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 permitted without express written permission.

Interested in learning more?
Check out the list of upcoming events offering "Securing Windows and PowerShell Automation (Security 505)" at http://www.giac.org/registration/gcwn
Securing Windows 2000 for Web Server Deployment

A step-by-step guide

Jay Robinson

April 2001

Written to complete
Table of Contents

Introduction

Section 1 - Physical Security

Section 2 - Network Security

Section 3 – Operating System Security

Section 4 – Securing Services

Section 5 – Account Security

Section 6 – Directory and File Security

Section 7 – Auditing and Security Options

Section 8 – TCP/IP Security

References
Introduction

This document is intended to be a basic, step-by-step guide to building a Windows 2000 web server for Internet use. It is presented in a format that is easy to follow, for administrators that may have limited experience with Windows 2000 security.

The guide can also be used for busy security experts who wish to have less experienced team members build their servers. Once the basic web server is configured the system can later be fine-tuned for higher levels of security.

Please be aware that due to the focus of this document some advanced topics have been omitted. Administrators that are interested in more advanced security topics should refer to the additional resources listed at the end of this document.

Section 1 - Physical Security

Physical access to a Windows 2000 server can compromise the system is several ways:

- Direct Data Access: Using a boot disk with NTFS support is it possible to access files directly on the server. Someone could either access confidential files directly, or take a copy of the SAM database for later use.
- Indirect Data Access: By simply removing the tape from a local backup device it is possible to obtain a copy of all data on the server.
- Physical Removal: The server itself could be removed.
- Physical Destruction: Damage sufficient to permanently disable the server could be inflicted.

In order to minimize the risk of physical compromise it is important to keep access to your server as restricted as possible. A data center with locked doors is preferable. Monitoring equipment can also be installed to audit physical access to your server.

Section 2 - Network Security

Where a server is placed on a network can be as important as where it is placed physically.
DMZ – The term DMZ is derived from the military term: demilitarized zone. It represents an area of a network that is the common ground between internal resources and the Internet. In a DMZ configuration web servers are placed on a separate network that is given restricted accessibility from the Internet. Hosts from the internal network are then allowed to use additional services as necessary. The example below is one way of setting up a DMZ network.

– Operating System Security

For the highest level of security a new Windows 2000 web server installation should be performed OFF the network. Unfortunately, this is not always possible. This document assumes that the server will be configured on a network that has been appropriately secured. Once secured, the system can be moved to a DMZ for production.

Installation

A Windows 2000 web server should be installed with at least two partitions: One for the operating system and one for the web server files. Both of these drives should be formatted with the NTFS file system. If the server is not already setup with the NTFS file system open a Command Prompt and issue the following command to convert each drive:
convert [drive:] /fs:ntfs

For example:

```
C:>convert /? 
Converts FAT volumes to NTFS.
CONVERT volume /FS:NTFS [/U]
  volume  Specifies the drive letter (followed by a colon),
  mount point, or volume name.
  /FS:NTFS  Specified that the volume to be converted to NTFS.
  /U  Specifies that Convert should be run in verbose mode.
C:>convert c: /fs:ntfs
```

**High Encryption Pack**

After the initial server installation the High Encryption Pack should be applied: http://www.microsoft.com/windows2000/downloads/recommended/encryption/default.asp

Note the following from Microsoft:

“The Windows 2000 High Encryption Pack is eligible for export from the U.S. to all customers worldwide, except to US embargoed destinations. Please see http://www.microsoft.com/exporting/ for details. Other countries may exercise separate jurisdiction over the import, export or use of encryption products. Users who download this product should observe any local regulations that may apply to the distribution or use of encryption products.”

Select the **Standard Download** when prompted:

**Windows 2000 High Encryption Pack - U.S. English**

**Important**

- You can install the Windows 2000 High Encryption Pack on any copy of Microsoft Windows 2000 you have licensed, but you must accept the license agreement presented to you upon installation of the Windows 2000 High Encryption Pack before you can use it. If you do not accept the terms of the license agreement, you are not authorized to use the component and should promptly remove it from your computer.
- Once you have installed the Windows 2000 High Encryption Pack, you must restart your computer before installing any additional software.

```
Standard Download

192 KB | 1 min. 40 sec. @ 28.8
Available for users wishing to install the Windows 2000 High Encryption Pack on their computer.
```

Then select *Run this program from its current location* and click *OK* to begin the installation.
Once the High Encryption Pack is installed you will need to reboot your server.

