GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

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

Security Procedures for a new IIS Server

BY:
Michael Wherley
GIAC Security Essentials Certification (GSEC) Pratical Assignment Version 1.4b

INTRODUCTION

Any system administrator that has attempted to set up Microsoft Internet Information Server (IIS) knows about the painstaking process of securing the server. It seems that everybody has a checklist that is supposed to make the administrator's job easier. These checklists then redirect the administrator to multiple other white papers / websites to complete a particular task. There are many vendors who are more than willing to sell you a software product that supposedly will do all this for the administrator, but these usually cost a lot of money. This paper is an attempt to present the key modifications to the default Windows 2000 Service Pack 3 IIS server installation in one self-contained document in an economical manner.

There are many sub-systems integral to the successful secure deployment of an IIS server. They are 1) the physical security of the web server, 2) the security attributes of the network to which the server is attached, 3) the underlying operating system, 4) the IIS application, 5) remote administration, and 6) the ongoing everyday maintenance of the whole system. In addition to securing IIS itself, all the supporting infrastructure must also be secure or all your effort will be wasted. For example, if you buy a super strong steel-reinforced door for your house, but the rest of your house is made out of paper, anyone can get into your house with a pocketknife. While this example is a little extreme, it points out that you need to consider the entire system that encompasses your IIS server. We will address each of the above six issues in detail below.

PHYSICAL SECURITY

One of the key, security protocols that you need to follow when configuring a Microsoft Web Server is physical security. If you implement all the actions in this paper and secure your IIS server, people will have a difficult time breaking into your system. But, if you forget to physically secure the server and I can walk up to it, then I can have full access in less then 5 minutes. So please be sure to physically secure your server by:

1. Locating the server behind locked doors
2. Limiting access to the server to only a couple of administrators
3. Not disabling the requirement for using CTRL-ALT-DEL to logon
4. Ensuring that the server has adequate air conditioning (an overheated server will shutdown, and you will have an effective denial of service)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

5. Testing all patches and settings on a test server before implementing on a production server (also potential denial of service against yourself)

NETWORK SECURITY

While this topic has the potential to be hundreds of pages, there are only a few key attributes that are crucial for implementing a secure IIS environment.

- Separate the connection to the Internet with a hardware firewall
- Separate the connection to the rest of your internal network with a hardware firewall
- Utilize 1-to-1 Network Address Translation (not necessary, but helpful)

These three attributes can be accomplished with one hardware firewall with the web server running in the De-Militarized Zone (DMZ) port. The discussion of which firewall to use is outside the scope of the document. At a minimum, the firewall needs to be configured to only allow the minimum set of services through to the DMZ. This may be more than what the web server needs (see discussion later) because there may be other servers on the DMZ than just the web server.

*IMPORTANT NOTE: You must install and configure the operating system and IIS prior to connecting the server to the network or else you may get hacked prior to hardening the server completely.

OPERATING SYSTEM SECURITY

There is a lot of information available on this subject, and it could fill many books (just check out the local library or do an Internet search on Windows 2000 security). Here, I will highlight the main improvements over the default installation, as appropriate for a web server. The following is extracted from various sources (personal experience, John Davis' From Blueprint to Fortress: A Guide to Securing IIS 5.0, David Courington's A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server, Philip Cox's Hardening Windows 2000, the NSA Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set, the NSA Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, the NSA Guide to Securing Microsoft Windows 2000 File and Disk Resources, SANS Securing Windows 2000 Step by Step, and many Microsoft TechNet articles). Please note that since some of these are direct registry edits, you should backup up your registry before editing it. To access the registry, go to Start• Run• regedit.

