have one or more roles assigned to it. For example, a server might provide FTP services to the organization and also function as the site's internal web server. Here are two clearly defined roles that require independent security needs. The SCW wizard has the capability to configure the server as required by the Security Configuration Database to meet the application's needs for security.

There are multiple security settings that can be applied with the Security Configuration Wizard. In many occasions security was compromise due to services running in the systems without the knowledge of the Administrator. Servers were not configuring properly or unneeded services were never turned off. This created a major problem for security since patches for different vulnerabilities were not applied to those unknown services. The Security Configuration Wizard provides the capability to turn off all unneeded services and keep them turned off.

Another benefit of SCW wizard is the capability to block unneeded inbound ports. We, as security professionals, know the risks involved on leaving unneeded ports turned on or not configured. The SCW will link an application to needed ports and let the application mange the ports as needed. This includes turning off the port when it is not being used by the application. There are a few limitations to the level of port security provided by the SCW. Ports 88 UCP, 88 TCP, and 389 UDP cannot be configured by the SCW.

As discussed earlier, security templates can be incorporated in to the SCW to allow for a higher lever of security. In the case of conflicting setting between the SCW and the security template, the SCW will take precedence over the security template. If this situation ever happens, perhaps it would be a wise idea to look over you security configuration guide to identify and correct this issue.

A few years ago I had the privilege of learning about NTLMv2 the hard way. While working on the local policy of our brand spanking new Windows 2000 domain controller, I changed the LAN Manager Authentication level to "Send NTLMv2 response only\refuse LM and NTLM". It only took a few minutes for the help desk to call in and ask if we had any problems with the network. After about an hour of researching and downtime, I finally narrowed it down to the specific change. It was fixed right away, but a big lesson was learned. Never make changes unless you know what you're changing and how it will affect your network. To our good fortune, the SCW comes equipped with a rollback capability. This means that if you made a few changes to the SCW policy with out first testing in the lab or if things just went wrong, the SCW can save the day and minimize down time (translation: money).

As with many of the other Microsoft policy base tools, auditing can be also configures with the SCW. This capability is extremely important since it serves as the historical library of the server, no audits means no history and no history is the equivalent of saying "I don't know".

SCW Lab

Installation

The SCW is not an independent downloadable tool at this time; it can only be

obtain with the installation of Service Pack 1 on a Windows 2003 server. If you do not find the SCW in you Administrative tools after installing Service Pack 1, don't be alarm. Microsoft decided not to install the tool by default. You will have to go to the Add/Remove Windows Components in the Control Panel to do a manual install. The installation of the tool does not require any specific knowledge, however, there are a few requirements that must be consider prior to the installation of the SCW. As of the latest revision of this document, the SCW was only supported on the Windows 2003 family of server with Service Pack 1. Microsoft has not release any statements promising support for pre Windows 2003 Servers. Keep this in mind especially if your domain is in a mix 2000/2003 environment, policies created with the SCW will not affect 2000 server. It would be a wise move to create a separate GPO for you 2003 server and deploy you SCW policies there.

Creating a policy with the SCW

The process of creating the SCW policy is not as complicated as one might think. Microsoft made it simple enough that a monkey can click "Next" a few times and have an effective SCW policy. Prior to the creation of the policy, a few items must be taken into consideration for better results. All services must be running in the system at the time of the SCW scan. The SCW does a scan of the system to determine what services are running and associates them with pre configured roles. Once the services and roles are linked, the wizard automatically closes all unneeded ports and configures discovered roles base on its configuration database.

Execute the Security Configuration Wizard by going to Start>Programs>Administrative Tools>Security Configuration Wizard. The Welcome screen will pop up with a basic navigational menu.

- Make sure all applications that required inbound ports are running.
- If this is your first time running the wizard, take the time to read the help pages. They provide useful information on the inner working of the wizard.

Click "Next", this will bring you to the "Configuration Action" where you can select what operation the Wizard will be performing. For the purpose of this lab, we will select "Create a new security policy". You also have the options to:

- Edit an existing security policy
- Apply an existing security policy
- Rollback the last applied security policy

Once you have selected the desired action click "Next". The next step is to select a server that will server as the base line for the policy. If selecting a server other than the local computer, make sure the Security Configuration

Wizard is installed on that server for better results. Once you have selected the server click "Next".

