Global Information Assurance Certification Paper

Case Study: Securing Windows 2000 Server in an NT 4.0 Domain

GSEC Version 1.4b Option 2

Prepared by: Rick Kincer

Abstract

In an industry where companies are racing to provide Internet access to their information, security sometimes takes a backseat to expediency. Within this paper I will review server security lockdown procedures that were performed on a pre-production server to both configure the server to conform to the corporate policy and mitigate threats both inside and outside our firewalls. Within an NT domain we will examine securing a Windows 2000 Server by:

1) Collecting the security requirements for the server.
2) Verifying the server's level of security prior to any work being done.
3) Locking down any possible vulnerabilities through:
    a. Security patches
    b. Security templates
    c. Security checklists
    d. IDS (Intrusion Detection System)
4) Performing a final check for any vulnerability by running:
    a. Vulnerability testing tool
    b. Security scoring tool
    c. Completing a lockdown completion checklist

Keeping in mind that with each step taken to secure the server "Defense in Depth" should be increased; meaning that it is important to add as many levels of security as possible and still allow the server to serve its function. As an onion has multiple layers so should the server have multiple layers of security, so that the intruder will have to "peel off" each layer in an attempt to reach the center, which in this case would be the valuable information on the server or the use of the server for other malicious purposes. With these procedures completed and the corporate policy satisfied the servers have proven to adequately mitigate the threat of intrusion.

1.0 Before Snapshot

Defining the problem

With today's fast paced, "fast food" society, corporations are driven to place their sensitive, confidential and sometimes classified information outside of the confines of the physical location (under lock and key) and into a virtual keyless world in cyberspace; in order to provide access to this data for customers, remote offices and field employees which is required to conduct business outside of their building, city or state. With all new technologies come those who wish to exploit them. Black-hat hackers and script kiddies digging around for an open door to come in and play, bringing with them "weapons of mass disruption" which could cost the companies invaded millions. To mitigate these threats, the need for security policies and procedures for securing servers and the information transferred between them is paramount.

We must focus our efforts to achieve the completion of the following three items that sum up the purpose of system security:

- Maintain the highest level of Availability of the information to be accessed.
- Preserve the Integrity of that information such that no content is altered from its original form.
- Insure Confidentiality so that access to the information is strictly limited to those permitted.

Working in a company that does business in areas that deal with personal health information and financial services, the new HIPPA (The Health Insurance Portability and Accountability Act of 1996) (http://www.cms.gov/hipaa/hipaa2/default.asp or http://www.hipaadvisory.com/) and GLB (Gramm-Leach-Bliley Act of 1999) (http://www.senate.gov/~banking/conf/confrpt.htm) laws create a whole new level of significance for the tasks mentioned above.

Project teams within our Information Technologies (IT) department have been developing applications to deliver company/customer information outside our firewalls through the Internet. Implementing these solutions and installing them on un-secured servers makes our company information highly vulnerable to unauthorized intruders. It is therefore a priority to mitigate intrusions prior to the servers being placed into production. Mitigating a threat of intrusion requires the locking down of the operating system (OS) and applications installed on the servers, this process is also known as "hardening."

Defining the Vulnerability

During the planning of hardening a server a balance must be struck between the security of the server and the functionality. The only totally secure computer is one that is unplugged from the network or powered off.

Windows 2000 Server "out of the box" is not secure and will not hold up against the many methods used to compromise the operating system. Since the release of Win2K there has been the release of service packs, hot fixes, security patches and other updates to counter the vulnerabilities found in the base operating system. If you have ever subscribed to any of the security e-mail notification lists you know that there are many notifications sent out, some rating the vulnerability as, Moderate, High and Critical and giving details of what should be done to mitigate the risk the vulnerability creates. Placing a server in a segment of the firewall that is accessible from the Internet is asking for trouble. With the large number of active scans (intruders running scripts or applications that send out queries to see if they receive a desired response) going across the Internet searching for a vulnerable server, it would not be too long before the server was compromised and used for any number of things; possibly reading company or customer information. Even if the server does not house the actual information, which in our configuration they don't, it can still be used as a gateway to break into our other servers looking for the actual data. The server could also be used as a launch point to attack servers on the Internet, if SMTP (Simple Mail Transport Protocol) is installed it would more likely be used to send unsolicited e-mails (SPAM).

With the base install of Windows 2000 an intruder could "set up shop" on the server and could go undetected, they could do small "behind the scenes" or "stealth" scans that could go completely unnoticed until it was too late. With this knowledge, our company has decided that it is imperative that we be proactive in the prevention of these and other types of threats.

Quoting from a SANS conference, "Vulnerabilities are the gateways by which threats are made manifest."

Defining the Risk

As with so many other companies the risk of exposing sensitive company and customer information is too high not to take the time and effort to avoid a system compromise. After accessing the threat, there was a point where we had to realize that there is always going to be an amount of risk that has to be accepted. It is very difficult, more like impossible, to configure a server to be impenetrable and still be functional. Our ISO (Information Security Office) has completed the threat assessment, defined the risk, documented them both and planned accordingly.

So looking at the big picture; we took the risk of losing data, customer confidence, company reputation, revenue and since, as I mentioned earlier, our company is held to the HIPPA and GLBA standards, we now must include the chance of legal proceedings, fines and even jail time for not meeting the standards, and weighed them against the cost of implementing controls. The choice of action at this point was clear, especially since the majority of the resources used to perform the lockdown was my time and the cost of an IDS agent and an Anti-virus client.

Server Build/OS Install

Prior to the server build I worked with the Network Services' Server group, which handles all server hardware configuration and operating system installations, steps have been added to the OS installation to assist in the lockdown process prior to the server being released to me for the complete lockdown.

The additional steps include:

1) The server is located in a secure location to prevent unauthorized physical access.
2) An anti-virus client was installed and configured to be managed from a central console.
3) The hard drives are formatted using NTFS.
4) The administrator account password, that was entered during the install of the OS, contains at least three out of the following four items:
   a. Longer than seven characters.
   b. Password should contain three out of the following four choices:
      - Uppercase characters.
      - Lowercase characters.
      - Numbers.
      - Non-alpha numeric characters.
   c. The password does not contain usernames or common words.

Characteristics of a Strong Password

A weak password:

Is no password at all.

Contains your user name, real name, or company name.

Contains a complete dictionary word. For example, *Password* is a weak password.

A strong password:

Is at least seven characters long.

Does not contain your user name, real name, or company name.

Does not contain a complete dictionary word.

Is significantly different from previous passwords. Passwords that increment (*Password1*, *Password2*, *Password3*...) are not strong.

Contains characters from each of the following four groups:

Group

Examples

Uppercase letters

A, B, C ...

Lowercase letters

a, b, c ...

Numerals

0, 1, 2, 3, 4, 5, 6, 7, 8, 9

Symbols found on the keyboard (all keyboard characters not defined as letters or numerals)

` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /

An example of a strong password is *J*p2leO4>F*.

REF: Strong Passwords:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/windows_password_tips.asp

5) The default user account is disabled and given a secure password meeting the above listed password criteria.

6) An emergency repair disk has been created and placed in a secure location.
    - Note: An ERD should be created once the lockdown has been completed to reflect the changes.
7) The screen saver settings are set so the "password protected" checkbox is selected and a ten-minute timeout has been set.
8) The server should start out as secure, so in the network configuration properties the "File and Print Sharing for Microsoft Networks" is deselected and "NetBIOS over TCP/IP" is disabled from within the Device Manager. This will prevent network enumeration, which is "mapping" or detailing of the network to find additional resources, by an intruder.
9) The project team, requesting the server, submits an Access Request Form (ARF) for any special rights they may require to install, configure and manage the application they are working with to the Network Administration team which manages corporate user accounts, server access, rights and permissions.

Determining the level of security

Using a Check List to Determine Needs

Once the server was physically secured, the next step was determining the level of security required for the server. This was done by the use of a checklist. Creating a checklist helps to define the job of the server, its placement within the organization and the level of security required.

Levels of security might change due to location:

a) DMZ (Demilitarized Zone) or a public segment of the firewall that is open to Internet access would require the highest level of security lockdown, while still allowing the server to function.
b) Inside segment or what can be considered a production segment of the firewall where inbound Internet access is not permitted, may require less of a security lockdown to allow employees the required access to the information needed to perform their duties and communication between other servers to access information housed on the server.

The checklist can be created as a request form, possibly titled "Server Lockdown Request Form" and given to the group requesting the server to be completed and returned. This information will prove valuable as the lockdown procedures are laid out and will answer questions as to what can be done and what cannot.

Examples of the questions on the checklist are:

1) Name and IP addresses of server(s) that will communicate or be communicated from the server to be configured.
    - This will allow the IDS (Intrusion Detection System) agent to be configured to allow only specific port traffic between two servers, i.e. Server1 will be communicating with Server2 in which is a SQL server. That means that the IDS can be configured to allow specific communication on TCP port 1433 (this is the port SQL uses to communicate), between those two servers only. If the IDS is configured to allow port TCP1433, without an explicit IP specified, then anyone can hit that port from any server.

2) The server's main function, IIS, SQL, Proxy, etc.
3) The applications that will run on the server and its function.
4) What users will be accessing the server, inside access or Internet access and what method will they access the server?
5) Domain or Firewall Segment where the server will reside.
6) Service ports required including both TCP and UDP ports.
7) Services required, and what access the service account requires.