1. Partition the Hard Drive: Assuming at least a 35 GB hard drive, use a minimum of four hard drive partitions:
    a. C - 5 GB for Operating System
    b. D - 5 GB for swap file

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

c. F - minimum of 10 GB for WWW files
d. L - 15 GB for log files

2. Use NTFS disk partitions.
   a. Check via Computer Manager: Start• Programs• Administrative Tools• Computer Management• Storage• Disk Management
   b. Convert, if needed: Start• Run• cmd.exe, then type sans quotes "convert *file_system_drive_letter* /FS:NTFS [/V]" Then "/V" is only needed if want to run in verbose mode.
   c. Reboot the server
3. Assign the Administrator a strong password (minimum 8 characters, at least one lower case, at least one upper case, at least one number, and at least one special character). From Philip Cox's paper on Hardening Windows 2000, "It is very important to select a strong password for the administrator. This will be the password that is stored in the local SAM database."
4. Keep as a Member Server, do not promote it to a domain controller
5. Run Windows Update (Start• Windows Update) to get all the latest patches. If the server does not have direct access to the Internet, go to http://www.microsoft.com/technet/treeview/?url=/technet/security/current.asp?frame=true to get the latest patches for Windows 2000 and IIS 5, and then install them on the server.
6. Disable the following services (that are installed by default) via the Services applet (Start• Programs• Administrative Tools• Services). To disable, highlight the service and select Action• Properties, and then change Startup Type to "Disabled." Depending on the configuration that the administrator choose during the initial installation, some of these may not be listed.
   a. Alerter
   b. ClipBook
   c. Computer Browser
   d. DHCP Client
   e. Distributed File System
   f. Distributed Link Tracking Client
   g. License Logging Service
   h. Logical Disk Manager Administrator Service
   i. Messenger
   j. NetBIOS Interface
   k. Netlogon (unless users will be authenticating to a domain)
   l. Network DDE
   m. Network DDE DSDM
   n. Network Monitor Agent
   o. NNTP (unless you will be hosting a Network News service)
   p. NWLink NetBIOS
   q. Print Spooler
   r. Remote Registry Service
   s. Removable Storage

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

t. RunAs Service
u. Server (this prevents file and print sharing; DO NOT disable it if you plan on using NNTP or SMTP)
v. Simple TCP/IP Services
w. SNMP
x. Spooler
y. TCP/IP NetBIOS Helper
z. Telephony
aa. Windows Installer
bb. Windows Time
cc. Workstation (Only need if part of a domain)

7. Implement Microsoft's High Security Web Template (Hisecweb.inf) for a secure IIS server
    a. Download "Hisecweb.exe" from Microsoft (http://support.microsoft.com/default.aspx?scid=kb;en-us;316347) and expand to your C:\WINNT\security\templates folder
    b. Modify the Hisecweb.inf using the Security Configuration Manager (Start• Run• MMC [enter]• Console• Add/Remove Snap-in• Add• highlight "Security Templates" and click the Add button• click the Close button• click the OK button):
        i. Open Hisecweb template (Console Root• Security Templates• C:\WINNT\Security\Templates• Hisecweb)
        ii. Edit Event Log (Event Log• Settings for Event Log)
            1. Maximum application log size• 4194240
            2. Maximum security log size• 4194240
            3. Maximum system log size• 4194240
            4. Retain application log• 7
            5. Retain security log• 7
            6. Retain system log• 7
            7. Retention method for application log• Do not overwrite events (clear log manually)
            8. Retention method for security log• Do not overwrite events (clear log manually)
            9. Retention method for system log• Do not overwrite events (clear log manually)
            10. Enable "Shut down the computer when the security audit log is full"
        iii. Right-click on hisecweb• select Save As• create new filename (e.g., *my-hisecweb*)
    c. Apply your new template.
        i. From the MMC console• Add/Remove Snap-in• Add• highlight "Security Configuration and Analysis" and click the Add button• click the Close button• click the OK button
        ii. Right-click on Security Configuration and Analysis• Open Database• type *my-hisecweb*• OK• select *my-hisecweb.inf*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

