Global Information Assurance Certification Paper

Hisecweb.inf – An Analysis
Colleen L'Abbe
November 23, 2001

Introduction

The task of securing IIS is much simpler due to the fact that many of the settings found in NT 4.0 and IIS 4.0 are disabled by default in Windows 2000 and IIS 5.0. The other reason is that many of the system settings are now configurable through a security policy template that Microsoft provides, called hisecweb.

The hisecweb security template is not part of the base security templates that are installed with Windows 2000. It is available for download from Microsoft and is recommended as part of the IIS 5.0 security checklist.

This security policy should not be implemented without first analyzing the changes that it makes to your system and a backup of the system is recommended, as the changes cannot be automatically reversed.

It is important to remember that security templates are incremental so applying hisecweb by itself does not complete secure your system. You should review all of the templates and determine which are appropriate for your installation.

When using the hisecweb template, the following assumptions are made:

- The computer is not a domain controller
- The computer is not part of a domain (standalone)
- The computer is a dedicated web server
- The computer is physically protected
- The computer has clean install of Windows 2000
- No modifications have been made to ACLS or user rights
- No one can log on locally except administrators
- No one can log on over the network
- Administrator and Guest accounts are not renamed

An analysis of hisecweb.inf

The only way to fully understand what changes the hisecweb security template makes, is to analyze each line of the inf file. The hisecweb security policy settings are summarized in the following tables. The settings are categorized into account polices, event log settings, local security policies, changes to services and finally other registry changes.

Account Policies – Password Policy	
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	2 day
Minimum password length	8 characters
Passwords must meet complexity requirements	Enabled
Store password using reversible encryption for all users in the domain	Disabled

Account Policies – Account Lockout Policy	
Account lockout duration	0 (administrator must unlock)
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Event Log – Settings for Event Log	
Maximum security log size	10240K
Restrict guest access to application log	Enabled
Restrict guest access to security log	Enabled
Restrict guest access to system log	Enabled
Retention method for security log	As needed

Local Policies – Audit Policy	
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Success, Failure
Audit system events	Success, Failure

Local Policies – Security Options	
Prevent users from installing printer drivers	Enabled
LAN Manager Authentication Level	Send LM & NTLM responses

Additional restrictions for anonymous access	No access without explicit anonymous permissions
Clear virtual memory pagefile when system shuts down	Enabled
Digitally sign server communication (when possible)	Enabled
Digitally sign client communication (when possible)	Enabled
Send unencrypted password to connect to third party SMB servers	Disabled
Secure channel: Digitally encrypt secure channel data (when possible)	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Enabled
Unsigned driver installation behavior	Do not allow installation
Disable Ctrl+Alt+Del requirement for logon	Disabled
Do not display last user name in logon screen	Enabled
Allow system to be shut down without logging on	Disabled
Restrict CD-ROM access to locally logged on user only	Enabled
Restrict floppy access to locally logged on user only	Enabled
Message text for users attempting to log on	This is a private computer system <add your own text>
Message title for users attempting to log on	A T T E N T I O N !
Audit use of backup and restore privilege	Enabled
Automatically logoff users when logon time expires	Enabled
Strengthen default permissions of global system objects	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Disabled

Changes to Services	
Alerter	Disabled
Clipbook	Disabled
Computer Browser	Disabled
DHCP Client	Disabled
Fax Service	Disabled

Internet Connection Sharing	Disabled
Messenger	Disabled
Netmeeting Remote Desktop	Disabled
Print Spooler	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Remote Registry Service	Disabled
Task Scheduler	Disabled
Telephony	Disabled
Terminal Service	Disabled
Infrared Monitoring	Disabled

Additional Registry Changes
MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\DisableWebPrinting=4,1 • disables support for the Internet Printing Protocol (IPP) • provides workaround for unchecked buffer security vulnerability (www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-023.asp
MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation=4,1 • disables 8.3 name creation on NTFS partitions • increases file performance • 16-bit applications may not be able to locate files and directories using long filenames
MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoShareServer=4,0 • prevents the creation of administrative shares (e.g. c$, d$, admin$, IPC$)

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect=4,0 • prevents Windows 2000 from altering its route table if ICMP redirect messages are sent to it from network devices such as routers
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableSecurityFilters=4,1 • allows IP security filters to be used • configure filtering through TCP/IP properties under Network and Dial-up Connections
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnableDeadGWDetect=4,0 • prevents TCP from performing dead-gateway detection and possibly asking IP to change to a backup gateway.
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\EnablePMTUDiscovery=4,0 • restricts the largest packet size (MTU) to 576 bytes for all connections that are not to the local subnet.
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\KeepAliveTime=4,300000 • controls how often TCP attempts to verify that an idle connection is still intact • sends a keep-alive packet and if the remote system is still functioning, it will acknowledge the keep-alive • only used if requested by an application.
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting=4,1 • prevents forwarding of source routed packets • tools such as tracert and ping use source routing