The checklist returned from the Development group for this server was fairly generic. The server will be a development server in the early stages of application development and the decision of what firewall segment the server will reside has not yet been determined. Therefore I decided to, as they say "error on the side of caution", by assuming the server will be accessible from the Internet and conducted the lockdown accordingly.

Note: Your checklist should be configured to query enough information so the server can be configured to meet your corporate security policy.

Server Scanning

Running LANguard Network Scanner to Determine Vulnerabilities

LANguard Network Scanner, GFI Software Ltd. http://www.gfi.com/lannetscan/, was used to scan the server after the security patches were installed. A few of the items found in the scan include:

1) Administrator account was not renamed.
2) Admin shares were not removed.
3) Password Policy was not secure.
4) Services that were unused or unnecessary were enabled.
5) There are vulnerable ports listed;
    a. TCP port 135, RPC (Remote Procedure Call) Endpoint Mapper. A few of the services using this port are:

    - DHCP (Dynamic Host Configuration Protocol) server communications
    - DNS (Domain Name Service) server administration
    - WINS (Windows Internet Name Service) server

    As an example, MS Exchange clients use port 135 to communicate with the Exchange server, if there is an IDS client is installed on the Exchange server and is set to block port 135 the Exchange clients (MS Outlook) will not be able to make a connection.

    b. TCP port 139, NetBIOS Session, I was once told that this is the single most dangerous port to leave open because this is the port that File and Print Sharing uses to communicate. With this closed no one on the network can see the shares,

but on an outside accessible server there should be no directories shared so it should be blocked.

c. TCP port 445 is used as a new transport for Windows 2000 SMB over TCP and UDP. This replaces the older implementation that was over ports 137 (NetBIOS name service), 138 (NetBIOS datagram) and 139 (NetBIOS Session). In our mixed network we will be using all of these.

d. TCP port 3389 - used by Terminal Services for communication between two servers.

6) Terminal Services were installed.

xxx.xxx.xxx.xxx [BLADE18] (Windows 2000)

LANguard Network Scanner

IP Address : **xxx.xxx.xxx.xxx**
HostName : **BLADE18**
MAC : **00-0B-CG-33-71-9A**
UserName : **BLADE18**
LAN Manager : **Windows 2000 LAN Manager**
Domain : domain
Operating System : **Windows 2000**
Computer usage : **NT/2k Member Server**
Service Pack 3
Time to live (TTL) : **128 (128) - Same network segment**

Shares (5)
- IPC$ - Remote IPC
- D$ - Default share
- F$ - Default share
- ADMIN$ - Remote Admin
- C$ - Default share

Groups (6)
- **Administrators** - Administrators have complete and unrestricted access to the computer/domain
- **Backup Operators** - Backup Operators can override security restrictions for the sole purpose of backing up or restoring files
- **Guests** - Guests have the same access as members of the Users group by default, except for the Guest account which is further restricted
- **Power Users** - Power Users possess most administrative powers with some restrictions. Thus, Power Users can run legacy applications in addition to certified applications
- **Replicator** - Supports file replication in a domain
- **Users** - Users are prevented from making accidental or intentional system-wide changes. Thus, Users can run certified applications, but not most legacy applications

Services (49)
- **ALERTER** - Alerter
- **BROWSER** - Computer Browser
- **CPQNicMgmt** - Compaq NIC Agents
- **CpqRcmc** - Compaq Remote Monitor Service
- **CpqSCW** - CpqSCW
- **cpqvcagent** - Version Control Agent
- **CpqWebMgmt** - Compaq Web Agent

- **CqMgHost** - Compaq Foundation Agents
- **CqMgServ** - Compaq Server Agents
- **CqMgStor** - Compaq Storage Agents
- **DefWatch** - DefWatch
- **Dfs** - Distributed File System
- **Dhcp** - DHCP Client
- **dmserver** - Logical Disk Manager
- **Dnscache** - DNS Client
- **Eventlog** - Event Log
- **EventSystem** - COM+ Event System
- **lanmanserver** - Server
- **lanmanworkstation** - Workstation
- **LicenseService** - License Logging Service
- **LmHosts** - TCP/IP NetBIOS Helper Service
- **MESSENGER** - Messenger
- **MSDTC** - Distributed Transaction Coordinator
- **NetBackup INET Daemon** - NetBackup Client Service
- **NETLOGON** - Net Logon
- **Netman** - Network Connections
- **Norton AntiVirus Server** - Symantec AntiVirus Client
- **NtmsSvc** - Removable Storage
- **PlugPlay** - Plug and Play
- **PolicyAgent** - IPSEC Policy Agent
- **ProtectedStorage** - Protected Storage
- **RasMan** - Remote Access Connection Manager
- **RemoteRegistry** - Remote Registry Service
- **RpcSs** - Remote Procedure Call (RPC)
- **SamSs** - Security Accounts Manager
- **Schedule** - Task Scheduler
- **seclogon** - RunAs Service
- **SENS** - System Event Notification
- **SNMP** - SNMP Service
- **SPOOLER** - Print Spooler
- **Surveyor** - Surveyor
- **sysdown** - HP ProLiant System Shutdown Service
- **TapiSrv** - Telephony
- **TermService** - Terminal Services
- **TrkWks** - Distributed Link Tracking Client
- **W32Time** - Windows Time
- **WinMgmt** - Windows Management Instrumentation
- **Wmi** - Windows Management Instrumentation Driver Extensions
- **wuauserv** - Automatic Updates

Password policy

- **Minimum password length : 0 chars**
- **Maximum password age : 42 days**

Minimum password age : no delay
Force logoff : never force
Password history : no history

HotFixes (18)
- **Q147222**
- **Q322842 - Windows 2000 Hotfix (Pre-SP4) [See Q322842 for more information]**
- **q323172 - Windows 2000 Hotfix (Pre-SP4) [See q323172 for more information]**
- **Q323255 - Windows 2000 Hotfix (Pre-SP4) [See Q323255 for more information]**
- **Q324096 - Windows 2000 Hotfix (Pre-SP4) [See Q324096 for more information]**
- **Q324380 - Windows 2000 Hotfix (Pre-SP4) [See Q324380 for more information]**
- **Q326830 - Windows 2000 Hotfix (Pre-SP4) [See Q326830 for more information]**
- **Q326886 - Windows 2000 Hotfix (Pre-SP4) [See Q326886 for more information]**
- **Q328310 - Windows 2000 Hotfix (Pre-SP4) Q328310**
- **Q329115 - Windows 2000 Hotfix (Pre-SP4) [See Q329115 for more information]**
- **Q329170 - Windows 2000 Hotfix (Pre-SP4) Q329170**
- **Q329834 - Windows 2000 Hotfix (Pre-SP4) [See Q329834 for more information]**
- **Q331953 - Windows 2000 Hotfix (Pre-SP4) Q331953**
- **Q810030 - Windows 2000 Hotfix (Pre-SP4) Q810030**
- **Q810833 - Windows 2000 Hotfix (Pre-SP4) Q810833**
- **Q811493 - Windows 2000 Hotfix (SP4) Q811493**
- **Q816093 - Windows 2000 Hotfix (Special Release) Q816093**
- **ServicePackUninstall**

Open Ports (4)
- **135 [epmap => DCE endpoint resolution]**
- **139 [Netbios-ssn => NETBIOS Session Service]**
- **445 [Microsoft-Ds]**
- **3389 [Terminal Services]**

Alerts (7) (**Legend : - High - Medium - Low - Information**)

Service_Alerts (3)

Administrator account exists
Description : It is recommended to rename this account

User Guest ( ) never logged on
Description : It is recommended to remove this account if not used

Alerter service enabled
Description : This service could be use in social engineering attacks. It is recommended to disable this service.
Bugtraq ID/URL : http://support.microsoft.com/support/kb/articles/q189/2/71.asp

Registry_Alerts (3)