- The local computer is selected by default

At this time the server is scanned and contrasted with the Security Configuration Database to determine the following:

- Roles that are install in the server
- Roles that are likely being performed by the server
- Services that are installed but not part of the Security Configuration Database
- IP addresses and subnets that are configured for the server

Once the scan is complete, click "Next" to proceed to the Role-Based Service Configuration page.

Role-Based Service Configuration

The first page informs the user of possible consequences that might result if not knowledgeable enough about the services provided by the server. Select **Next** if you feel you have a thorough knowledge of the server.

The wizard will display a list of roles detected currently installed or recommend roles bases on the detected services. A server can perform multiple roles but it might not be a good idea. The more you have in the server, the more roles required and the greater the risk of braking the box.
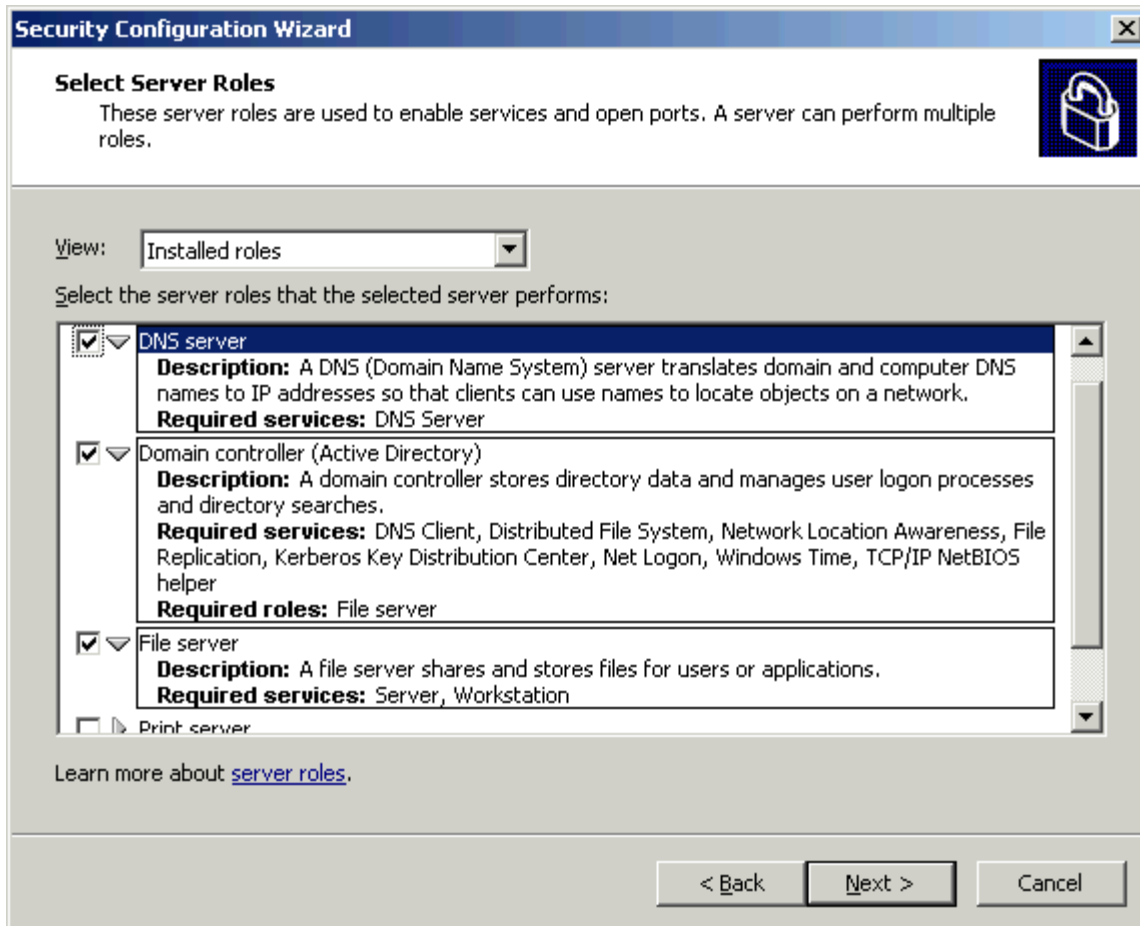
Once you have review your roles click Next to view the selected client features. The server also performs as a client to other servers in the domain. For example, a domain controller might be a DHCP client and a DNS client as well. The Security Configuration Wizard will configure the required services for the client to run; any other services not selected will be disabled by default. This is a critical section of the wizard that can disable needed services if not configured properly. Make sure the recommended settings are carefully scrutinized to make sure everything works as needed. When done click "Next" to proceed to the next section.