**Latest Service Pack**

After the High Encryption Pack the latest services pack should be installed. As of the writing of this document the latest services pack for Windows 2000 was SP1: http://www.microsoft.com/windows2000/downloads/recommended/SP1

Select the **Express Installation** when prompted:

**Windows 2000 Service Pack 1**

U.S. English

[Express Installation]

Windows 2000 Professional | 13.8 MB typical | 66 minutes @ 28.8 | 2 minutes @ T1
Windows 2000 Server and Advanced Server | 29.6 MB typical | 2.4 hours @ 28.8 | 3 minutes @ T1

The Express installation detects your system components and installs only those updates that are necessary for your computer. For example, files for Windows 2000 Professional will not be installed if your computer is running Windows 2000 Server. This method is recommended for customers who want to reduce their download time:

- Fastest way to install SP1.
- For single computer installation only.
- Some anti-virus software programs may interfere with the installation. Please disable anti-virus software while installing SP1.

Then select **Run this program from its current location** and click **OK** to begin the installation.
Hotfixes


After you download and run the program you will be prompted for where to extract the files. Enter c:\tools\ and click OK:

You will be prompted to create the directory. Click Yes.

In order to run the Hotfix Checking Tool for IIS 5.0 you will need to change your default script host to CScript from the default (WScript). To do this open a Command Prompt and enter the following:

cscript //h:cscript
You can now run hfcheck to generate the list of hotfixes that need to be applied:

Instead of using this list, enter the Application Log in the Event Viewer.

The log entries will show each needed hotfix as well as a convenient link the associated Microsoft web page.
Finally, hfcheck should be set to run at least once a week. To schedule it to run every Friday at 3:00am, open a command prompt and issue the following command:

```
at 3am /interactive /every:friday c:\tools\hfcheck.wsf
```

### Section 4 – Securing Services

All services should be disabled that are not required for the operation of the web server. Below is a list of all services that are automatically started after a default installation of Windows 2000 server and IIS. Click on the *Startup Type* tab to sort by that column.
The following services are not required and should be removed:

- Alerter
- Computer Browser
- DHCP Client
- Distributed File System
- Distributed Link Tracking Client
- Distributed Transaction Coordinator
- License Logging Service
- Messenger
- Server
- Print Spooler
- Remote Registry
- Removable Storage
- Simple Mail Transport Protocol (SMTP)
- TCP-IP NetBIOS Helper Service
Right click on each service and select **Properties**. Next click **Startup type** and change it to **Manual**.

After all the unnecessary services have been changed the services window should look like this:
Section 5 – Account Security

To edit the default account policies first load the Local Security Policy editor:
Once the Local Security Policy editor is open, select Account Policies and then Password Policy. The values should be changed as follows:

- **Enforce password history** to 24
- **Minimum password age** to 1
- **Minimum password length** to 8
- **Passwords must meet complexity requirements** to Enabled
Note that these settings are only guidelines. Your security policy should dictate the actual values are used here.

Next, select Account Lockout Policy and change:

- *Account lockout threshold* to 5

### Section 6 – Directory and File Security

It is important to properly secure directories and files on a web server to prevent malicious users from damaging the system. There is minimal file security on Windows 2000 web server files by default so these settings need to be changed.

Depending on the configuration of your web server you may have various types of files in different locations. Wherever these files may be located, it’s important to secure them properly. For administrative purposes it is easiest to create directories for each type of file. For example the web server directory structure might look like this:

```
D:\inetpub\wwwroot\mainwebserver\CGI
```
Once the directory structure is in place the NTFS permissions should be modified. Right click on each directory, select Properties and then click the Security Tab. Uncheck the Allow inheritable permissions from parent to propagate to this object box at the bottom of the window. The following window should appear:

Click Copy to keep the current rights. Now select the CREATOR OWNER name and click Remove. The window should now look like this:

Modify the settings using the following table as a guideline:
### CGI (.exe, .dll, .cmd, .pl)
- Everyone (X)
- Administrators (Full Control)
- System (Full Control)

### Script files (.asp)
- Everyone (X)
- Administrators (Full Control)
- System (Full Control)

### Include files (.inc, .shtm, .shtml)
- Everyone (X)
- Administrators (Full Control)
- System (Full Control)

### Static content (.txt, .gif, .jpg, .html)
- Everyone (R)
- Administrators (Full Control)
- System (Full Control)

Repeat the previous step for each directory that was created.