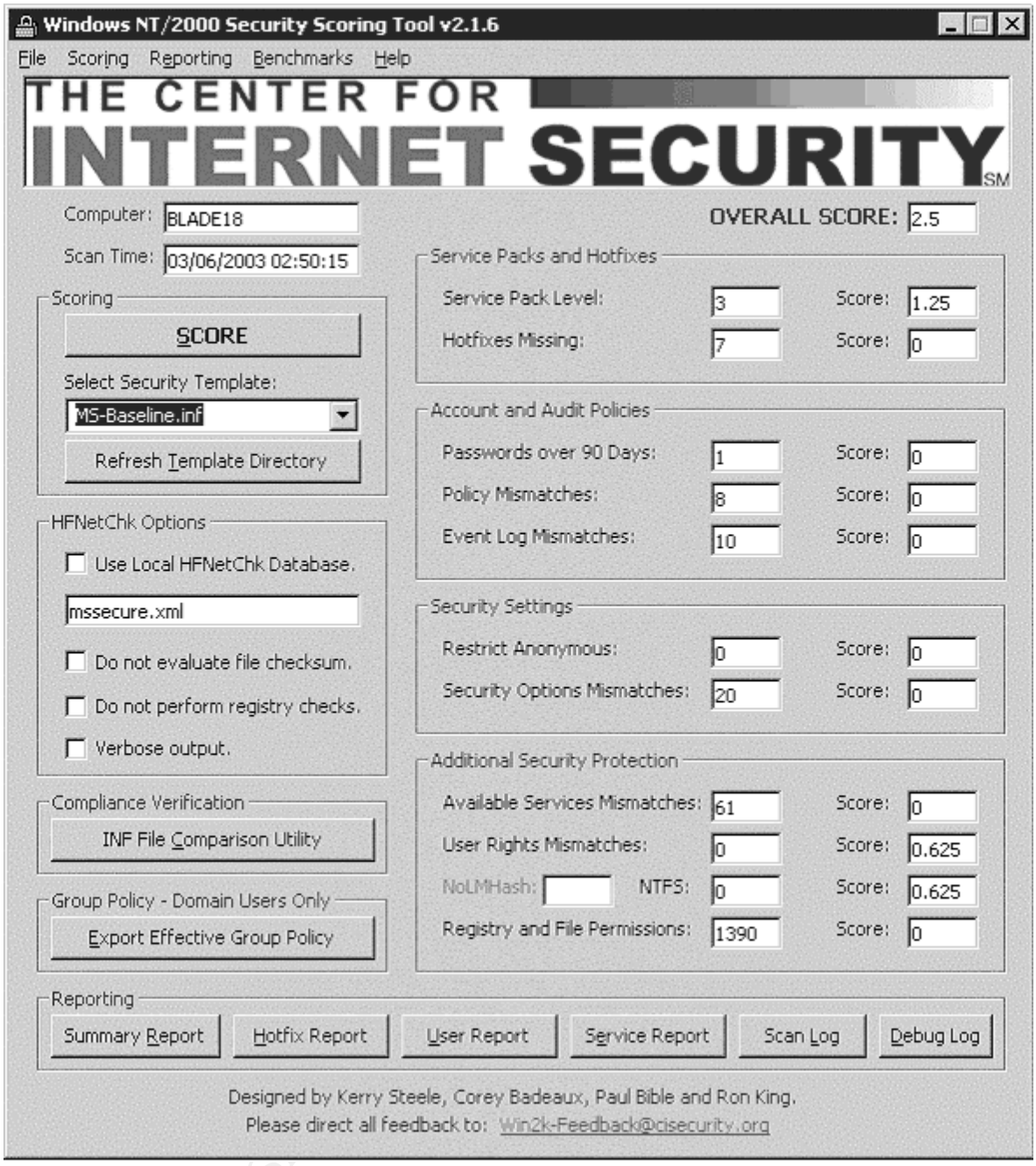
AutoShareServer (1)
Description : The administrative shares (C$,D$,ADMIN$,etc) are created on this machine.If you don't use them set AutoShareServer to 0 to stop creating this shares
Bugtraq ID/URL : http://support.microsoft.com/support/kb/articles/Q245/1/17.asp

Cached Logon Credentials
Description : Could lead to information exposure. Should be set to 0
Bugtraq ID/URL : http://archives.indenial.com/hypermail/ntbugtraq/1998/April1998/0003.html
DCOM is enabled
Description : DCOM is used to execute code on remote computers.Should be disabled if not used.
Bugtraq ID/URL : http://support.microsoft.com/support/kb/articles/Q158/5/08.asp

Info_Alerts (1)
Terminal Services
Description : Terminal Services are installed on this computer

Running CIS Tool to Score the Server

Next, I used CIS (Center for Internet Security Tool (http://www.cisecurity.org/), to scan the server using both the MS-baseline.inf and the Win2kSrvGold.inf files, both included in the CIS package, to get a comparison of the results. (Figure 1.1) These findings were kept for comparison after the lockdown.



(Figure 1.1) CIS Tool First Scan

Note: Only one scan is shown since both scores were the same.

2.0 During Snapshot

Apply Security Patches, Service Packs and Hotfixes

Terminology

In this guide we use the terms patch, service pack and hotfix interchangeably to mean changes to the software after its release. This is because the process for deploying them is the same in each case. However, each does have a more specific definition:

Service Packs

Service packs keep the product current, correct known problems, and may also extend your computer's functionality. They include tools, drivers, and updates, including enhancements developed after the product released. They are conveniently packaged for easy downloading.

Service packs are product specific, so there are separate service packs for each product. However, the same service back will generally be used for different versions of the same product. For example, the same service pack is used to update

Windows 2000 Server and Windows 2000 Professional.

Service packs are also cumulative — each new service pack contains all the fixes in previous service packs, as well as any new fixes and system modifications that have been recommended since. You do not need to install a previous service pack before you install the latest one.

Hotfixes or QFEs

Quick Fix Engineering (QFE) is a group within Microsoft that produces hotfixes — code patches for products. These are provided to individual customers when they experience critical problems for which no feasible workaround is available.

Occasionally you will see technical documentation refer to hotfixes as QFEs.

Hotfixes do not undergo extensive regression testing and are very issue specific — you should apply one only if you experience the exact issue it addresses and are using the current software version with the latest service pack.

Groups of hotfixes are periodically incorporated into service packs, at which time they undergo more rigorous testing, and are made available to all customers.

Security Patches

Security patches are designed to eliminate security vulnerabilities. Attackers wanting to break into systems can exploit these vulnerabilities. These are analogous to hotfixes but are deemed mandatory, if the circumstances match, and need to be deployed quickly.

Many security updates released are for client-side (often browser) issues. They may or may not be relevant to a server installation. You need to obtain the client patch to update your current client base and the admin patch to update the client build area on your server.

REF: Security Operations Guide for Windows 2000 Server:
http://www.microsoft.com/brasil/security/content/resources/resources/SOG_download.pdf

Applications I have Found Useful

There are various products on the market to check for required security patches, service packs and hotfixes. Some of these products will not only check for patches but will also install them. During the lockdown described in this practical only three of these applications were used, I am listing the other applications I have used on other occasions which have proven to be quite useful, applications such as:

Windows Update – Installed with Win2K, or can be accessed through the browser from: http://v4.windowsupdate.microsoft.com/en/default.asp, Windows update allows a computer, connected to the Internet, to be configured to automatically download and, if set, can install patches, as they are released without interaction. This can be used manually by selecting Start then selecting Windows Update. A browser window will open, connect to the Microsoft website where the "Scan for updates" link can be selected, Windows Update will scan the server and display the results. From this window the patches can be reviewed, selected or deselected depending on what is needed. When download is selected the patches are installed. This method is good for a small network but gets quite cumbersome in a larger size network. However this works well for newly built servers and can be adopted as one of the final steps in the server build process. Once completed another program, one listed below, will be used to verify that there are no additional patches needed.

Microsoft Baseline Security Analyzer- Free application provided by Microsoft, available for download, to scan and view missing patches, other security items needing attention will also be listed. The program URL is: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp.

This product is very helpful and can be used as the main scanning program or in tandem with other scanning applications to verify the findings of the second scanning application. This will help to increase Defense in Depth in that one application may not find all of the vulnerabilities and may suggest additional steps to be taken to lock down the server. Not all vulnerability-scanning programs are the "end-all" to server security.

HFNetChk – Command line tool to check for missing patches. This application makes up the base of the MBSA program listed above, #2. The program URL is: http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=34935A76-0B20-4F91-A0DE-BAAF969CED2B

If you prefer to use command line programs there is another program named **Qchain.exe** that will make the installation much quicker. QChain will allow the install of multiple patches with only one reboot. It is available for download from Microsoft webpage, the article detailing the options and switches can be read at: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861

Next command line program can be used to verify and list what patches are installed on the server. If the validation process finds a problem with an installed patch it will display it as a "hot fix number" and the suggested course of action, i.e. "Q329115: This hot fix should be reinstalled." The program URL is: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q282784

HFNetChkLT – Free version provided by the company that wrote the original HFNetChk used by Microsoft. This program will provide a GUI to view the results. The program URL is: http://www.shavlik.com/pHFNetChkLT.aspx. There is also a commercial version available.

UpdateExpert, from St. Bernard Software, can be used to determine the patch level of the server being prepared for production. UpdateExpert is typically installed on a centralized server having access to all segments of the network and allows the selection of servers to be scanned and the results can be viewed in a window where they can be reviewed by clicking on the patch in question and the related Microsoft article is retrieved from the Internet and displayed.