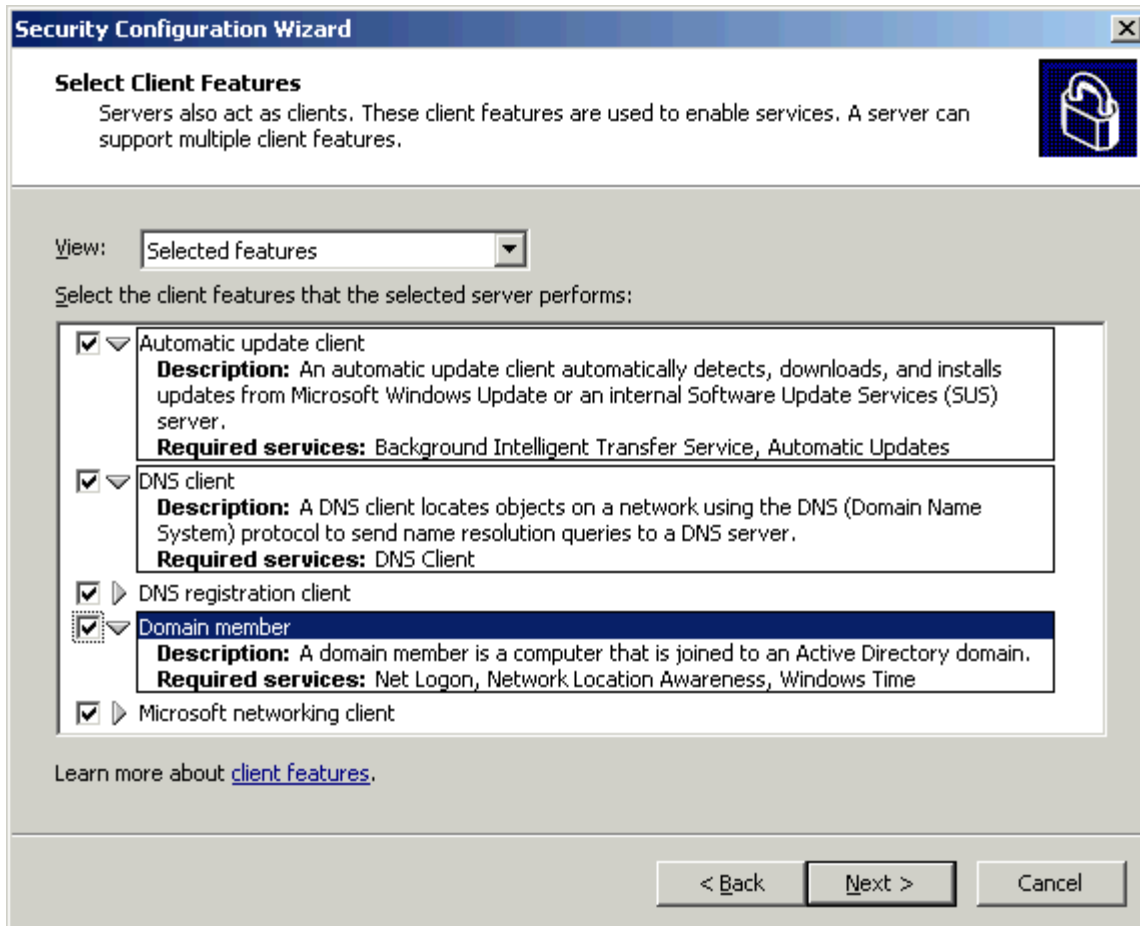
A specific section was designed for administration and other options. In this section, you can select options use for administrative action that requires a specific service and port. If it is not needed, disable it. It would be too easy for an administrator to just select all and click next. It requires research and careful planning to determine what is needed and what is not prior to the implementation of this policy. All unselected services will be uninstalled by default. Select **Next** when done.
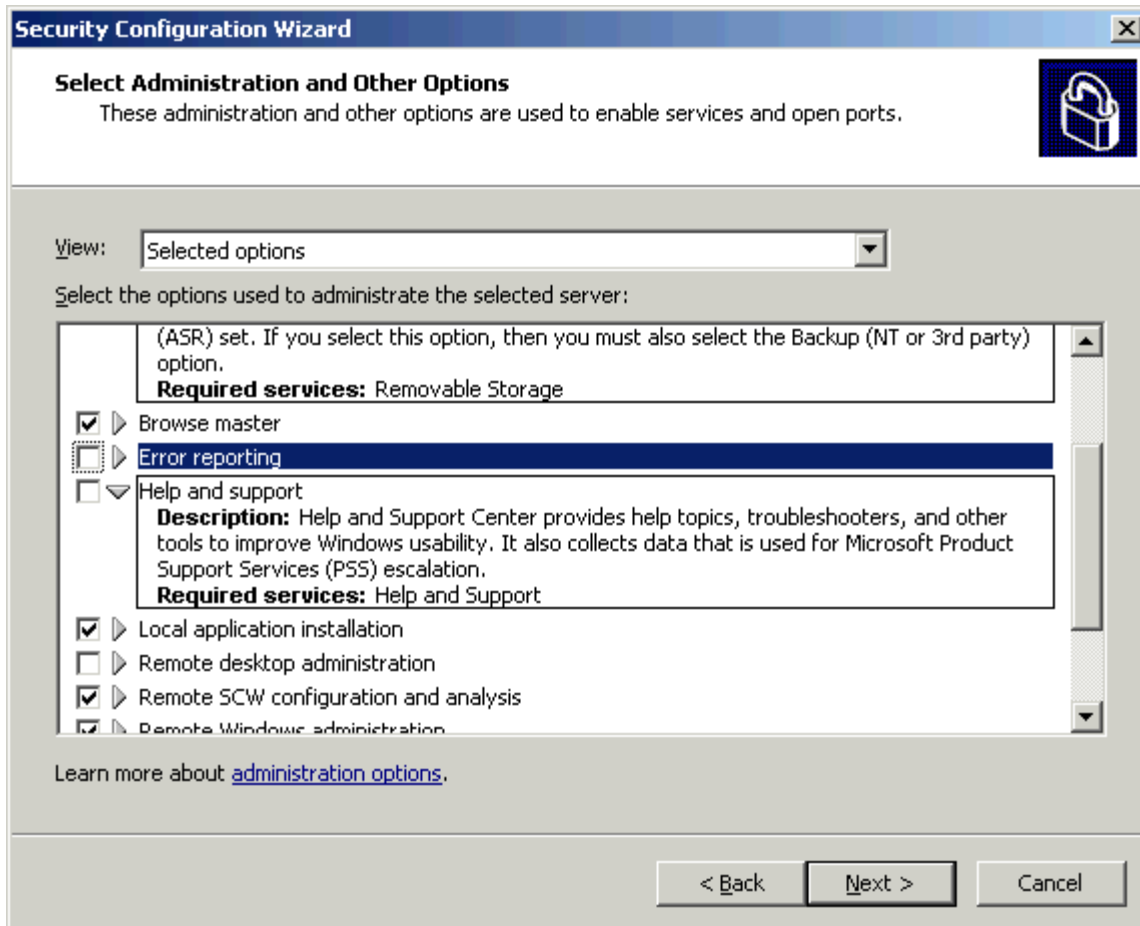
Out next step would be to determine what to do with unspecified services, that is services not installed in the server or not identified by the Security Configuration Database. We have two options:

