Global Information Assurance Certification Paper

Quick Guide to IIS Web Server Security

GSEC Practical Assignment Version 1.2d
Brian LeVasseur
July 19, 2001

With more and more companies placing their business on line, whether it's e-commerce or B2B, System Administrators have to learn how to secure their systems on the fly. Keeping systems up and running is difficult enough without having to make sure that someone with ill intentions does not bring them down. So where does the busy Systems Administrator go to acquire the knowledge needed to protect their systems and calm the rising fears of management? The fastest way to beat the learning curve is to learn from those who have done it. I am a systems administrator who took over an e-commerce/B2B "web farm" six months ago. Prior to this position, I was the SMS (Microsoft Systems Management Server) administrator. All the servers and software I worked on resided behind the corporate firewall in the corporate private network. I had very little experience with IIS and I was even less knowledgeable about firewalls. Fortunately, I was not responsible for the firewall just the web servers. Unfortunately, the previous administrator had not implemented any form of security, and management wanted that changed immediately. For all of the Systems Administrators that find themselves in this type of situation, I hope my experiences can help.

Where To Start

Where did I start? Even though I knew very little about security, I knew that IIS was my biggest concern. Therefore, I started my journey through security by researching IIS security vulnerabilities. At the time Microsoft provided a web page that simply listed all of the known security bulletins for all of their products. I had to wade through them and research the ones that looked relevant. Now, the Microsoft site allows you to choose the product and service pack, then a list of security bulletins relative to your specifications is listed.

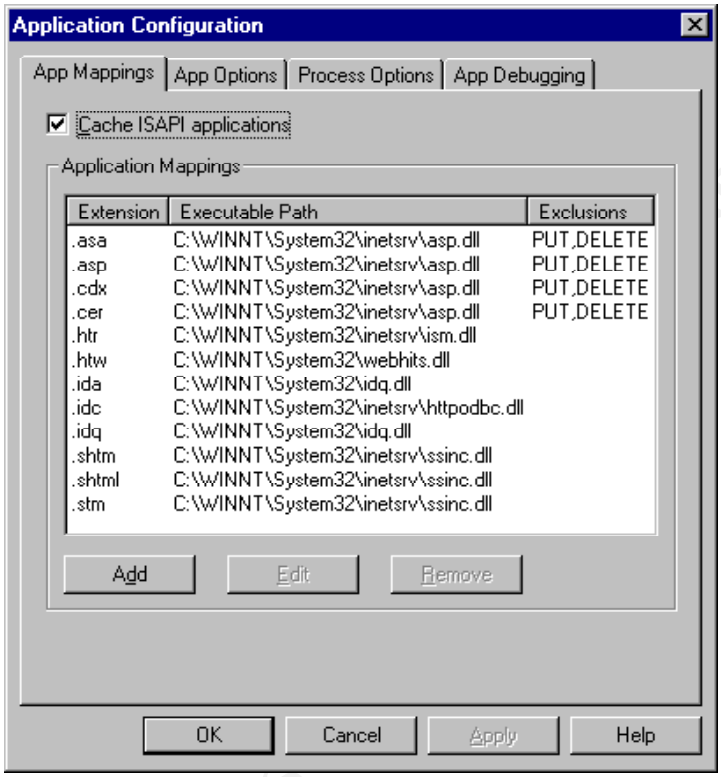
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/current.asp

I give Microsoft two thumbs up for their new security page. It would be well worth your while to review all the security bulletins for IIS, but for the system administrator in a hurry there are four bulletins and hot fixes you must spend some time with. Security bulletins MS99-025, MS99-013, MS01-026 and MS01-033 are the critical security bulletins regarding IIS. Similar to their web site for security bulletins, Microsoft finally got their act together and released MS01-026, a cumulative security hot fix for IIS. While MS01-026 takes care of IIS 5, it does not completely cover IIS 4. MS99-025 and MS99-013 are critical hot fixes for IIS 4. All of the aforementioned hot fixes, except MS99-025, require you to download an executable and run it on your server. MS99-025 requires you to delete a few registry keys, assuming you do not need RDS functionality. If you do use RDS, read MS99-025 for an alternative fix, otherwise delete: [1]

- HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch \RDSServer.DataFactory
- HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch \AdvancedDataFactory
- HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Services \W3SVC \Parameters \ADCLaunch \VbBusObj.VbBusObjCls

MS01-033 was released after MS01-026 and therefore must still be applied if the idq.dll (Indexing ISAPI) has not been removed. A good rule of thumb is to remove all ISAPI

extensions that are not used. [2] Several exploitations, including an IIS worm, use ISAPI extensions to create a buffer overflow and take control of the machine. [3] For more information on ISAPI extensions, see (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/iisref/html/psdk/asp/isgu80v9.asp). For the system administrator in a hurry, removing ISAPI extensions can be accomplished by opening the property page for your web server. Make sure you do this for the server and not an individual web site, unless some sites use ISAPI extensions that other sites do not. Right click the server name in the IIS MMC and select "Properties". Under "Master Properties" edit "WWW Service". Click on the "Home Directory" tab. Click on "Configuration". You should see a window similar to the following.