Once the items are selected they can all be installed at one time with or without a reboot between patches, depending what selection is made, or scheduled for installation of all selected patches at a later time. The database is updated from the UpdateExpert website after the newly released patches are reviewed. UpdateExpert will allow you to review a database of items which are classified by using different icons such as a lighting bolt to designate a critical update, a key to designate a security patch and so on. A "Conformance Report" can be generated to list what patches are not installed and are needed after comparing the list of items previously chosen from the master list along with other lists to help better identify the patch level of the server. The program URL is:

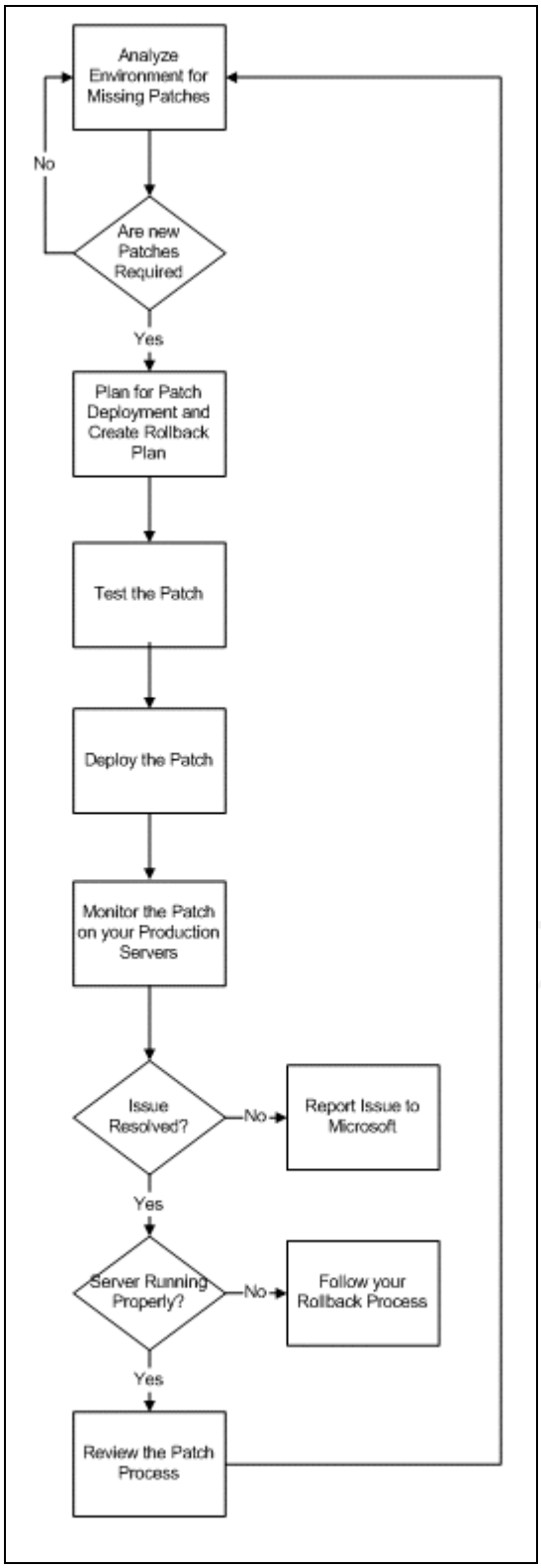
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

Important Note on Patches

Verifying the compatibility of all patches with server OS and installed applications in a test environment is imperative. This means that if there is a server running SQL 6.0 and a server running SQL 2000 and a set of SQL servers in a cluster then you must test the patches on each server in a test area. If you have three web servers and one with a custom application installed which is wired into IIS then you must test the patches for that server in a test environment also. It is very difficult to predict what the patches will do and what effect they would have on the applications and their configuration. Taking down a production server because an untested patch was applied and caused unexpected negative results is not a pretty site.

Security Patch Decision Making Flowchart

This reference flowchart helps in the decision making process of installing patches.



Ref: Microsoft Solution for Securing Windows 2000 Server – http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/SecWin2k/08patman.asp

SCANNING FOR PATCHES

Microsoft Baseline Security Analyzer

I first used MBSA to get a listing of both vulnerabilities and patches needed to secure the server. Using more than one program to scan a server provides a double-check which has proved to work well (and since the MBSA is provided free, as mentioned above, there was no additional strain on the budget). MBSA was installed on a workstation class server, (a high-end workstation with Win2K server installed), which has a primary function of scanning for vulnerabilities and applying patches. MBSA is one of a few different applications built for this task.

Once installed this application was pretty much straight forward. I will detail the steps used to retrieve the information.

On the Welcome screen “Scan a computer” was selected.

There was a choice of inputting the domain and server name, i.e., “\\domain\servername” or the IP address of the server that is to be scanned. I chose to use domain and server name, this also verifies that the server can be seen by its name over the network.

Leaving the “security report name” i.e. “%domain% - %computerName% (%date%)” at its default setting makes the filename easy to find when later selecting “Pick a security report to view” on the main menu.

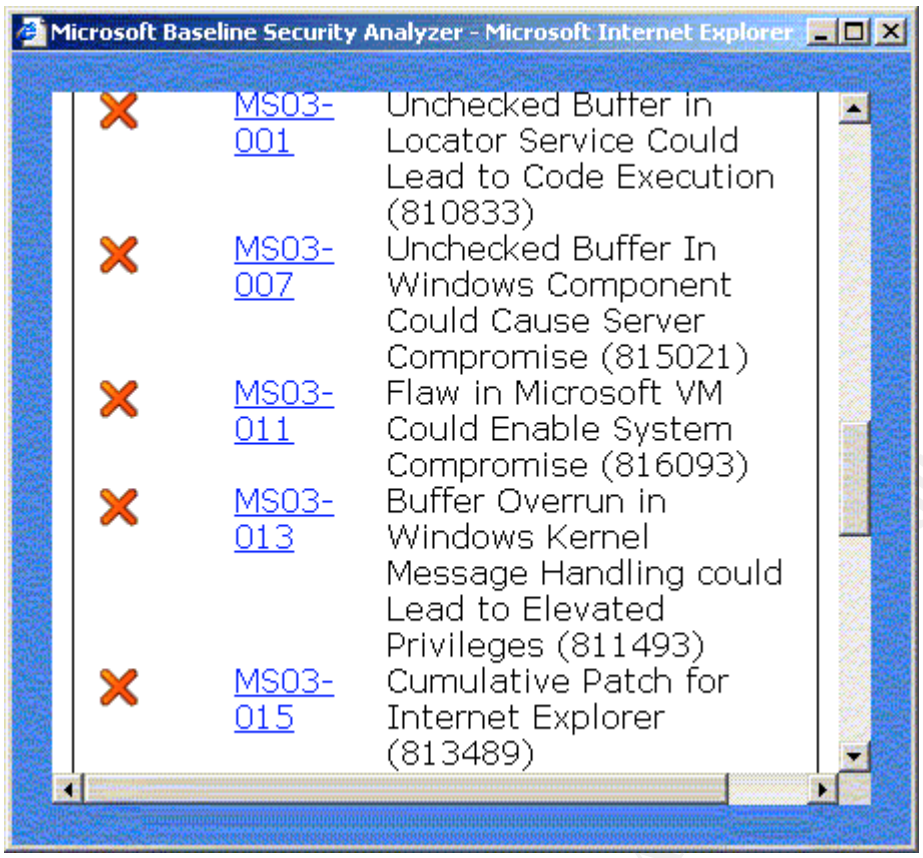
Next all checkboxes next to the scanning options were selected to provide as much detail as possible.

“Start scan” was selected. A security-warning box was displayed but since it was signed and distributed by Microsoft Corporation “Yes” was selected.

Once the scanning was complete the application presented a security report with a screen that included the items needing attention and those that did not (Figure 2.1). A red or a yellow “X”, a green checkmark, a blue star or a lowercase “i” in a circle denotes areas scanned and what action is suggested.

(Figure 2.1)

To view the missing patches I selected the “result details” link next to the “Windows Hotfixes” in the right hand window, which launched a new window (Figure 2.2) listing the patches and if they have been confirmed as missing or found on the computer.



(Figure 2.2)

The “Hotfix” MS number link can be selected, i.e. MS03-007, to launch the browser which will displays the Microsoft article page with a full description of the patch.

Even though I used Update Expert to apply the patches, I am adding details of Qchain since I have found it to be a good tool to have in my security-patching arsenal.

Once the patches are downloaded to a directory they can be run individually or there may be multiple patches that could require a reboot between each patch. “Qchain”, as mentioned above will make the install of multiple patches much smoother.

Qchain

Listing A shows sample code that illustrates how to use Qchain in a script to deploy hotfixes. The first three lines of the sample script apply three hotfixes. The -z switch applies the hotfix without rebooting; -m applies the hotfix in unattended mode, without administrative intervention; and -q applies the hotfix in quiet mode, hiding the extract and copy actions that take place. If you're applying patches manually, you might want to leave out the -q switch to view the progress of the hotfix.

Listing A: Sample Code to Chain Hotfix Deployments

```
Q296185_W2K_SP3_x86_en.EXE -z -m -q
Q285851_W2K_SP3_x86_en.EXE -z -m -q
Q285156_W2K_SP3_x86_en.EXE -z -m -q
qchain \\fschicago\logs\%computername%_qchainlog_060101.txt
shutdown /l /r
```

The fourth line in the script runs Qchain and specifies a file in which to log Qchain's results. The sample code puts the log file in the Logs directory on a server named Fschicago and specifies a unique filename based on the computer name and the date the script ran. Because you're likely to run Qchain at a later date, a unique log name prevents you from overwriting older logs. Finally, the Shutdown utility (from the *Microsoft Windows 2000 Server Resource Kit* or the *Microsoft Windows NT Server Resource Kit*) performs a local reboot of the machine by using the /l and /r switches. The /l switch performs a logoff; the /r switch performs a clean shutdown and a restart.