iii. Right-click on Security Configuration and Analysis• Analyze Computer Now • OK
iv. Review the analysis
v. If you agree with the results, right-click on Security Configuration and Analysis• Configure Computer Now • OK
vi. Or, from a command prompt in the C:\WINNT\security\templates directory, enter the following command: secedit /configure /cfg "Hisecweb.inf" /db newdb.sdb /log logfile.txt /overwrite

d. Reboot the server

8. Change some of the Local Policy settings (Start• Programs• Administrative Tools• Local Security Policy):
   a. Restrict Anonymous listing of shares (Local Policies• Security Options• Additional restrictions for anonymous connections set to No access without explicit anonymous permissions)
   b. Restrict CDROM access to locally logged on user only (Local Policies• Security Options• Ensure that the policy "Restrict CD-ROM access to the locally logged on user only" is enabled)
   c. Restrict Floppy access to locally logged on user only (Local Policies• Security Options• Ensure that the policy "Restrict floppy access to the locally logged on user only" is enabled)
   d. Auditing Backup and Restore Actions for suspicious activity (Local Policies• Security Options• Enable the setting "Audit and Restore privilege")
9. Delete Subsystem Executables (in this order)
   a. From the C:\WINNT\System32\dllcache (if you don't see this folder, go to Tools• View Tab• and uncheck "Hide protected operating system files") delete the following files:
      os2.exe
      os2ss.exe
      os2srv.exe
   b. From the C:\WINNT\System32 directory, delete:
      os2.exe
      os2ss.exe
      os2srv.exe
      psxss.exe
      posix.exe
      psxdll.dll
      the entire \os2 directory
10. Delete the following registry keys using Regedit:

Hive	HKEY_LOCAL_MACHINE
Key	System\CurrentControlSet\Control\Session Manager\Environment
Value Name	Os2LibPath

Hive	HKEY_LOCAL_MACHINE
Key	System\CurrentControlSet\ Control\Session Manager\Subsystems
Value Name	Optional

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Hive HKEY_LOCAL_MACHINE
Key System\CurrentControlSet\ Control\Session Manager\Subsystems
Value Name Os2

Hive HKEY_LOCAL_MACHINE
Key System\CurrentControlSet\ Control\Session Manager\Subsystems
Value Name Posix

11. Harden the Registry
    a. Disable Autorun on CDs using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key System\CurrentControlSet\Services\CDRom
       Value Name Autorun
       Type REG_DWORD
       Value 0
    b. Restrict Null User access using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key System\CurrentControlSet\Control\LSA
       Value Name RestrictAnonymous
       Type REG_DWORD
       Value 2
    c. Restrict Null Session Access (this will disable many network utilities, only do this if the web server is truly standalone) using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key \System\CurrentControlSet\Services\LanManServer\Parameters
       Value Name RestrictNullSessAccess
       Type REG_DWORD
       Value 1
    d. Reduce Risk of Denial of Service via a Syn Flood Attack using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key System\CurrentControlSet\Services\Tcpip\Parameters
       Value Name SynAttackProtect
       Type REG_DWORD
       Value 2
    e. Disable IP Source Routing using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key System\CurrentControlSet\Services\Tcpip\Parameters
       Value Name DisableIPSourceRouting
       Type REG_DWORD
       Value 1
    f. Tune the TCP/IP KeepAlive Time using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key System\CurrentControlSet\Services\Tcpip\Parameters
       Value Name KeepAliveTime
       Type REG_DWORD
       Value 300000
    g. Disable ICMP Redirects using Regedit:
       Hive HKEY_LOCAL_MACHINE
       Key System\CurrentControlSet\Services\Tcpip\Parameters
       Value Name EnableICMPRedirect
       Type REG_DWORD
       Value 0