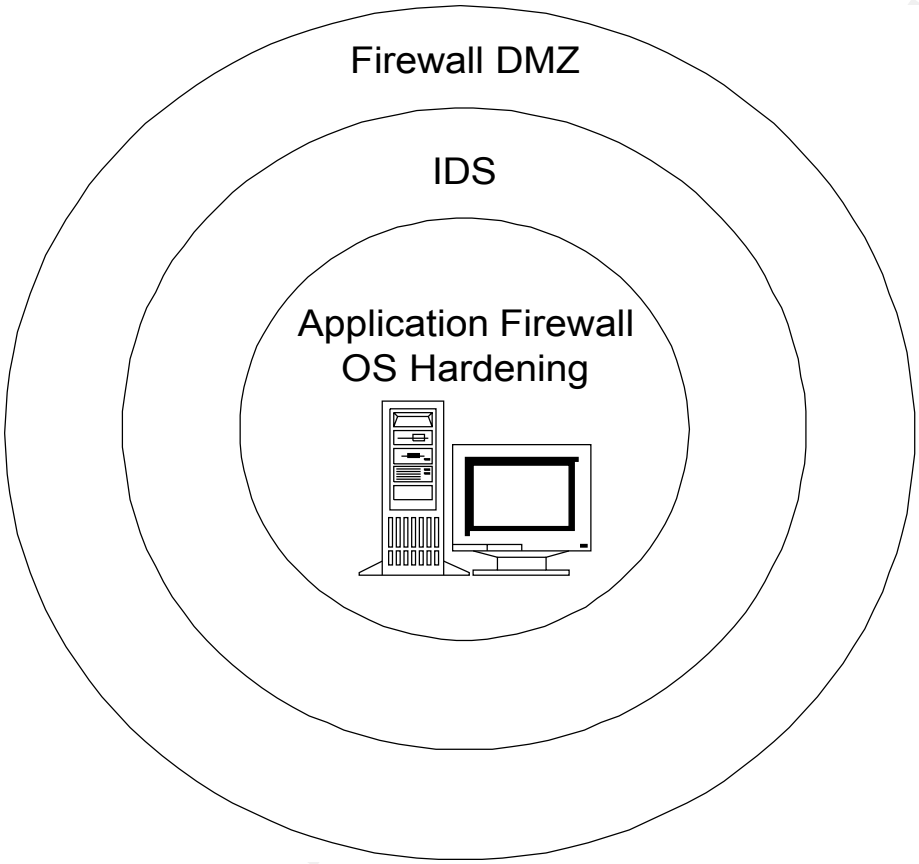
Remove all the Application Mappings that are not needed.

Defense in Depth

There is much more to securing IIS than what I have covered, but applying the current hot fixes and removing unused ISAPI extensions will get you ahead of the learning curve quickly. For a thorough checklist on securing IIS, review the "Microsoft Internet Information Server 4.0 Security Checklist".

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iischk.asp

While researching IIS security, I learned that I was just scratching the surface on security as a whole. The most important concept I came to understand is "Defense in Depth". In other words, multiple layers of security should be implemented. [4] One should consider security efforts as a means of slowing a hacker down. Using layers of security will enable you to detect intrusions and stop them before your systems are compromised. The most common strategy for "Defense in Depth" is diagramed below.



First Layer

First layer (perimeter) of defense is a DMZ (Demilitarized Zone). A DMZ is a network segment that is isolated from the rest of the network by two or more firewalls. The DMZ resides between two firewalls. Optimally, the firewalls should be from different vendors. This way, a hacker has to find his or her way through two different products. The heart of the DMZ is the firewall. In simple terms, the firewall resides between your private network and the Internet and uses rules to control and filter ingress and egress traffic. Check Point Firewall-1 (http://www.checkpoint.com/products/firewall-1/index.html) is the industry leader. For most IIS installations, you want the firewall to allow ingress traffic to access port 80 and

443 on your server. However, you do not want the firewall to allow egress traffic from your servers to access the Internet. This will prevent a hacker that has compromised your system from being able to download hacking tools from the Internet onto the compromised system. The firewall is a very important first layer of defense, but it is not invulnerable. CERT recently issued a security warning for Check Point FireWall-1. [5] Just like IIS, your firewall should be updated with the latest patches.

Second Layer

Second layer of defense is an IDS (Intrusion Detection System). Unlike the firewall, an IDS is not concerned with the direction, source, or destination of traffic. It looks at the content of traffic, files on the host, and at logs generated by applications and the OS. The IDS analyzes this data for signs of malicious activity. Tripwire (http://www.tripwire.com/products/servers/index.cfml) and ISS (http://www.iss.net/securing_e-business/security_products/intrusion_detection) are examples of Intrusion Detection Systems. Snort (http://www.snort.org) is a very popular and free IDS. My current IDS is comprised of freely available security tools. A commercial IDS such as those provided by Internet Security Systems and Tripwire would provide a more robust IDS and require less administration and development. My current IDS consists of the following:

NTLast (http://www.foundstone.com/rdlabs/proddesc/ntlast.html)
- Checks for Administrator account logons within last 24 hours
- Checks for failed logons within last 24 hours

Fscan (http://www.foundstone.com/rdlabs/proddesc/fscan.html)
- Checks for open ports

Fport (http://www.foundstone.com/rdlabs/proddesc/fport.html)
- Reports all open TCP/IP and UDP ports and maps them to the owning application

NetSvc
- Checks for changes in installed services

I developed a wrapper for the above tools with Visual Basic. The wrapper allows me to automate the use of the tools and generates email alerts when specific conditions are found. Perl and most other languages can provide this same functionality.