REF:

How to Install Multiple Windows Updates or Hotfixes with Only One Reboot:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861

and

Managing Security Hotfixes

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tips/sechotfx.asp

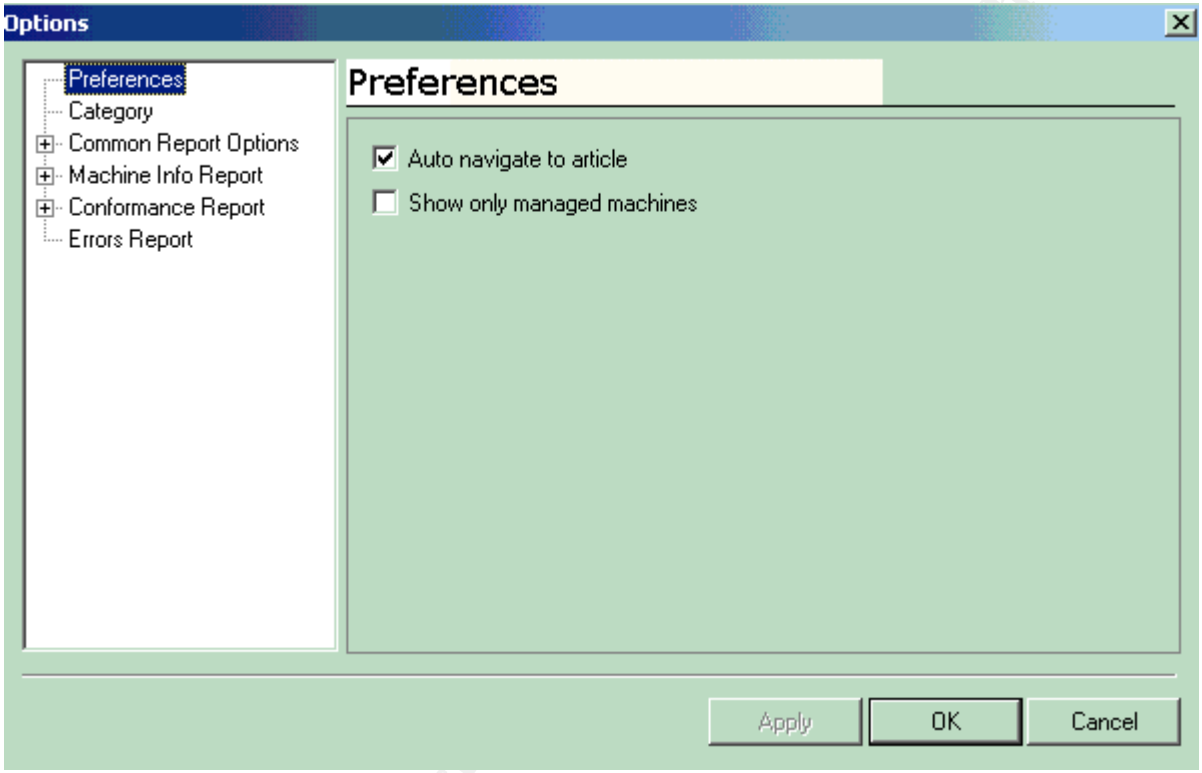
UpdateExpert

UpdateExpert 6.0 was used to determine the patch level of the server and install the patches. UpdateExpert (UE) is typically installed on a centralized server having access to all segments of the network.

Once UpdateExpert console was running I select the domain where the server resides.

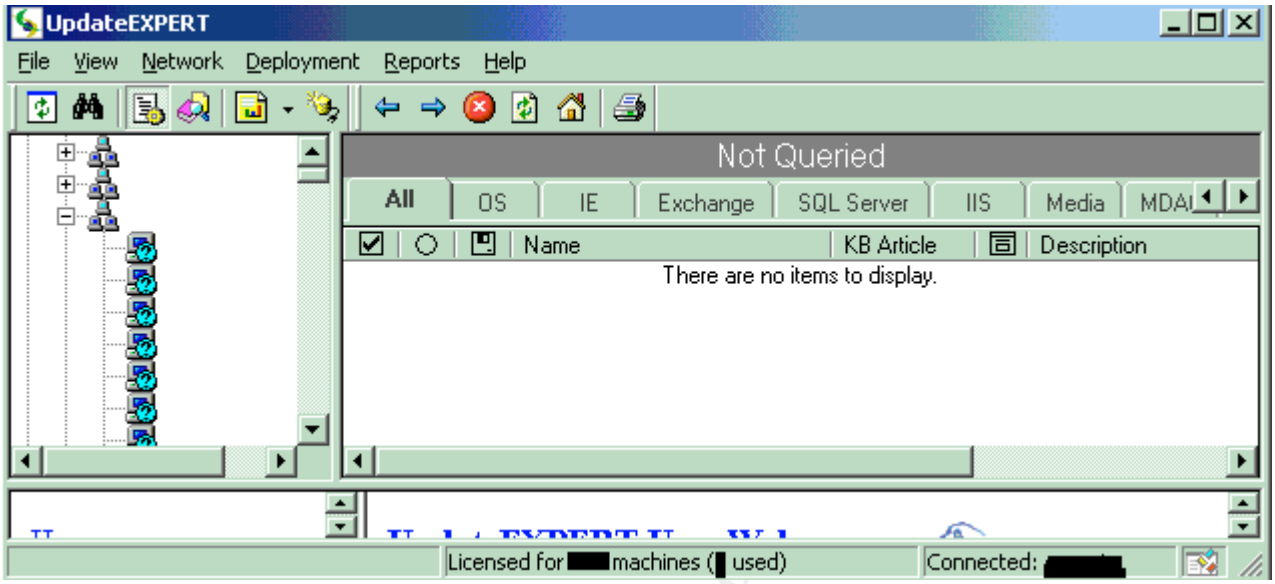
From “View – Options”

On right side the Options screen I removed the checkmark from “Show only manager machines.” (Figure 2.3.) Then selected “OK”



(Figure2.3)

On the left side of the screen (Figure 2.4) there is a list of servers and/or domains, I expand the domain by clicking on the "+" and then selected the server by right clicking and selecting "Manage Selected."



(Figure 2.4)

I returned to the "View – Options" window and selected "Show only managed machines. This removed all other servers from the list except for the server I was about to manage.

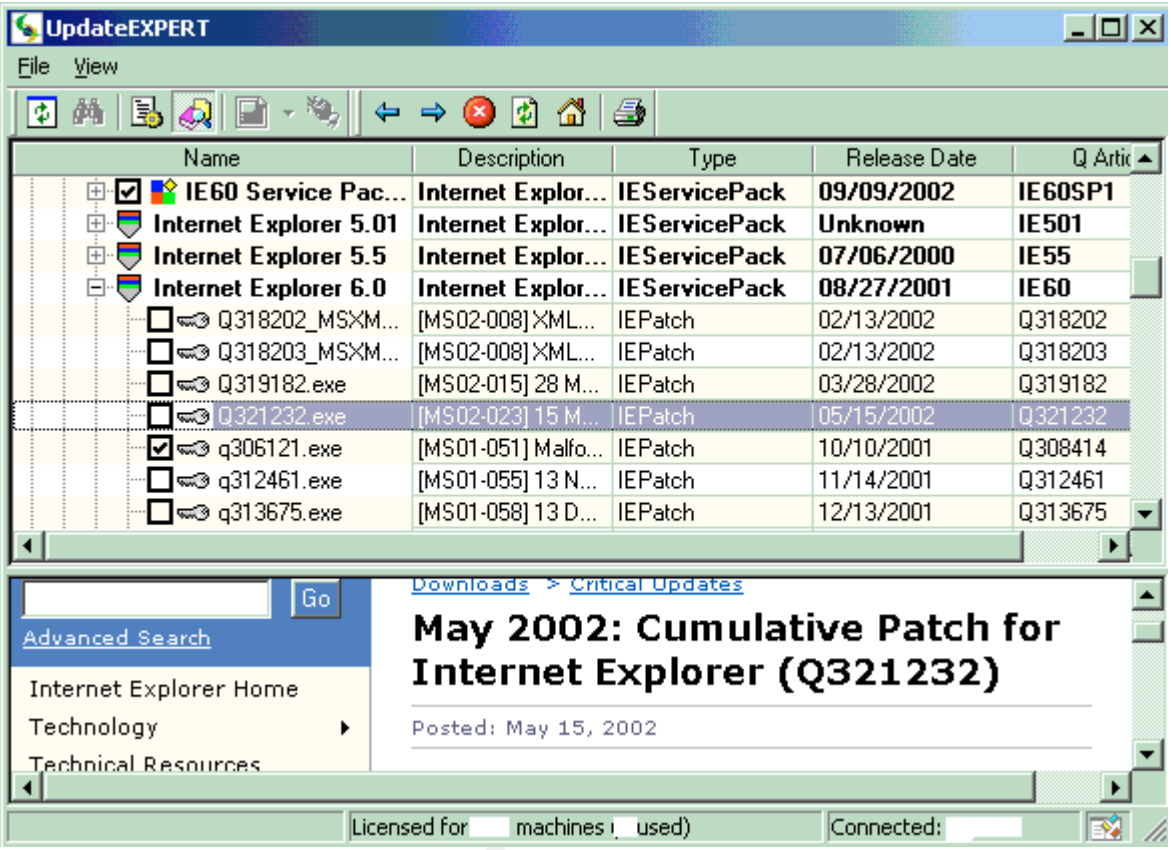
I right clicked on the server and selected "Query." This verified the connection to the server and the server OS (Win2K or NT). I then selected "Validate." This verified the patches already installed on the server.

At this point there was a list of service packs, hotfixes and patches in the right window. When the setting in "View – Show only Required Updates" was selected only those updates selected were shown.