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

h. Disable External Name Release using Regedit:
   Hive HKEY_LOCAL_MACHINE
   Key System\CurrentControlSet\Services\Tcpip\Parameters
   Value Name NoNameReleaseOnDemand
   Type REG_DWORD
   Value 1
i. Remove Administrative Shares (only if not required for backup / administrative purposes) using Regedit:
   Hive HKEY_LOCAL_MACHINE
   Key System\CurrentControlSet\Services\LanManServer\Parameters
   Value Name AutoShareServer
   Type REG_DWORD
   Value 0
j. Disable 8.3 Filename Creation using Regedit:
   Hive HKEY_LOCAL_MACHINE
   Key System\CurrentControlSet\Control\Filesystem
   Value Name NTFSDisable8dot3NameCreation
   Type REG_DWORD
   Value 1
k. Restrict Access to the Registry from a Remote Computer using Regedit:
   Hive HKEY_LOCAL_MACHINE
   Key System\CurrentControlSet\Control\Filesystem
   Value Name NTFSDisable8dot3NameCreation
   Type REG_DWORD
   Value 1
l. Disable WebDAV using Regedit:
   Hive HKEY_LOCAL_MACHINE
   Key System\CurrentControlSet\Services\W3SVC\Parameters
   Value Name DisableWebDAV
   Type REG_DWORD
   Value 1
m. Disable Web Printing using Regedit:
   Hive HKEY_LOCAL_MACHINE
   Key System\CurrentControlSet\Services\W3SVC\Parameters
   Value Name DisableWebDAV
   Type REG_DWORD
   Value 1
n. Verify that the following registry key exists and that only the permissions are that the Administrators have Full Control (Start• Run• Regedit32.exe, then after selecting the following key, click on Security• Permissions):
   Hive HKEY_LOCAL_MACHINE
   Key \CurrentControlSet\Control\SecurePipeServers
   Value Name \winreg

12. Protect the SAM database with Syskey (optional). From Philip Cox's paper on Hardening Windows: "By default, Win2K strongly encrypts the local SAM database. This is the Syskey option in WinNT. The potential problem is that the key used to decrypt the database is stored in an obfuscated form in the registry. This could be a potential problem. To eliminate the problem, you can reconfigure Syskey to require manual password entry or to read it off a floppy. You open the configuration by

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

running the SYSKEY command from the command line, and then using the Update option. The problem with either of these two options is that they require some level of user intervention (unless you leave the floppy in the drive, which has its own security problems). So you will want to reconfigure this only for highly secure systems that will require manual intervention to start up."

13. Delete the SAM file from the C:\WINNT\Repair directory
14. Change the location of the System Page File from C: drive:
    a. Navigate to:Start• Settings• Control Panel• System• Advanced Tab• Performance Options• Change Virtual memory
    b. Set the initial size and maximum size to 0
    c. Select the Set button
    d. Highlight the D: drive and the set the initial size to 3199 and maximum to 4596
15. Disable Windows Scripting Host.
    a. Start Windows Explorer (Start• Programs• Accessories• Windows Explorer)
    b. Select Tools• Folder Options• File Types Tab
    c. Find and delete the "VBS" file extension entry for "VBScript Script File"
16. Disable NetBIOS over TCP/IP: Start• Settings• Control Panel• Network and Dial-up Connections• Local Area Connection• Properties• Select properties for Internet Protocol (TCP/IP)• Advanced• WINS Tab• Click on "Disable NetBIOS over TCP/IP"
17. Enable TCP/IP Filtering (Start• Settings• Control Panel• Network and Dial-up Connections• Local Area Connection• Properties• Select properties for Internet Protocol (TCP/IP)• Advanced• Options Tab• Select properties for TCP/IP filtering)
    a. Check the "Enable TCP/IP Filtering (All Adapters)"
    b. Check "Permit Only" for TCP Ports. Add the following ports: 80 (http), 443 (https). Add other ports, as appropriate (e.g., FTP, SMTP). For a list of commonly used ports, see http://www.iss.net/security_center/advice/Exploits/Ports/default.htm.
    c. Check "Permit Only" for UDP Ports. Do not add any ports.
    d. Check "Permit All" for IP Protocols
18. Create three User Groups (Start• Administrative Tools• Computer Management• Local Users and Groups• Groups) by selecting Action• New Group
    a. WebUsers (Add the IUSR_*computername* and remove this user from the Guests group)
    b. WebAdmins (users in here are the administrators of the web site)
    c. AdminTools (for special access to OS tools)
19. Ensure that only the AdminTools group has read / execute permissions (right-click on tool• Properties• Security Tab• Add) and delete everyone else for the following tools.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