- Do not change the startup mode of the services
- Disable the service

If you decide to leave the services alone, nothing will change and if new services are installed at a later time, the Security Configuration Wizard will ignore them. In the other hand, if you decide to disable the services, then every time you install a new service in the server the policy will have to be edited to accommodate the new service in the policy. Select "Next" once a decision has been made.

This brings us to the end of the Role Configuration module of the wizard. A summary will display all install services ant the outcome base on the selected roles. You can view all services or filter to only services being affected by the wizard. Make sure this information is documented in your servers' configuration library, if any.

Network Security

Our next section would be the configuration of Network Security. If you decide to complete this section, Windows Firewall will be enabled and can possible brake a few things in your server if not implemented correctly. Within this section, ports can be secure or block depending on the requirements. A benefit of configuring this section is that application can manage ports as needed. For example, if an application uses a specific port, the Security Configuration Wizard will give authority to the application to use the port as needed and block it when it is not being use. A function that I find extremely useful and if configure properly the security risk of the server will drastically decrease.

To proceed to the configuration of Network Security uncheck the "Skip this section" box and click "Next". This will bring you to the list of opened ports and approved applications. Here you can select the ports you want configured, the applications you want approved for port management and set advance port setting. The advance options give you more flexibility to secure independent ports. Ports can be configured to accept traffic from only approved list of remote addresses and physical device. When finish configuring the ports, click "Next" to display the status of the port, security options and restriction. This concludes the Network Security block, click Next to move on to Registry Settings.
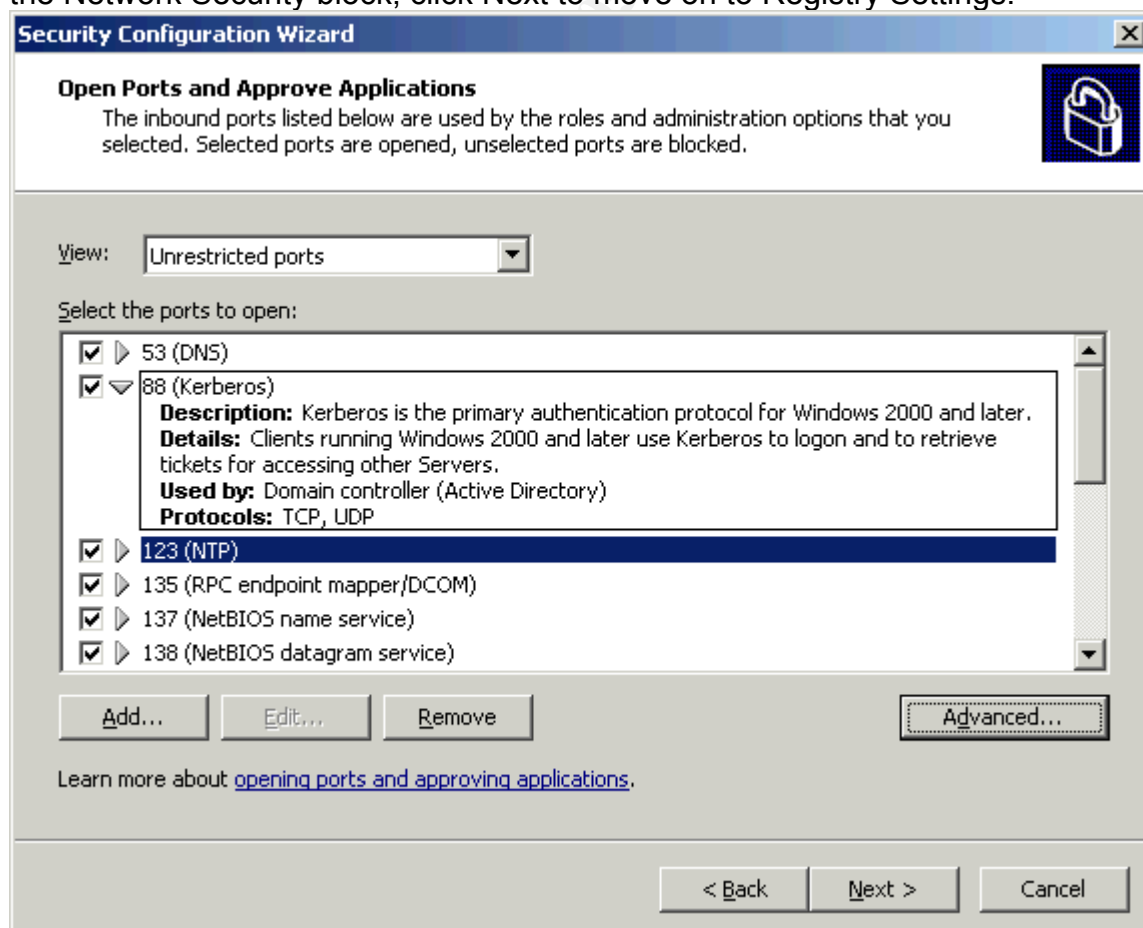
Registry Settings