Note on patch selection: Select only patches that you have verified as being required. Take caution when doing this, it is best to read each item to verify its use. For example, the Microsoft website patch description page states that a certain patch should only be applied to "correct a problem", so if that problem does not exist on your server then do not select that patch, just because it is a patch does not mean that it must be installed. An exception to that rule is when it is stated that the "patch should only be applied to correct a problem OR if the server is in an area where it may be vulnerable." This could mean that the risk of applying the patch might outweigh the risk of not applying it. This is a judgment call that is not always clear; some additional research may be required.

Updating patches where the update might interfere with development of an application, i.e. newer MDAC than required or adding SP3 when the application running on the server requires SP2 could cause undesired results. There are many variables, which must be tested and verified that they will function properly with the server where they will reside.

From the menu I selected “View – Research view” (Figure 2.5), changed the page to a view where I could select the OS and OS application i.e.: Internet Explorer, and the patches to be placed in the “Selected” patch list. As I clicked on each patch listed the Microsoft patch description page was displayed in the lower frame where I could review the details.



(Figure 2.5)

Note: (Internet access is required to view the description pages).

UpdateExpert Conformance Report

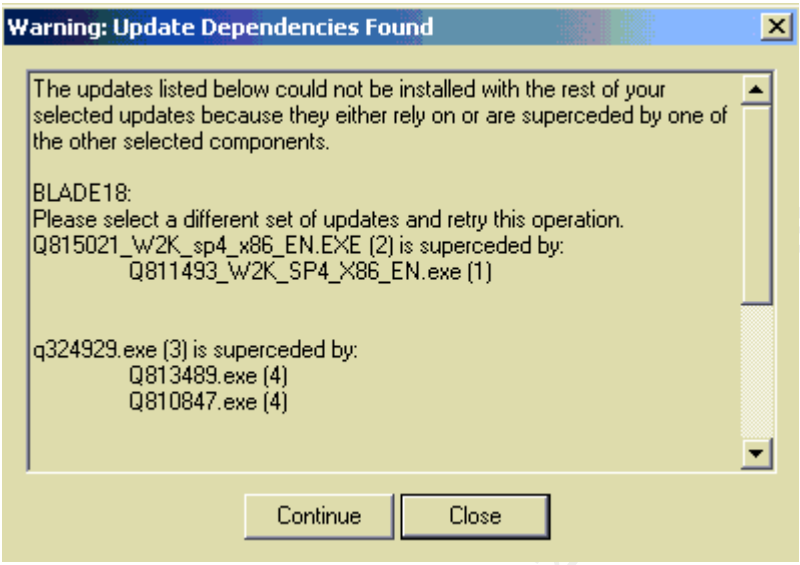
At this point from the taskbar I selected “Reports” – “Conformance Report”, in the lower screen a report showed which required patches were missing, this list was taken from the test server:

Group	UpdateEXPERT Conformance Report		
Machine Name	Operating System	Service Pack	Time Queried
QArticle	Description		Time Installed
Does Not Conform			
MICROSOFT WINDOWS NETWORK			
BLADE18	Windows 2000 Server	Service Pack 3	05/29/2003
Q324929	[MS02-068] December 2002, Cumulative Patch for Internet Explorer		Not Available
Q810847	[MS03-004] Cumulative Patch for Internet Explorer (Q810847)		Not Available
Q813951	February 2003, Update for Internet Explorer 6 SP1		Not Available
Q813489	[MS03-015] April, 2003,Cumulative Patch for Internet Explorer (Q813489)		Not Available
Q322842	A Lock Occurs Between Two Threads of System GDI in Windows 2000		Not Available
Q329170	[MS02-070] Flaw in SMB Signing Could Enable Group Policy to be Modified		Not Available
Q328310	[MS02-071] Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation		Not Available
Q810030	[MS02-069] Flaw in Microsoft VM Could Enable System Compromise		Not Available
Q810833	[MS03-001] Unchecked Buffer in the Locator Service Might Permit Code to Run		Not Available
Q815021	[MS03-007] Unchecked buffer in Windows component could cause web server compromise		Not Available
Q814078	[MS03-008] Flaw in Windows Script Engine Could Allow Code Execution		Not Available
Q331953	[MS03-010] Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks		Not Available
Q816093	[MS03-011] Security Update for Microsoft Virtual Machine (Microsoft VM)		Not Available

Q811493	[MS03-013] Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges	Not Available
MDAC27SP1	Microsoft Data Access Components 2.7 Service Pack 1	Not Available

Once the patches were selected and the screens switched back to “Network View”, I selected the server where the patches were to be installed, from the taskbar I choose “Deployment” – “Install Required.” At this point I was presented with a pop-up screen (Figure 2.6) stating that some patches may be “superseded” by others selected.

Note: It is not always necessary to select other patches as suggested; the patches that supersede are newer patches and contain what is needed to complete the install. If I am not sure I typically run the check again to see if any of the latest patches were not installed.



(Figure 2.6)

There were multiple screens displayed with two or three patches listed in each. The patches on each screen were to be installed together and the ones listed on the next screen were installed together and so on. The application makes sure that the patches are installed in order, if there is an order required. On each screen I removed the checkmark from the checkbox next to “Reboot”, (the application will not allow the checkmark to be removed if one of the patches on that window requires a reboot). When the last screen was displayed I left the “Reboot” checkbox selected to insure that the server would reboot once the installs were complete. An informational screen was displayed telling me that some installs were to be delayed, I selected “OK” to continue, this tells me that some patches relied on others to be installed first.

Applying a Security Template

There are a variety of security templates provided with the install of Windows 2000 (Win2K) residing in the “C:\WINNT\security\templates“ directory. These templates are configured for use on different types of servers.

- Templates that end in DC are configured for use in domain controllers.
- Templates that end in WK are configured for use in Win2K Professional workstations.

- Templates that end in SV are configured for use in standalone or member servers.

The basic and default templates are used to bring the server back to the same configuration the server was in when the base OS was installed. So if a mistake is made and the wrong template is applied then a basic template can be applied to turn back the changes made by the template to where the settings were when the OS was installed. The high security templates (i.e. highsecdc and highsecws) are, as the name implies, higher security templates. However in this configuration are not usable in their current state due to the fact that using the high security templates the Win2K server will refuse LAN and NTLM communications from pre-Win2K or "legacy" systems such as Windows NT or Windows 9X and these servers and workstations are in the NT 4.0 environment.

For detailed information reference the Win2K Help by going to "Start – Help" and search for "Templates" or "Predefined Security Templates."

There are many security templates available aside from the default templates some of the URLs are:

http://www.cisecurity.org/bench_win2000.html - Several templates are packaged within the CIS Benchmark Security Scoring Tool package and do add a bit more of a variety to choose from and use to test against the current or custom templates.

http://www.nsa.gov/snac/win2k/download.htm - Templates available including many security recommendation guides from NSA (National Security Agency). This is an excellent resource for not only templates but also whitepapers that detail securing many types of configurations such as Windows 2000, IIS, ISA, Active Directory, IPsec and many others.

To configure the MMC for applying templates reference article 309689 on Microsoft's website http://support.microsoft.com/default.aspx?scid=kb;en-us;309689 or the white paper "Step-by-Step Guide to Using the Security Configuration Tool Set" located at http://www.microsoft.com/windows2000/techinfo/planning/security/secconfsteps.asp which will give a more detailed view of applying security templates. Once the plug-ins are installed the MMC will look somewhat like the screenshot (Figure 2.7) below:

Security Templates MMC (Figure 2.7)

I have made it a practice that if the implementation of a customized security template is delayed, I will apply one of the pre-configured templates to secure the server until a customized template is created, tested and applied. This is preferred over allowing a server to run with only default settings leaving it much more vulnerable.

Once the security snap-ins were installed I applied a pre-configured template to the BLADE18 server by the steps outlined below:

1) I right clicked on the "Security Configuration and Analysis" snap-in and selected "Open Database", this is the file where the configuration will be saved for the server to access when the server is started and periodically during operation, (I used the server name to name the database, it is helpful to name the database the same name as the server for later reference and if they are stored in a central location), I then selected "Open."
2) A second window appeared; I selected "securews.inf", (good for securing workstations and servers), and then selected "Open."
3) I right clicked on "Security Configuration and Analysis" and selected "Analyze Computer Now"; this compared the template settings with the current configuration data.
4) I clicked "OK" on the "Perform Analysis" window.
5) At this point I reviewed the settings by selecting the "+" and expanding the various selections.
6) When I was finished reviewing the settings, I right clicked on the "Security Configuration and Analysis" snap-in and selected "Configure Computer Now." This applied the settings to the server. There was no need to configure the settings at that time since I knew I was going to custom-configure a template.