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1 • provides protection against denial of service attacks • reduces the number of retransmission retries and delayed route cache entries if the TcpMaxHalfOpen and TcpMaxHalfOpenRetried settings are met.
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxConnectResponseRetransmissions=4,2 • this value must be set at greater than or equal to 2, so that the TCP stack will read the registry values for syn-attack protection
MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions=4,3 • controls the number of times TCP retransmits an individual data segment before aborting the connection
MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\NoNameReleaseOnDemand=4,1 • protects against malicious name-release attacks by preventing the computer from releasing its NetBIOS name when it receives a name-release request from the network.
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\EnableDynamicBacklog=4,1 • enables the new dynamic backlog feature of afd.sys • afd.sys supports large numbers of connections in “half-open” (SYN_RECEIVED) state without denying access to legitimate connections
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MinimumDynamicBacklog=4,20 • sets the minimum number of free connections allowed on a listening endpoint
MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\MaximumDynamicBacklog=4,20000 • sets the maximum number of free connections allowed on a listening endpoint

MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters\DynamicBacklog GrowthDelta=4,10

- sets the number of free connections to create when additional connections are required

Problems introduced by hisecweb

In our implementation of hisecweb, we have encountered problems when upgrades are performed or new applications are installed on the server. Most of the problems relate to two specific registry settings:

- MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3Name Creation=4,1
  - This registry setting disables the 8.3 name creation on ntfs
- MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters\AutoSha reServer=4,0
  - This registry setting disables the creation of administrative shares such as c$ and d$

We have experienced problems where applications cannot install or be upgraded unless these settings are enabled. Once installed, the application runs fine with the settings disabled.

Security settings not changed by hisecweb

There are security settings that are not affected by the hisecweb policy. They include:

IPSEC policies
File, directory, and registry access control lists
Permissions on files, directories, and sites in IIS 5.0
Sample files and content directories

Conclusion

It is important to implement the hisecweb security policy as part of the overall security hardening of Windows 2000 and IIS 5.0 but it not the only step that should be taken. There are comprehensive checklists available that provide step-by-step instructions for complete protection.

It is also possible that hisecweb may implement changes to settings that you do not wish to be changed. It is important to review the template and make the necessary modifications so that it reflects your corporate policies.

References

David B. Koconis, “Comprehensive Review of Windows 2000 Security Policy Templates and Security Configuration Tool”, (http://www.ists.dartmouth.edu/IRIA/knowledge_base/sectemplates/sectemplates_full.htm), Institute for Security Technology Studies, Dartmouth College, , March 6, 2001,

William E. Walker IV, “Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0”, National Security Agency, June 19, 2001 Version 1.1.4

Microsoft Technet, “Security Configuration Manager Tools”, (http://www.microsoft.com/technet/treeview/default.asp?url=/Technet/prodtechnol/winxppro/proddocs/ALL_tools.asp)

Microsoft Technet, “Microsoft Windows 2000 TCP/IP Implementation Details”, (http://www.microsoft.com/technet/itsolutions/network/deploy/depovg/tcpip2k.asp)

Microsoft Technet, “Security Considerations for Network Attacks”, (http://www.microsoft.com/technet/security/website/dosrv.asp)

Microsoft Technet, “Secure Internet Information Services 5 Checklist”, (http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/tips/iis5chk.asp)

Microsoft Knowledge Base Article Q296576 – “Unchecked Buffer in ISAPI Extension Could Compromise Internet Information Services 5.0” (http://support.microsoft.com/support/kb/articles/q296/5/76.asp)

Microsoft Knowledge Base Article Q121007 – “How to Disable the 8.3 Name Creation on NTFS Partitions” (http://support.microsoft.com/support/kb/articles/q121/0/07.asp)

Microsoft Knowledge Base Article Q288164 – “How to Prevent the Creation of Administrative Shares on Windows NT Server 4.0 (http://support.microsoft.com/support/kb/articles/q288/1/64.asp)

The SANS Institute, Security Essentials, “IIS Security”

ZDNet: Developer, “Using Security Templates to Batten Down the Hatches”, (http://www.zdnet.com/devhead/stories/articles/0,4413,2598645,00.html)