Tripwire (Soon to be installed. http://www.tripwire.com/products/servers/index.cfml)
- "Monitors file changes, verifies integrity, and notifies you of any violations of data at rest on network servers" [6]
- "Monitors all file changes—regardless of whether they originated inside or outside of

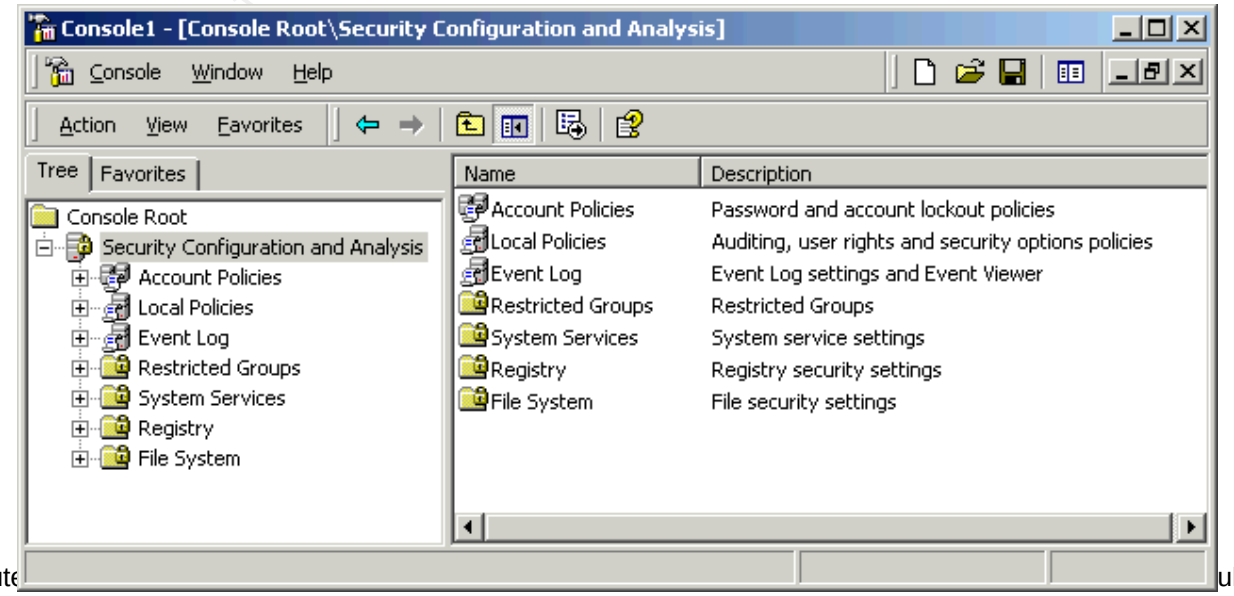
your organization" [6]

- "Identifies changes to system attributes including file size, access flags, write time, and more" [6]
- "Enables the establishment of network policies that detect intentional tampering, user error, software failure, and introductions of malicious software, as well as "open doors" for robust protection of critical systems" [6]

Third Layer

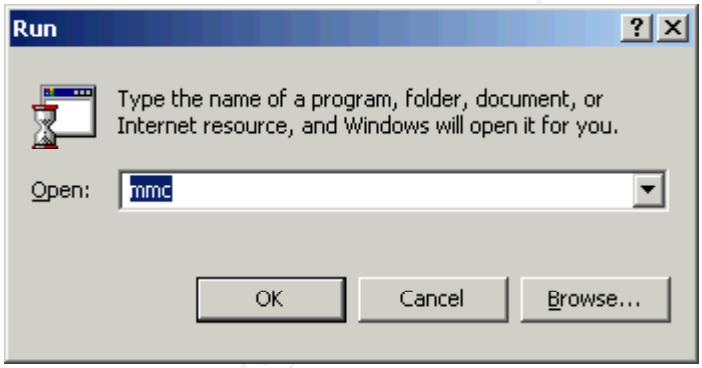
Third layer of defense is OS hardening and application/host based firewalls. The NT operating system is not secure by default. It must be hardened and have the latest patches applied. OS hardening can be quickly implemented via Microsoft Security Configuration Manager (SCM). SCM is provided on the NT 4.0 Service Pack 4 CD or you can download it from http://www.microsoft.com/NTServer/nts/downloads/recommended/scm/default.asp. Windows 2000 has SCM built in. After installing SCM on NT 4.0, you need to create a security template or use one of the templates provided by Microsoft. It is **VERY** important to remember that once a security template is applied to the system, the majority of it can not be unapplied. The only way to un-apply a security template is to manually back out each individual change. After reviewing the templates provided by Microsoft, you will understand how daunting of a task it would be to back out any of them. Microsoft highly recommends that you test their templates on a non-production system. I strongly agree. There is no substitution for testing, but the reality for many administrators is that the time and resources required for testing do not exist. For the administrator that finds him or herself short on time and resources, I recommend creating your own template using Microsoft's template as a guide. SCM allows you to configure the following seven areas:

1. Account Policies
2. Local Policies
3. Event Log
4. Restricted Groups
5. System Services
6. Registry
7. File System

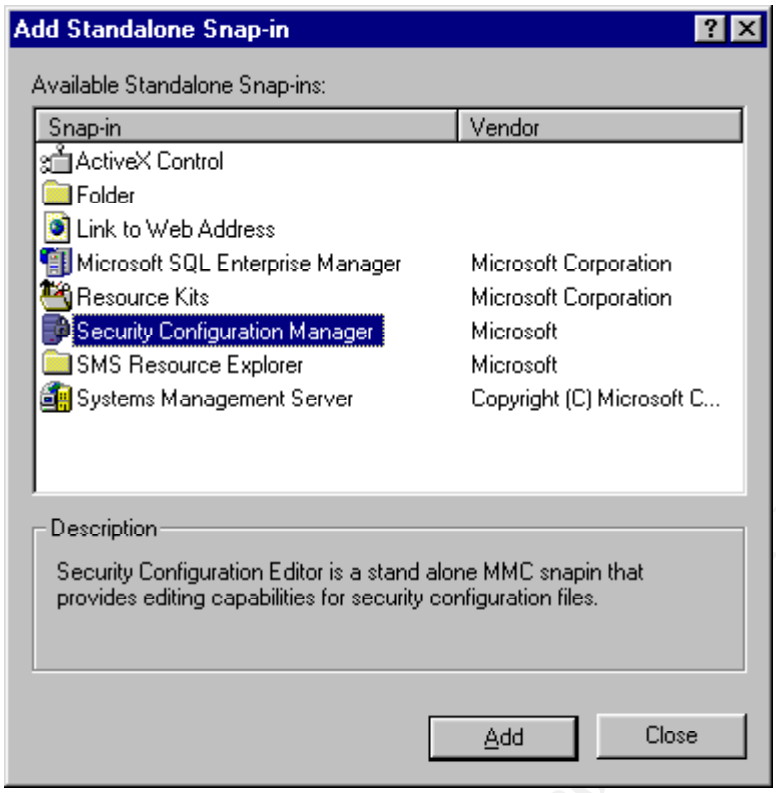


SCM in Windows 2000

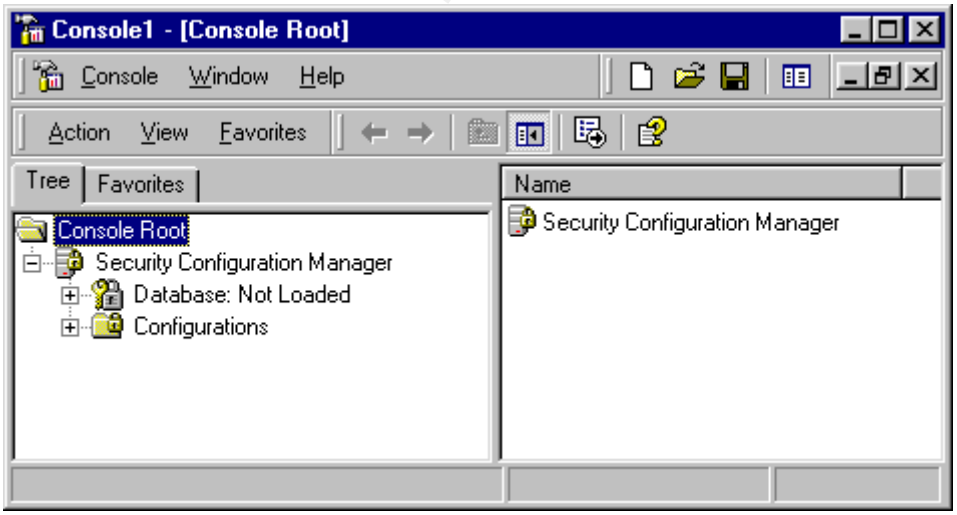
Creating a template that only configures Account Policies, Local Policies, Event Log, and System Services will provide you with a good degree of security quickly. These areas are easily configured and can be backed out via SCM. Once you have applied your custom template, you can add Restricted Groups, Registry, and File System as you find time to research them. I recommend applying changes to these areas one at a time as they can not be backed out via SCM and can cause your system to crash. In order to find the security configurations that need to be made as soon as possible, I ran Nessus (http://www.nessus.org/index.html) against my server and used its report to help me configure my SCM template. Any security scanner can help you decide what should be secured via SCM first. Retina Security Scanner (http://www.eeye.com/html/Products/Retina/index.html) is a very easy to use Windows based security scanner and can be used free for 15 days.
To use SCM on NT 4.0, download it from the Microsoft web site. The version that comes with SP 4 is not current. Therefore, make sure you acquire the latest version from the Microsoft site.
(http://www.microsoft.com/NTServer/nts/downloads/recommended/scm/default.asp)
After installing SCM, click "Start", then "Run", type in "MMC", and click "OK".



Once the MMC displays, click "Console", click "Add/Remove Snap-in", click "Add", and you should see the following window.