Customizing the Template

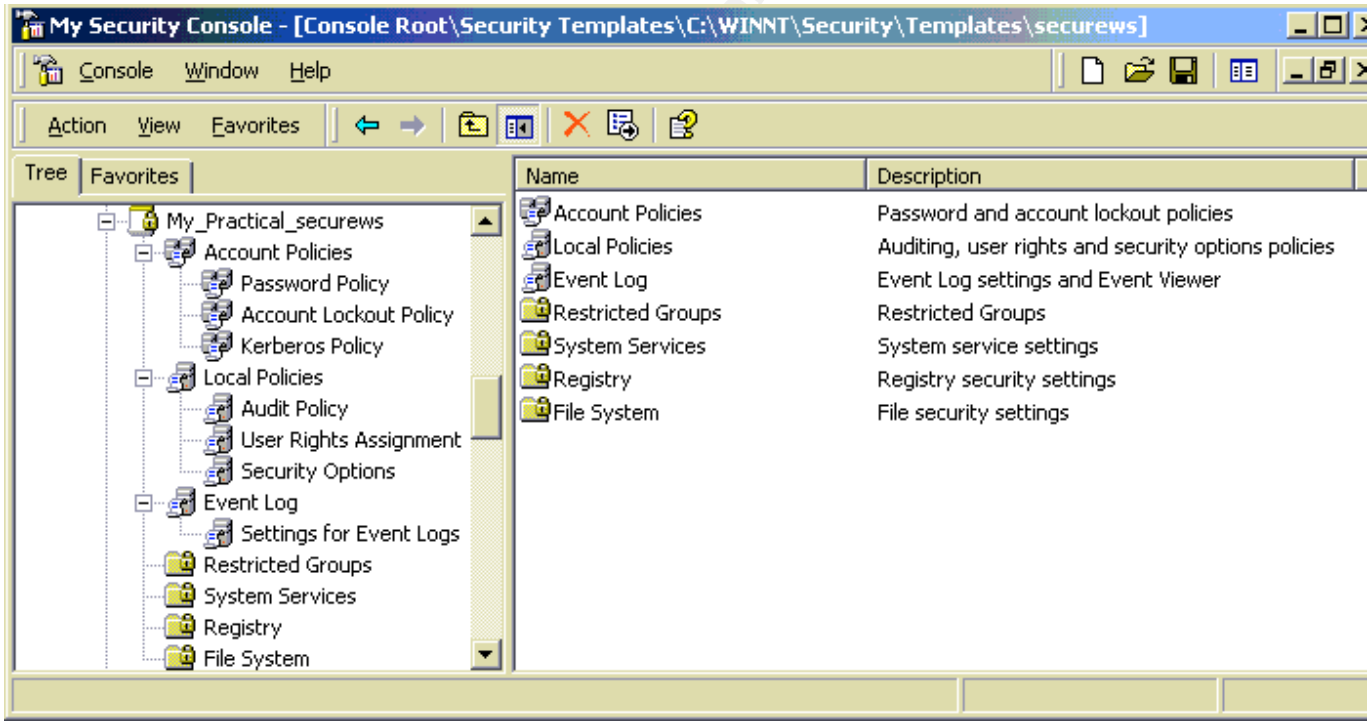
Configuring the MMC

To begin

1) I selected “Start” – “Run” – “Administrative Tools”, selected what should be named “ServerName.msc”, this is the MMC console configured earlier containing the “Security Configuration and Analysis” and “Templates” snap-ins.
2) I expanded “Security Templates” and “C:\WINNT\SecuityTemplates”, there was a list of templates displayed.
3) I right clicked on “securews” and selected “Save As.” Selecting a new name and clicked “Save.”

(A new template can also be created by right-clicking on the “C:\WINNT\Security\Templates” and selecting New Template, give it a name and description and select OK)

4) I located the newly named template in the list, expanded the list of root items, (Figure 2.8) and began to review the settings, adjusting accordingly.
5) Once completed with the changes I right clicked on the template and selected “Save.”



(Figure 2.8)

I have placed the security template examples in Appendix A and have included only those settings that were changed. The listings are taken directly from the "Security Configuration and Analysis" and the "Templates" snap-ins. After the server was handed over to the group using it and the server should go into production these settings, along with all the others, will be reviewed to see if there have been any changes to make the server vulnerable**.**

I cannot stress enough the need to complete secondary check prior to a server going into production. I have had servers that were initially locked down, had applications installed and configured and were requested to be placed into production only to find that the server was now unsecured by items being changed or added like, anonymous FTP enabled, anonymous IIS user enabled with a simple password, an account similar to a guest account created with too much access and allowing the Everyone group Full share and NTFS access to (Parent) directories and the (children) directories below. It is not always an easy task to keep track of the servers but working with others to track the requests I have found that it is best that the requests to move a server into production pass my desk, we do this by a checklist that accompanies each server through the request process. If the checkbox for a security scan is not checked the server does not make production and management backs us all the way.

Reviewing the Security Policies

Account Policies

The Account Policies are made up of three areas:

Password Policy – Changing these settings make it more difficult for passwords to be guessed.

Account Lockout - Changing these settings make it more difficult for an intrude to break into the server, as I have set, if the intruder attempts to log in more than five times they will be locked out of the system for 30 minutes. If this is a random intrusion attempt most intruders will get fed up and move on to easier pastures.

Kerberos – Is a private key encryption security protocol used in Windows 2000, which is replacing NT LAN Manager used in NT4.0. Since ours is an NT network NTLM is still required, so this area of the template was skipped.

Local Policies

The Account Policies are made up of three areas:

Audit Policy – Most of the auditing was changed, an item to note is the setting "Audit object access", this setting is one that would fill the Event Viewer very quickly due to, as the name suggests, ever time an object is accessed it is logged. This setting should only be used when a lot of data needs to be collected, an example would be assisting in troubleshooting an application; this setting was left set to "No Auditing."

User Rights Assignment – Adjusting the user rights here is important to understand. In some documentation I have read, the understanding of the affect that these changes have on a system seems to be assumed. It is a good practice that all templates settings, especially these, be tested on a server where the OS can be wiped out and reinstalled without the loss of important data.

Early on I found that once you place a "Deny" you must also place an "Allow", an example would be setting "Deny logon locally" set to deny "Guests" but then leaving the "Log On Locally" not set or set with no username specified, (the checkbox selected next to "Define these policy settings in the template") will result in no one being able to log into the server. This is because the server was told who could not log in but was not told who could. This includes accessing the server locally and via Terminal Services.

If the server is locked down and admin shares removed the server is most likely going to need to be re-installed, however if the admin shares, (i.e. \\servername\C$\), are still in place there is a way to get the settings back to allow a login by using the "ntrights.exe" from the command line or from a batch file. This command is part of the Win2K Resource Kit. I have listed MS articles referring to this command and its use, #279664, 285793, 276590 and 279664. These articles all relate to the message that is received when the above scenario has been applied, "The local policy on this system does not permit you to log on interactively." An example of its use would be, from a command prompt of a server on the same domain:

Note: These two lines can be placed into a batch file or typed one at a time.

Ntrights –m \\servername -u Guests –r seDenyInteractiveLogonRight

Ntrights –m \\servername -u Everyone +r SeInteractiveLogonRight

The first line will remove the "Guest" account from the local security settings on the server specified. The second line will add the "Everyone" account to the local policy to allow the server to be logged into. I used the "Everyone" group and changed it later but any account could be used in its place.

Security Options

This section covers many items that deal with controlling security settings for the server.

I set the two options "Rename administrator account" and "Rename guest account" to "Not defined." The administrator and guest account should be set manually on each server, if it is set in the template and used on several servers then if one account is compromised you have the same name on each server to be used to compromise those servers. With a different name on each server we increase the Defense in Depth.

There are two other settings that I have configured that can help to protect the company legally. The legal statements below are seen, when anyone logs onto the server, as a message screen where the person logging in would have to click "OK" to continue and with that are accepting the terms.

- "Message Text for users attempting to log on" – "This system is restricted to authorized users for legitimate business purposes and is subject to audit and monitoring. Actual or attempted unauthorized access, use or modifications of computer systems is a violation of federal and state laws. Information obtained on this server is proprietary to "Company Name" and its subsidiaries and affiliates. Use of such information is restricted to purposes for which access has been authorized, and all information must be kept confidential in accordance with state and federal privacy laws."
- "Message title for users attempting to log on" – "Company Name" - Access Restricted

Event Log - We use a Syslog server to collect Event Log information, for this reason I have set the logs to be overwritten "As needed" and the size of the logs to 10 Megs, this lessens the chance of the log being overwritten too quickly, gives us time to collect logs from multiple servers and makes it more difficult for an intruder to cover their tracks by an event that would be written enough times that the log fills up and overwrites the evidence of them being there. Collecting logs also allows the "Shut down server when the event logs are full" to be "disabled."