This section asks a serious of question to determine different registry settings listed below:

- Required SMB security signatures
- Required LDAP signing
- Outbound authentication methods
- Outbound authentication methods using domain accounts
- Outbound authentication using local accounts
- Inbound authentication methods

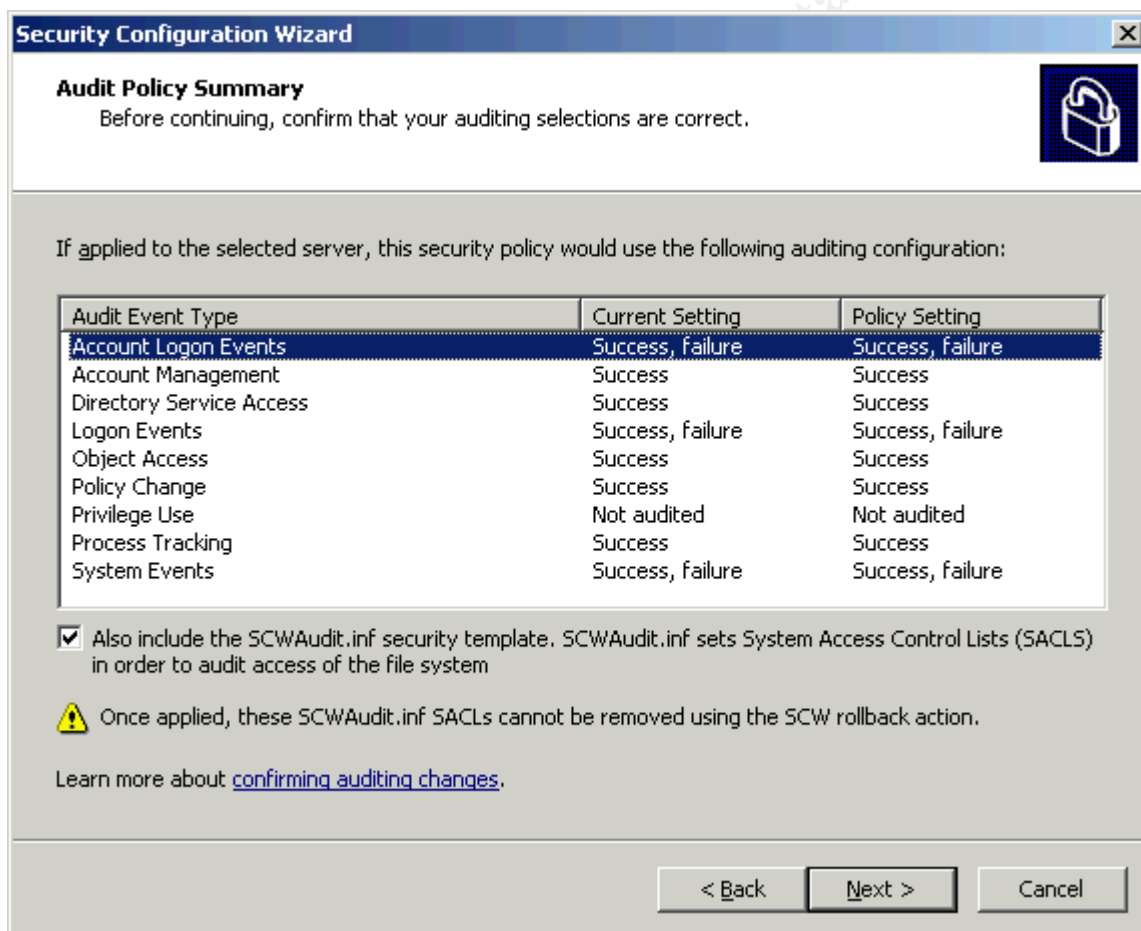This section concludes with a summary of all registry setting that will be implemented.
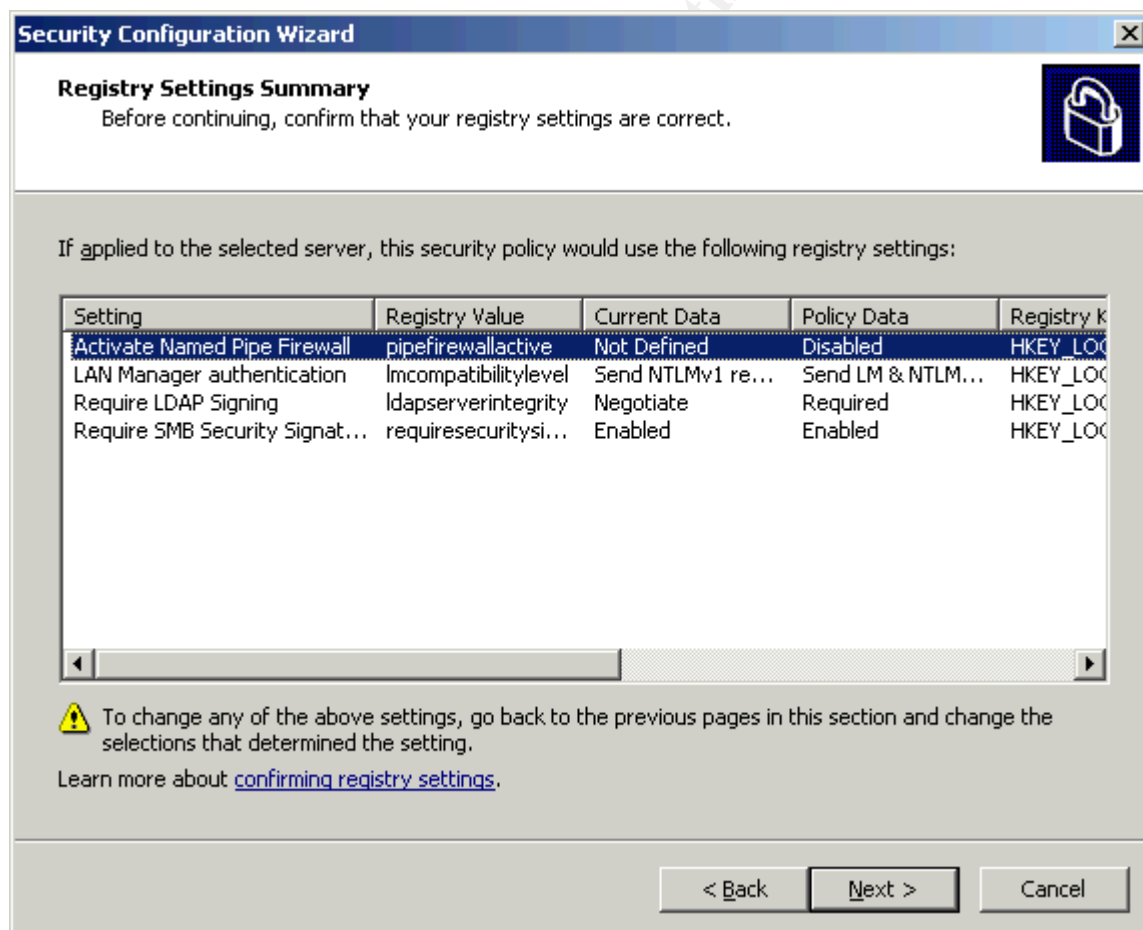
Audit Policy