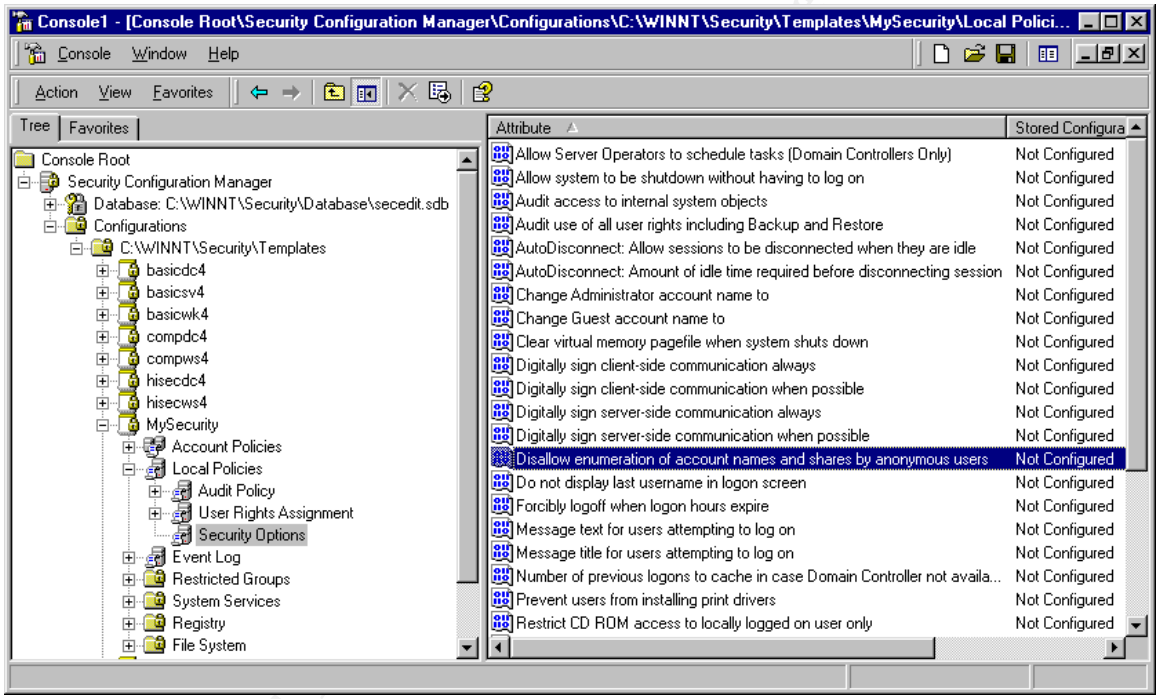


Select "Security Configuration Manager" and click "Add". Close the "Add Standalone Snap-in" window and click "OK" on the "Add/Remove Snap-in" window. You should now see the following:

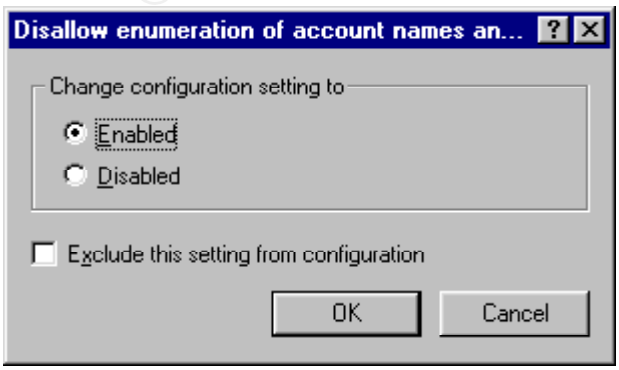


Notice that the database says *Not Loaded*. You can now configure your system with one of

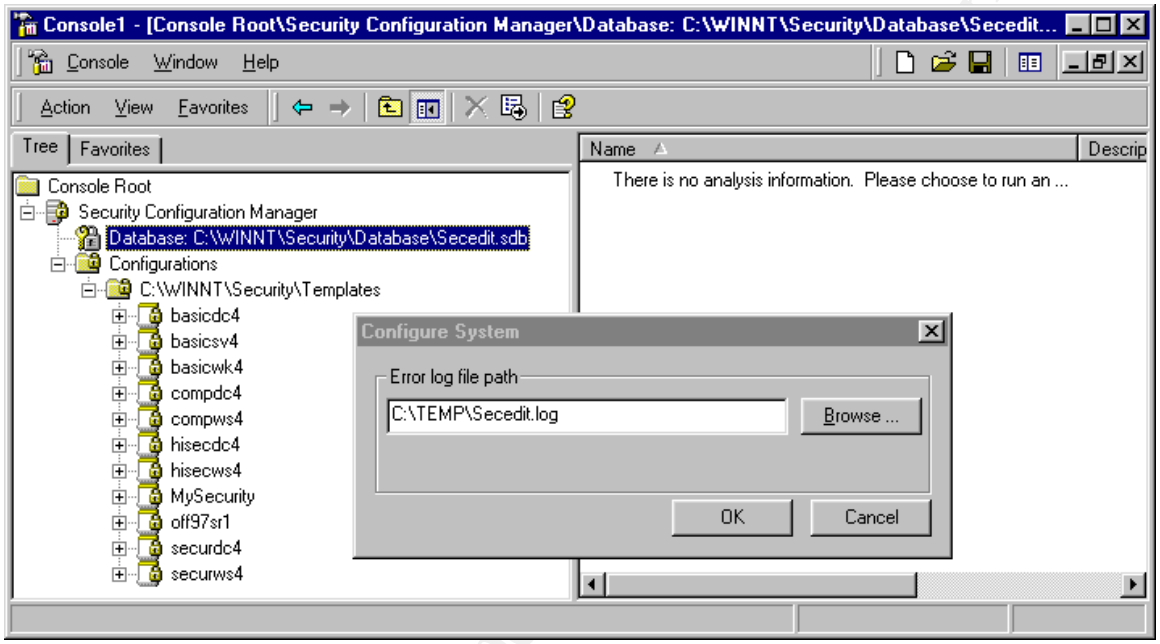
the templates provided by Microsoft or you can create your own. To create your own, right click on the templates folder and select "New Configuration". Enter in a name and description and click "OK". You should now see your custom template listed with the others. Remember that you can quickly and easily configure the Account Policies, Local Policies, Event Log, and System Services portions of your custom security template. Configuring and applying these components now will close several well-known vulnerabilities. When you have more time you can research the other sections of the security template. To configure SCM to prevent the anonymous enumeration of accounts and shares, expand your custom security template and double click the attribute "Disallow enumeration of account names and shares by anonymous users". This attribute is located in "Security Options" under "Local Polices".