C:\WINNT\

- explorer.exe
- regedit.exe

C:\WINNT\System32

- arp.exe
- at.exe
- atsvc.exe
- cacls.exe
- cmd.exe
- command.com
- cscript.exe
- debug.exe
- edit.exe
- edlin.exe
- finger.exe
- ftp.exe
- ipconfig.exe
- krnl386.exe
- nbtstat.exe
- net.exe
- net1.exe
- netsh.exe
- netstat.exe
- nslookup.exe
- ping.exe
- posix.exe
- poledit.exe
- taskman.exe
- qbasic.exe
- rcp.exe
- rdisk.exe
- regedit32.exe
- regini.exe
- regsrv32
- rexec.exe
- route.exe
- rsh.exe
- runas.exe
- runonce.exe
- secfixup.exe
- srvmgr.exe
- sysedit.exe
- syskey.exe
- telnet.exe
- tftp.exe
- tracert.exe
- usrmgr.exe
- wscript.exe
- xcopy.exe

20. Reboot the server

INTERNET INFORMATION SERVER SECURITY

By nature of have a web server, you are allowing anonymous users to read files on your server. The default installation of IIS, however, is unsecure. The following checklist will help you implement this without allowing these same anonymous users from accessing more information then you intended. This information is extracted from various sources (personal experience, Terri Carroll's Basic IIS 5.0 Default Web Server Security, the NSA Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, SANS Securing Windows 2000 Step by Step, and many Microsoft TechNet articles). Lastly, make sure that all of the following settings are made prior to loading any web site onto the server.

1. Install IIS Lockdown Tool and URLScan filter
    a. Download wizard from Microsoft (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp)
    b. Activate the wizard (iislockdown2-1.exe)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

c. Agree to the license information
d. Select either “Static Web server” or “Dynamic Web server (ASP enabled)” depending on whether or not you are allowing ASP. Also, make sure that “View template settings” is checked.
e. Select which services your server will be active (Web / FTP / SMTP / NNTP) and check the box, “Remove unselected services.”
f. Remove the script mappings that are not appropriate for your environment (ASP, Index Server, Server Side Includes, Internet Data Connector, HTR Printing)
g. Check everything on the Additional Security page (unnecessary virtual directories, limiting anonymous IIS user access, and disabling WebDAV)
h. Check “Install URLScan filter on the server”

2. Install only the necessary IIS services. Start• Settings• Control Panel• Add/Remove Programs• Add/Remove Windows Components• Internet Information Services (IIS) and select the Details button. Make sure the following subcomponents are not checked, then click OK• NEXT and finish installing / deleting IIS-specific services:
    a. Documentation
    b. File Transfer Protocol (FTP) Server, unless you want it
    c. FrontPage 2000 Server Extensions
    d. Internet Services Manger (HTML)
    e. NNTP Service, unless you want it
    f. SMTP Service, unless you want it
    g. Visual InterDev RAD Remote Deployment Support
3. Delete the following directories, if they still exist:
    a. C:\Inetpub\iissamples
    b. C:\Inetpub\scripts
    c. C:\Inetpub\wwwroot
    d. C:\WINNT\help\iishelp
    e. C:\WINNT\system32\inetsrv\iisadmpwd
    f. C:\WINNT\web\printers
    g. If you will not be running the NNTP Service, also delete:
        i. C:\Inetpub\nntpfile
        ii. C:\WINNT\Help\news
    h. If you will not be running the SMTP Service, also delete:
        i. C:\Inetpub\mailroot
        ii. C:\WINNT\Help\mail
4. Edit the IIS Master Properties (Start• Programs• Administrative Tools• Internet Services Manager• Select the server (should be the top-level entry under Internet Information Services in the left hand pane)• Action• Properties• Edit WWW Service:
    a. Web Site Tab
        i. Specify a Connection Timeout of 600 seconds to help prevent Denial of Service attacks
        ii. Ensure that “HTTP Keep-Alives Enabled” is checked