Finally, the following directories should be deleted unless they are specifically required:

- `%systemroot%\help\iishelp`
- `c:\program files\common files\system\msadc`
- `\Inetpub\Admcreens`

## Section 7 – Auditing and Security Options

The auditing policies on a new Windows 2000 web server should be changed to allow tracking of additional events. These changes will generate important security information in the Event Viewer for later review. Without these auditing changes it may be very difficult to track any future security incidents.

From the Local Security Policy editor select the **Audit Policy** and then make the following changes:

- *Audit account logon events to Success + Failure*
- Audit logon events to **Success + Failure**
- Audit object access to **Failure**
- Audit policy change to **Success + Failure**
- Audit privilege use to **Success + Failure**
- Audit system events to **Success + Failure**

Next the security options should be modified. The following changes will enable improved security options for a Windows 2000 web server:

- **Additional restrictions for anonymous connections** should be changed to **No access without explicit anonymous permissions**
- Audit use of Backup and Restore privilege to **Enabled**
- Digitally sign server communications (when possible) to **Enabled**
- Do not display last user name in logon screen to **Enabled**
- **LAN Manager Authentication Level** to Send LM & NTLM – use NTLM v2 session security if negotiated
- Message test for users attempting to log on to **This computer system is for authorized use only and may be monitored for inappropriate use.**
- Message title for users attempting to log on to **Warning!**
- Restrict CD-ROM access to locally logged-on user only to **Enabled**
- Restrict floppy access to locally logged-on user only to **Enabled**

**Section 8 - TCP/IP Security**

Due to the recent threat of SYN floods it is important to defend a Windows 2000 web server from these attacks as best as possible. To enable TCP settings that will help protect
the server a change in the registry will be necessary.

Open the Registry Editor by clicking Start then Run and then entering regedit

Next select the HKEY_LOCAL_MACHINE hive and navigate the following path: SYSTEM -> CurrentControlSet -> Services -> Tcpip -> Parameters.

Now open the synattackprotect key and change the value to 2.

It is also important to restrict what network ports are open on the system. Even though this server may be protected on a DMZ (see Section 2) it is possible that a nearby server could be compromised and then used as a point of attack against this one.

To restrict open ports TCP/IP filtering needs to be enabled:

Click Start -> Settings -> Network and Dial-up Connections
Next, right click Local Area Connection and select Properties

The Local Area Connection Properties window will appear:
Select **Internet Protocol (TCP/IP)** and click **Properties**. Click **Advanced** and the Advanced TCP/IP Settings window will appear.
Click the Options tab, select TCP/IP filtering and then click Properties.

Select Permit Only above the TCP Ports box. Next click Add and enter 80 to enable HTTP access to and from the server. If the web server will be using SSL then port 443 should be added as well. Additional ports may be required depending on how the server will be administered. If a remote control application is to be used, the appropriate ports...
should be added. Here are some common remote control applications and their associated port numbers:

- PCAnywhere 5631
- VNC 5900
- ControlIT 799
- Terminal Server 3389

Note: These applications should only be installed after the appropriate ports have been blocked from the Internet by a firewall or router.

Here is an example of what a DMZ network configured with web servers running PCAnywhere might look like:

Web server administrators that are interested in advanced security topics may want to review the following additional resources from Microsoft’s web site:


“Step-by-Step Guide to Internet Protocol Security (IPSec)”

“Step-by-Step Guide to Setting up a Certification Authority”


Administrators should also consider subscribing to at least one of the following list services to stay current with the latest security information:

www.microsoft.com/technet/security/notify.asp
www.sans.org/newlook/digests/ntdigest.htm
www.ntbugtraq.com
www.securityfocus.com
References


2. Microsoft Technet, “Secure Internet Information Services 5 Checklist”
   http://www.microsoft.com/technet/security/iis5chk.asp

3. HFCheck documentation file included in the Microsoft “Hotfix Checking Tool for IIS 5.0”
   http://download.microsoft.com/download/win2000platform/Patch/IIS5_HFC_1.0/NT
   5/EN-US/HFCINST.EXE


5. “Well known port numbers” http://www.isi.edu/in-notes/iana/assignments/port-numbers

# Upcoming Training

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Dates</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Security West 2020</td>
<td>San Diego, CA</td>
<td>May 11, 2020 - May 16, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANSFIRE 2020</td>
<td>, DC</td>
<td>Jun 13, 2020 - Jun 20, 2020</td>
<td>CyberCon</td>
</tr>
<tr>
<td>SANS Network Security 2020</td>
<td>Las Vegas, NV</td>
<td>Sep 20, 2020 - Sep 27, 2020</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Online</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
<tr>
<td>SANS SelfStudy</td>
<td>Books &amp; MP3s Only</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>