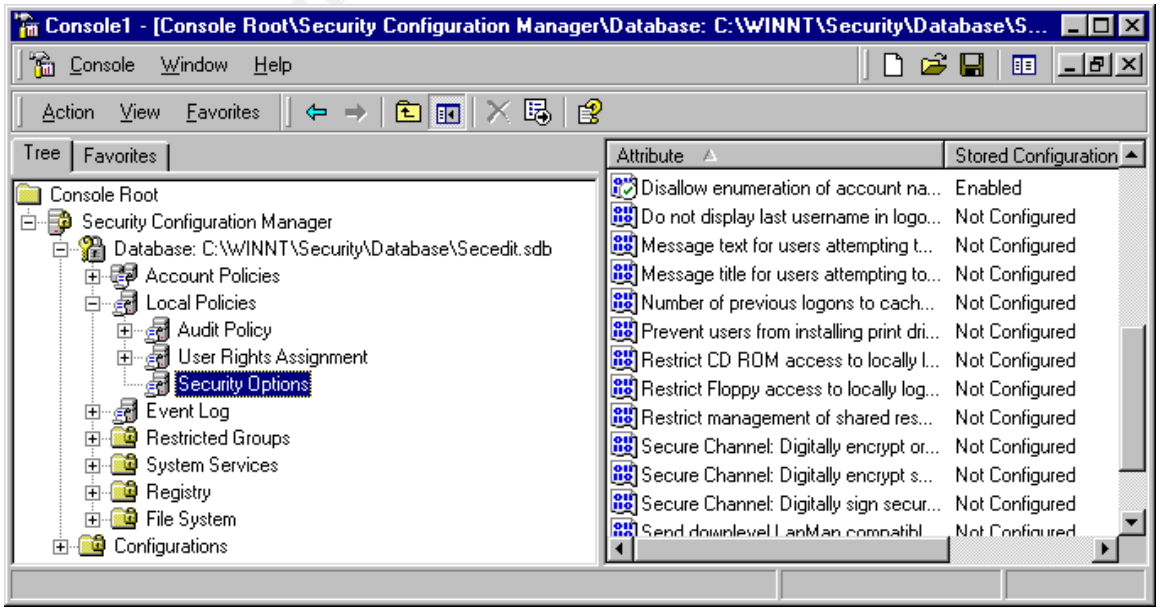
To enable this attribute, uncheck the "Exclude this setting from configuration" box, select "Enable", and click OK.



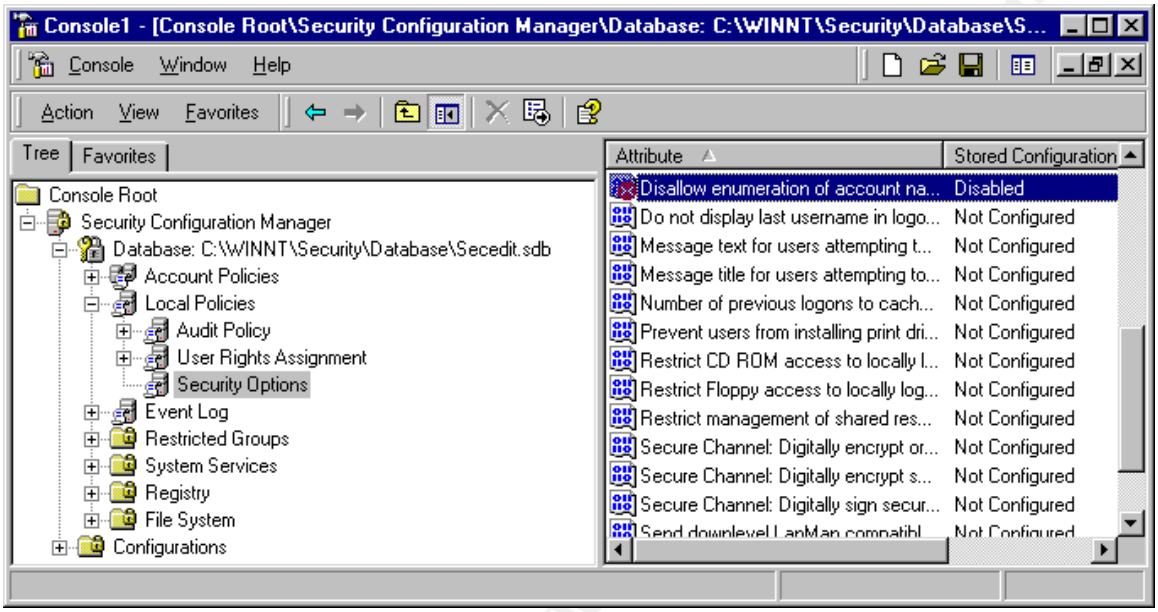
After configuring the rest of the attributes under Account Policies, Local Policies, Event Log, and System Services, save your template. Save your template by right clicking on it and selecting save. Once you have created a template, you apply it to the system by right clicking on the Database icon and selecting "Import Configuration". After importing a template, you apply it to the system by right clicking on the Database icon and selecting "Configure System Now". Click ,"OK" to confirm the error log location.



To view or change the current configuration, right click the Database icon and select "Analyze System Now". Click "OK" to confirm the error log location. You can now expand the current database configuration as you did your template. Expand the database and view the "Disallow enumeration of account names and shares by anonymous users" attribute. You will notice that it has a green check mark on it.



The check will turn into a red "X" if you manually change the attribute in the registry and then reanalyze the system. This feature allows you to quickly see if any of your security configurations have changed.



To access SCM that is built into Windows 2000, Click "Start", "Run", and then type in "MMC" and click "OK". Click "Console", "Add/Remove Snap-in", "Add", and add the "Security Configuration and Analysis" Snap-in and the "Security Templates" Snap-in. Click "Close" and "OK". Notice that SCM is actually named "Security Configuration and Analysis" under Windows 2000. For simplicity, I will continue to use SCM. Now that SCM and the SCM security templates are loaded in the MMC, double click "Security Configuration and Analysis" and follow the directions to create a new database. The procedures for creating and applying a custom security template under Server 2000 is the same for NT 4.0.