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

iii. Ensure that “Enable Logging” is checked
iv. Chose “W3C Extended Log File Format” and click on Properties
    1. Under General Properties Tab• Log file directory, change the directory to the L: drive
    2. Under Extended Properties Tab, make sure that the following are checked:
        a. Date
        b. Time
        c. Client IP Address
        d. User Name
        e. Server IP Address
        f. Server Port
        g. Method
        h. URI Stem
        i. URI Query
        j. Protocol Status
        k. Win32 Status
        l. User Agent
        m. Cookie
        n. Referrer

b. Make sure that “Log Visits” is checked on the Home Directory tab.
c. Home Directory Tab• Configuration button,
    i. Under App Mappings Tab, Remove the following Application Mappings (if you use the capabilities in the parentheses, then do not delete the application mapping):
        1. .bat
        2. .cdx (Channel Definition Files)
        3. .cer (used to support certificates)
        4. .htr
        5. .htw (Index Server)
        6. .ida
        7. .idc
        8. .idq (Index Server)
        9. .printer
        10. .shtm (Server Side Includes)
        11. .shtml (Server Side Includes)
        12. .stm (Server Side Includes)
    ii. Under App Options Tab, ensure that the “Enable parent paths” entry is not checked
    iii. Under App Debugging Tab• Script Error Messages, make sure that “Send text error message to client” is checked

5. Edit the IIS High level Server Extensions Properties (Start• Programs• Administrative Tools• Internet Services Manager• Select the server (should be the top-level entry under Internet

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Information Services in the left hand pane)• Action• Properties• Server Extensions Tab): Check the following permissions:

a. Log Authoring actions
b. Manage permissions manually
c. Require SSL for authoring
d. DO NOT check “Allow authors to upload executables”

6. Secure the log files: set the NTFS permissions on the L: drive to Full Control for Administrators and System only.
7. Delete the Default Web Site Directory (Start• Programs• Administrative Tools• Internet Services Manager• *ServerName*• Select Default Web Site• Action• Delete)
8. Do not install any development tools or application software on the server
9. Define File Structure. To change NTFS Permissions within windows explorer, right-click on folder• Properties• Security tab. To change IIS Permissions from Internet Services Manager, right-click on folder• Properties• Application Settings• Execute Permissions
    a. Create a directory on your F: drive that will be the root of web site (e.g., F:\MyWebSite\)
        i. NTFS Permissions
            1. Administrators – Full Control
            2. System – Full Control
            3. WebAdmins – Read / Write / Execute / Modify
            4. WebUsers – Read
        ii. IIS Execute Permissions - None
    b. Create a scripts (*.asp files) directory (e.g., F:\MyWebSite\scripts)
        i. NTFS Permissions
            1. Administrators – Full Control
            2. System – Full Control
            3. WebAdmins – Read / Write / Execute / Modify
            4. WebUsers – Special Access – Execute only
        ii. IIS Execute Permissions – Scripts Only
    c. Create an executable directory (e.g., F:\MyWebSite\cgi-bin)
        i. NTFS Permissions
            1. Administrators – Full Control
            2. System – Full Control
            3. WebAdmins – Read / Write / Execute / Modify
            4. WebUsers – Special Access – Execute only
        ii. IIS Execute Permissions – Scripts and Executables
    d. Create a directory for hosting local database files. They need to be outside of your webroot (e.g., F:\Databases\MyWebSite\)
        i. NTFS Permissions
            1. Administrators – Full Control
            2. System – Full Control
            3. WebAdmins – Read / Write / Execute / Modify
            4. WebUsers – Read / Write
        ii. IIS Execute Permissions – None