This section allows for audit configuration on the server. The Security Configuration Wizard provides you with three options listed below:

- Do not audit
- Audit successful activities - "Use this option to record only what users actually access, not what they try to access" (SCW Help Pages)
- Audit successful and unsuccessful activities: not recommended since it would generate too many logs and clutters useful information.

"Do not audit" is a choice you never want to select unless you find a justifiable need for no audits. Base on your organizations need, select the best option and click "Next". For the purpose of this lab I will select "Audit successful activities".

The last page of the Audit Policy will display a summary of the current audit setting as well as the recommended policy settings. Select "Next" when finished reviewing the audit policy.

Note: The SCWAudit.inf is not an effective file, I recommend not checking this box and creating your own inf file using the Security Configuration and Analysis
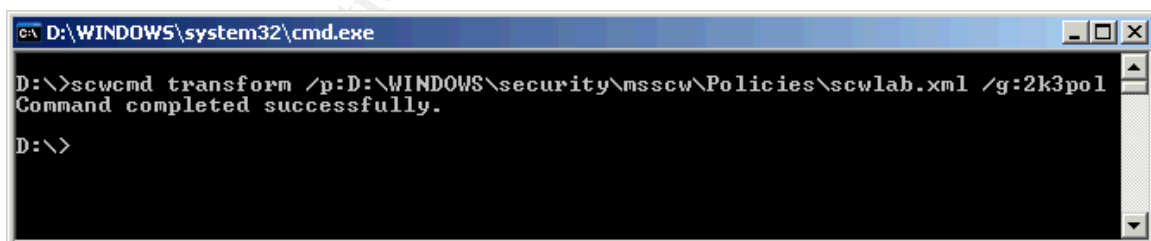
tool. The SCWAudit.inf will set "Overwrite events as needed" and set the permissions in multiple systems folders. The System Access Control List does not look harmful at a glance, but you might want to do more testing to verify that all the 72 access control entries modify by the inf file doesn't break anything.

Save Security Policy

Our final section allows us to save the policy, view the policy, import a Security Template and chose to apply now or later. It would be a wise idea to have the Security Template ready for deployment at this time. If no template is in place, I recommend creating one and later importing it to maximize the strength of your SCW security policy. If a conflict arises between the Security Template and the SCW security policy, then the SCW policy will take precedence over the template. Your last step is to apply the policy now or later. If you decide to apply now, the server will not have to be rebooted nor down time will be required, however, I recommend saving the policy and testing in a lab environment prior to deploying it in a network. You can later install the policy by running the SCW or executing the command-line tool.

Deploying the SCW policy with Active Directory

Deploying the SCW policy with Active Directory not as simple as creating the policy. A command-line tool is required for the policy to be imported into Active Directory. As stated by Microsoft, the SCW generated security policy is not natively understood by Group Policy and must be transform with the user of the "scwcmd transform" command. To execute the command you must first need to know the location of the xml file created by the SCW. The default location is "%systedrive%WINDOWS\security\msscw\Policies\". The command to transform the xml file is:


```
D:\>scwcmd transform /p:D:\WINDOWS\security\msscw\Policies\scwlab.xml /g:2k3pol
Command completed successfully.

D:\>
```

Once the command executes a Group Policy Object will be create and the new converted file will be imported in to it. The command arguments for importing the SCW security policy into Active Directory are:

- /p: location of xml file
- /g: name of GPO to be created by command.

The command-line tool also provides support for:

- analyze - determines if a machine is in compliance with a policy
- configure - applies a SCW policy to machines
- register - customizes the Security Configuration Database (SCD) or add to it from another SCD generated with new roles, ports, and services.
- rollback - resets the policy to its previous state
- view – display the xml policy with the SCW Viewer tool. It can also be printed from the viewer.

Conclusion

As mention earlier, the Security Configuration Wizard is not the solution to all your security problems. The SCW by itself is just another tool. The strengths are show when it is properly implemented with the help of a well written security plan. Microsoft kept their promise when stating that the SCW will "reduce the attack surface of Microsoft Windows Server".

References

Law, Fiona."Windows 2003 Group Policy Security"31 May 2004.SANS Institute.27 December 2005 <http://www.giac.org/practical/GSEC/Fiona_Law_GSEC.pdf>

Windows XP Professional Product Documentation."Security Configuration and Analysis"©2005 Microsoft Corporation.23 December 2004<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/sag_scmtopnode.mspx>

Microsoft Technology Center."Security Configuration Wizard for Windows Server 2003"©2005 Microsoft Corporation.12 December 2004<http://www.microsoft.com/windowsserver2003/technologies/security/configwiz/default.mspx>

Melber, Derek." Security Configuration Wizard in Windows Server 2003 Service Pack."20 January 2005.Windowsecurity.com.23 January 2005<http://www.windowsecurity.com/articles/Security-Configuration-Wizard-Windows-Server-2003-SP1.html>

Melber, Derek. "Ensuring Group Policy Security Settings Are Consistent" 15 December 2004.Enterprise Systems.01 February 2005<http://esj.com/security/article.aspx?EditorialsID=1224>

Student Manual:Windows 2000 Professional and Server Administration Principles W2PS-STMN-0013A.St. Louis, Misouri:Wave Technologies International,Inc.,2000.

Danseglio, Mike.Securing Windows Server 2003.Sebastopol, CA:O'Reilly Media Inc.,2005.

Security Configuration Wizard Help Pages.©2005 Microsoft Corporation. November 2004.