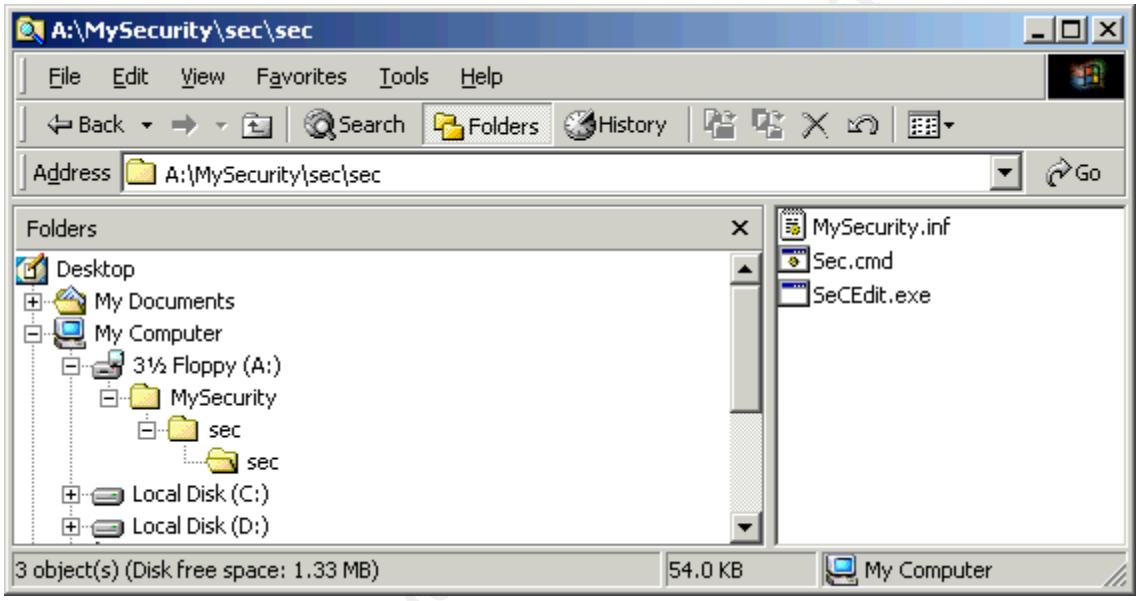
Below is a list of templates provided by Microsoft SCM for NT 4.0. They are located under WINNT\security\templates. Sever 2000 comes with a few more templates. **Remember to test these templates before applying to production systems.**

Configuration File	Security Level	Platform
Basicwk.inf	Default	NT4 Wksta
Basicsv.inf	Default	NT4 Server
Basicdc.inf	Default	NT4 DC
Compws4.inf	Compatible	NT4 Wksta\Server
Compdc4.inf	Compatible	NT4 DC
Securws4.inf	Secure	NT4 Wksta\Server
Securdc4.inf	Secure	NT4 DC
Hisecws4.inf	High Security	NT4 Wksta\Server
Hisecdc4.inf	High Security	NT4 DC

Off97SR1.inf	w/ Compatible	NT4 Wksta\Server

The SCM GUI is easy to use but requires a lot of time when dealing with many servers. In order to apply security to your servers quickly, we need to automate the process. SCM can be executed from the command prompt, not just the GUI, once it has been installed. To manage multiple servers, you can create a cmd file to copy the needed security files to your servers. Once the files have been copied to your servers, you only need to execute the script that you just copied. Remember that you have to install SCM on all servers first. This only applies to NT 4.0 as SCM is built in to Server 2000.

Create a directory named "MySecurity". Create a directory named "Sec" inside "MySecurity". Create a directory named "Sec" inside "Sec".



Create a file named Sec.cmd in MySecurity\Sec\Sec. Paste the following without the quotes into Sec.cmd.

"secedit.exe /configure /cfg mysecurity.inf /overwrite /log c:\temp\Sec.log /verbose"

Copy your security template and SeCEdit.exe into MySecurity\Sec\Sec. SeCEdit.exe can be found under WINNT\System32 on a machine that has SCM installed on it. Even though SeCEdit.exe is already in the path, I still place it in the directory with my security template to help keep my scripts simple. Then create a file named CopySec.cmd in the MySecurity directory and paste the following text into CopySec.cmd. You can add servers as needed.

```
xcopy sec \\server1\c$ /s
xcopy sec \\ server2\c$ /s
xcopy sec \\ server3\c$ /s
xcopy sec \\ server4\c$ /s
```

Executing CopySec.cmd will copy the innermost Sec directory and its files on to the C drive of the servers listed in CopySec.cmd. Once the Sec directory and its files are on your servers, execute Sec.cmd on each server to apply your security template.
This process can be automated too. You can create a scheduled task on each server to apply the security template daily. That way you only need to execute CopySec.cmd in order to place your current security template on your servers. This method will also automatically reconfigure any changes made by hackers or other administrators. Keep in mind that a good hacker could change the code in your CopySec.cmd and have it run with Administrator privileges. You could also create a cmd file that would execute soon.exe against all of your servers. Soon.exe is a command line utility that allows you to schedule tasks, to execute in the very near future, on remote machines. It can be found in the NT resource kit. There is more to SCM than what I have covered, but you should now be able to quickly use it to apply another layer of security on your systems.

Host Firewall

After hardening the OS, an application and/or host-based firewall should be installed. SecureIIS (http://www.eeye.com/html/Products/SecureIIS/index.html) is an example of an application firewall. It is designed to monitor a specific application and protect it from malicious actions. A host-based firewall is similar to the firewall implemented in the DMZ, except that it resides on the server and only polices traffic to and from that server. Black Ice Defender or Black Ice Agent for servers (http://www.networkice.com/products/blackice_agent.html) is a good example of a host-based firewall.