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

10. Modify IIS to return Fully Qualified Domain Name in banner instead of IP address using a command prompt from the C:\Inetpub\AdminScripts directory:
    a. Type (sans quotes) "adsutil set w3svc/UseHostName True" [enter]
    b. Restart IIS service (Start• Programs• Adminstrative Tools• Internet Services Manager• highlight *server_name*• Action• Restart IIS)

REMOTE ADMINISTRATION SECURITY

There are many choices for remote administration; full discussion is out of scope for this paper. For remote administration of Windows 2000 servers, I use Terminal Services. I will explain how to install and secure Terminal Services for remote administration. Most of this information is extracted from NSA's Guide to Securing Microsoft Windows 2000 Terminal Services.

To install Terminal Services:

1. Start• Settings• Control Panel• Add/Remove Programs• Add/Remove Windows Components• Check Terminal Services• Next
2. Select "Remote Administration Mode"• Next
3. Select "Permissions Compatible with Windows 2000 Users"• Next

To Configure Terminal Services Properties:

1. Start• Programs• Administrative Tools• Terminal Services Configuration• Connections• Select RDP-Tcp• Action• Properties
2. Under the General Tab
    a. Set the Encryption level to "High"
    b. Ensure that "Use standard Windows authentication" is NOT selected
3. Logon Settings Tab
    a. Use client-provided logon information• Selected
    b. Allows use the following logon information• NOT selected
    c. Always prompt for password• Selected
4. Sessions Tab
    a. Override user settings for session limits• Selected
        i. End a disconnected session• 1 day
        ii. Active session limit• Never
        iii. Idle session limit• 15 minutes
    b. Override user settings• Selected
        i. When session limit is reached or connection is broken• Disconnect from session
5. Environment Tab
    a. Ensure that "Override settings from user profile and Client Connection Manager wizard" is NOT selected
    b. Disable wallpaper• Selected
6. Remote Control Tab

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

    a. Do not allow remote control• Selected
7. Client Settings Tab
    a. Use connection settings from user settings• NOT selected
    b. Connect client printers at logon• NOT selected
    c. Default to main client printer• Selected
    d. Disable the following:
        i. Windows printer mapping• Selected
        ii. LPT port mapping• Selected
        iii. COM port mapping• Selected
        iv. Clipboard mapping• Selected
8. Permissions Tab• Leave it so only the Administrators and SYSTEM have Full Control
9. Click OK to Accept the changes and close the properties page

To Configure Terminal Services Server Settings:

1. Start• Programs• Administrative Tools• Terminal Services Configuration• Server Settings
2. Terminal server mode• Remote Administration
3. Delete temporary folders on exit• Yes
4. Use temporary folders per session• Yes
5. Internet Connector licensing• Disable
6. Active Desktop• Disable
7. Permission Compatibility• Windows 2000 Users

EVERYDAY SECURITY

Now that you have a significantly hardened IIS server, it is almost time to load your web site. You must first install both an anti-virus program and a host-based intrusion detection system. And, you must constantly update the signatures for each of these applications.

Another area that you, as the system administrator, need to pay attention to is patch management and security bulletins. The following online resources will enable you to receive notification and research current vulnerabilities:

1. Microsoft TechNet Security Web Site - Security Bulletins and Resources (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/default.asp)
2. Security Bulletin Mailing list – For Microsoft products (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/notify.asp)
3. Security Bulleting Search Site (http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/current.asp)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

CONCLUSION

Now that you have secured the IIS application, the Windows 2000 operating system on which the IIS application runs, the network on which Windows 2000 operates, the room in which the computer is located, the method of remote administration, and set in place the procedure for continued monitoring and security of the whole system, it is now time to load the web site. Good luck and have fun!!