Data Security

Data security is the process of securing data that resides on a server or is in transit. Encrypting customer information that is stored in a SQL database that supports an e-commerce web site is a good example of data security. Solutions such as the Entrust Secure Enterprise Solution family (http://www.entrust.com/truepass/features.htm) provide a mechanism for securing resident data. This is not a quick security solution to implement but should be seriously considered. Data security is especially important for e-commerce web servers.

Application Security

Applications are the source of most vulnerabilities. Applications, such as IIS, listen for requests on a specific port. Therefore, the firewall must allow ingress traffic to pass through to that port. With the firewall out of the picture, the application must provide its own security. Unfortunately, instead of providing security, applications are notorious for containing vulnerabilities like buffer overflows and dangerous sample code. Staying current

with security patches is the best defense.

Maintenance

Once a security system is in place, it must be maintained. New vulnerabilities are constantly being discovered. For example, Microsoft released two bulletins (MS01-026, MS01-023) in May 2001 that identify vulnerabilities in IIS that would allow hackers to compromise and take control of affected server. Maintenance is the most important aspect of security, but it is very resource consuming. Six crucial aspects of security maintenance are:

1. Keeping abreast of new vulnerabilities
2. Patching new vulnerabilities
3. Patching known vulnerabilities
4. Scanning your systems for vulnerabilities
5. Penetration testing your systems
6. Knowing your systems

Keeping abreast of new vulnerabilities is accomplished by subscribing to security mailing lists. Some recommended mailing lists that should be monitor are:

NT BugTraq
http://www.ntbugtraq.com/
Select "subscribe" under the Quick Links.

BugTraq
http://www.securityfocus.com/
Select forums, bugtraq, faq for details on subscribing.

Microsoft Security Notification Service
http://www.microsoft.com/security/services/subscribe.asp

NT Security
http://www.ntsecurity.net/

Allaire Security Notification Service
http://www.allaire.com/developer/securityzone/NotificationService.cfm
For those who run Coldfusion

SANS
http://www.sans.org/aboutsans.htm#1

Scanning systems and performing penetration tests confirm that our security measures are working against known vulnerabilities. Scanning should be performed from both inside the network and from the Internet. Scanning on a regular basis would alert us if a server had been reinstalled and not secured or if we missed a patch for a new vulnerability that the scanner is aware of. I use the Nessus security scanner (http://www.nessus.org/index.html). Nessus is an open source, free security scanner that runs on Linux. Nessus was rated as one of the best scanners by Network Computing. [7] For those of us that do not have to time to learn Linux, I recommend using the Retina Security Scanner (http://www.eeye.com/html/Products/Retina/index.html). It is very easy to use and you can try it for free for 15 days.

Summary

Security administration is an ever-changing process. For most Systems Administrators it is a new responsibility. Corporations are placing more and more of their business data online, yet few if any are considering the implications until it is too late. Then, management expects the Systems Administrator to suddenly become a security expert and secure their systems overnight. Unfortunately, the scope and complexities of security can not be learned overnight. On the other hand, certain utilities and procedures can be comprehended and implemented quickly to provide a reasonable degree of security. The hard part is knowing where to start. Once the quick fixes are in place, the Systems Administrators should continue their education in security and start applying layer upon layer of security methods. This process of "Defense in Depth" will gradually build a very strong wall around your information systems.

Acronyms

B2B – Business to Business
CD – Compact Disk
DMZ - Demilitarized Zone
GUI - Graphical User Interface
IDS - Intrusion Detection System
IIS – Internet Information Server
ISAPI - Internet Server API
ISS – Internet Security Systems
MMC – Microsoft Management Console
OS – Operating System
RDS – Remote Data Service
SCM -Microsoft Security Configuration Manager
SMS - Microsoft Systems Management Server
TCP/IP – Transmission Control Protocol/Internet Protocol
UDP – User Datagram Protocol

Glossary of Terms

Application/host based firewalls - similar to the firewall implemented in the DMZ, except that it resides on the server and only polices traffic to and from that server.
Demilitarized Zone (DMZ) - a network segment that is isolated from the rest of the network by two or more firewalls.
e-Commerce - conducting business on the Internet.
Egress – outbound traffic.
Firewall - a system designed to prevent unauthorized access to or from a private network.
Hot fix – an update to a software package that fixes a specific problem. They are released between service packs.
Ingress – inbound traffic.
Intrusion Detection System (IDS) – monitors the content of traffic, files on the host, and at logs generated by applications and the OS.
OS hardening – applying service packs, hot fixes, and configuration changes to the operating system in order eliminate known vulnerabilities.
Registry keys - a database used by the Windows operating system (Windows 95 and NT) to store configuration information.
Service pack - an update to a software version that fixes an existing problem, such as a bug, or provides enhancements to the product that will appear in the next version of the product.
Systems Administrator - an individual responsible for maintaining a multi-user computer system, including a local-area network (LAN).
Web farm - a group of networked servers that are housed in one location.

References

1 **"**Microsoft Security Program: Frequently Asked Questions: Microsoft Security Bulletin (MS99-025)"

"http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/fq99-025.asp"

2 "Microsoft Internet Information Server 4.0 Security Checklist"
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/security/tools/iischk.asp

3 ".ida "Code Red" Worm"
http://www.eeye.com/html/Research/Advisories/AL20010717.html

4 "Securing E-Commerce: An Overview of Defense In-depth**"**
http://www.sans.org/infosecFAQ/start/sec_ecom.htm

5 "FireWall-1 users feel the heat from security bug"
http://www.theregister.co.uk/content/55/20285.html

6 "Tripwire for Servers - Assuring Integrity of Servers and Data at Rest"
http://www.tripwire.com/products/servers/index.cfml

7 "Vulnerability Assessment Scanners "
http://www.nwc.com/1201/1201f1b1.html