REFERENCES

Carroll, Terri, Basic IIS 5.0 Default Web Server Security, SANS InfoSec Reading Room, April 11, 2001, URL: http://www.sans.org/rr/web/IIS5_sec.php (5 March 2003)

Courington, David S. "A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server." SANS InfoSec Reading Room, March 29, 2001, URL: http://www.sans.org/rr/win2000/win2000_sec.php (5 March 2003)

Cox, Philip, "Hardening Windows 2000, version 1.0." System Experts, March 30, 2001, URL: http://systemexperts.com/tutors/HardenW2K101.pdf (5 March 2003)

Davis, John, "From Blueprint to Fortress: A Guide to Securing IIS 5.0" Microsoft TechNet, June 2001, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/deploy/depovg/securiis.asp (5 March 2003)

DiMaria, Vincent J., James F. Barnes, CDR Jerry L. Birdsong, and Kathryn A. Merenyi, "Guide to Securing Microsoft Windows 2000 Terminal Services, version 1.0." NSA, July 2, 2001, URL: http://www.nsa.gov/snac/win2k/guides/w2k-19.pdf (5 March 2003)

Haney, J., Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set, version 1.2, NSA, December 3, 2002, URL: http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf (3 April 2003)

"How to Disable WebDAV for IIS 5.0" Microsoft Knowledge Base. March 24, 2003, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q241520 (4 April 2003)

"How to disable Windows Scripting Host," URL: http://www.sophos.com/support/faqs/wsh.html#2000Me (3 April 2003)

"How to Restrict Access to the Registry from a Remote Computer." Microsoft Knowledge Base. October 10, 2002, URL:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

http://support.microsoft.com/default.aspx?scid=kb;EN-US;153183 (5 March 2003)

"How to Use the RestrictAnonymous Registry Value in Windows 2000." Microsoft Knowledge Base. October 10, 2002, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q246261&sd=tech (4 April 2003)

Howard, Michael, "Secure Internet Information Services 5 Checklist." Microsoft TechNet, June 29, 2000, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/iis5chk.asp (5 March 2003)

"IIS 5: HiSecWeb Potential Risks and the IIS Lockdown Tool." Microsoft Knowledge Base. January 15, 2002, URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;316347 (5 March 2003)

"IIS Lockdown Tool." Microsoft TechNet, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/locktool.asp (5 March 2003)

"Internet Information Server Returns IP Address in HTTP Header (Content-Location)." Microsoft Knowledge Base. June 11, 2002, URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;218180 (5 March 2003)

"Microsoft Security Tool Kit: Guides, Updates, and Tools" Microsoft TechNet. 2003, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/stkintro.asp (4 April 2003)

Owen R. McGovern and Julie M. Haney, Guide to Securing Microsoft Windows 2000 File and Disk Resources, version 1.0, NSA, April 19, 2001, URL: http://www.nsa.gov/snac/win2k/guides/w2k-8.pdf (5 March 2003)

"Port Knowledgebase" Internet Security Systems, http://www.iss.net/security_center/advice/Exploits/Ports/default.htm (4 April 2003)

SANS Institute, Securing Windows 2000 Step By Step, Version 1.5, July 1, 2001

"The Twenty Most Critical Internet Security Vulnerabilities (Updated) ~ The Experts' Consensus." Version 3.22. March 3, 2003. URL: http://www.sans.org/top20/ (5 March 2003)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

"Urlscan Security Tool" Microsoft TechNet, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/urlscan.asp (5 March 2003)

Walker, William E., Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0, version 1.3.1. NSA, March 4, 2002, URL: http://www.nsa.gov/snac/win2k/guides/w2k-14.pdf (5 March 2003)

Wichman, Jeff, "Using Microsoft's IISlockdown Tool to Protect Your IIS Web Server" SANS InfoSec Reading Room, January 4, 2002, URL: http://www.sans.org/rr/web/IISlockdown.php (5 March 2003)

"Windows 2000 Server Baseline Security Checklist." Microsoft Knowledge Base. 2001, URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/chklist/w2ksvrcl.asp (5 March 2003)

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.