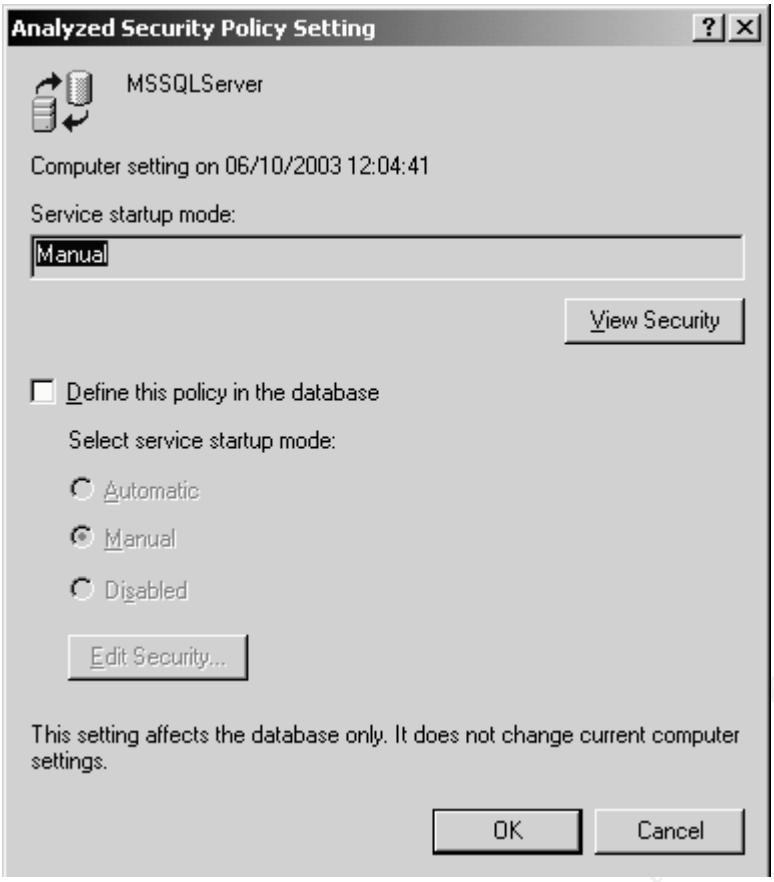
Restricted Groups – I did not add anything to the area, the settings here are only temporary and should not be set in a template. These settings can be used for granting temporary access to individual users by adding them into a group, such as Power Users or Backup Operators, but in this process it is not necessary to utilize this feature since it should only be used as a temporary manual change, i.e. the administrator will be out in training for a week and requires that someone assume their role for that timeframe.

System Services

I have found that some settings for system services will be different with each server and the task it performs but for the most part these settings have worked for most servers. The default "Startup" and "Permissions" settings of the template were all originally set to "Not Defined" so I removed that column and therefore the list in Appendix 1 will reflect the adjustments made to the services in the custom template.

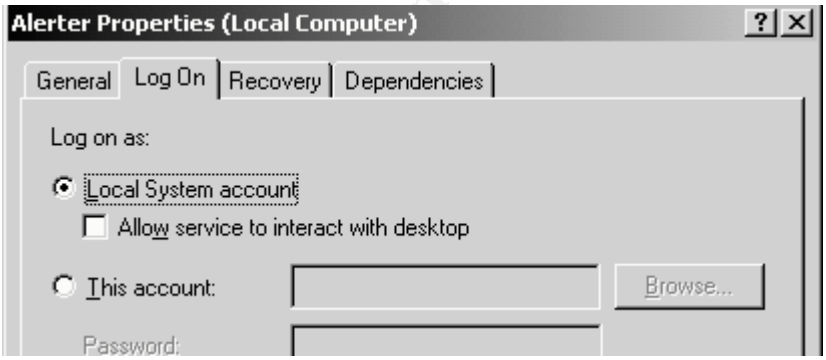
On a test server I applied the service settings individually to verify that there was no interruption in service. Therefore, it is important not to place the server into production directly after applying the template; there must be a testing period added into the time schedule.

In the Permission column, of the System Services chart in Appendix 1, the setting "Configured" means that the "Define this policy setting in the template" checkmark was set to adjust the permissions and the "Not Defined" means there is no change set. Refer to (Figure 2.9).



(Figure 2.9)

Take care when changing any permission for the services. A service typically operates under a "Service Account" which should have the minimum privileges necessary to complete the function that the service performs. This precaution prevents an intruder from accessing the account. The "Allow service to interact with desktop" should not be selected due to the fact that a malicious user could take control of the services. This would be accessed from the Services plug-in in the Computer Management screen or the Services MMC by "double-clicking" on the service and selecting the "Log-On" tab. (Figure 2.10)



(Figure 2.10)

For additional information on adjusting the permissions see:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sys_srv_permissions.asp

Applying Service Changes

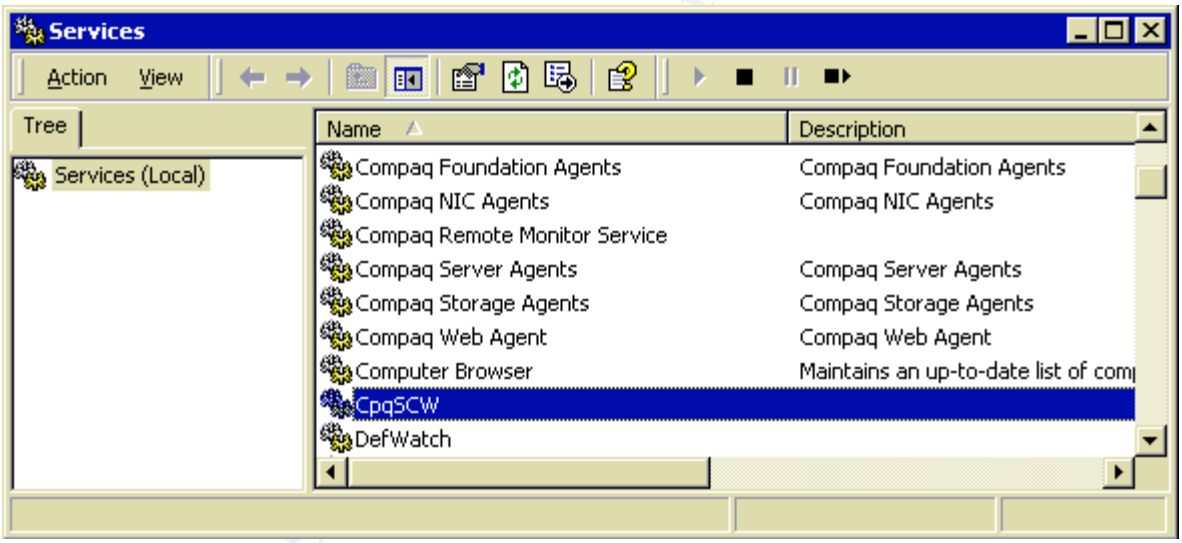
There are items to note in reference to changing the system services startup options.

If a service is set to manual, an application or service can start that service. As an example, on another test server where I had a spam server configured using IIS, I set the IIS service to manual, rebooted the server and checked the services list again and saw that the IIS service had started. I then double clicked on the “IIS Admin Service” and selected the “Dependencies” tab, I could see that one of the services used by the spam product was dependant (can not run without the other) on the IIS service, since that services was set to “Automatic” while it was starting it also started the service it needed, being the IIS service. When I “Disable” the IIS service the spam product will not work and I received errors stating:

“Error 1068:The dependency service or group failed to start”

Reviewing the dependant services is important to avoid a configuration that would allow one service to start another and with that creating a an additional Attack Vector (a route that can be used by an intruder to attack or exploit the server) or the Event Viewer receiving a number of errors because a service cannot start due to one of the services it is dependant upon being disabled.

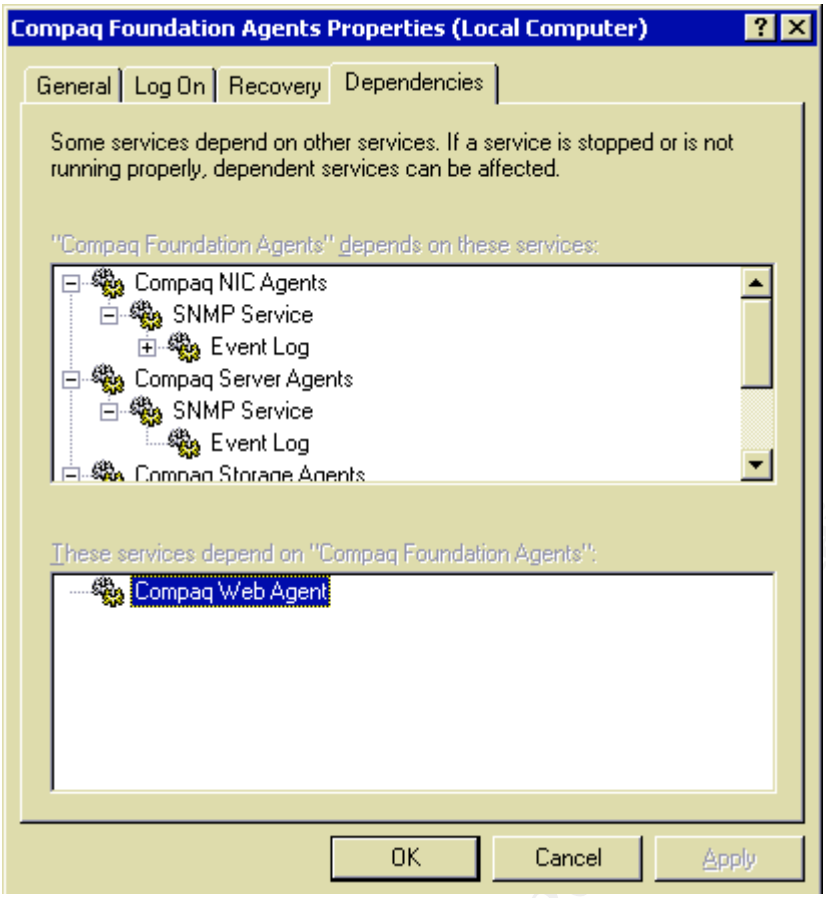
Other items I took into consideration were Compaq services installed to manage the hardware. See (Figure 2.11)



(Figure 2.11)

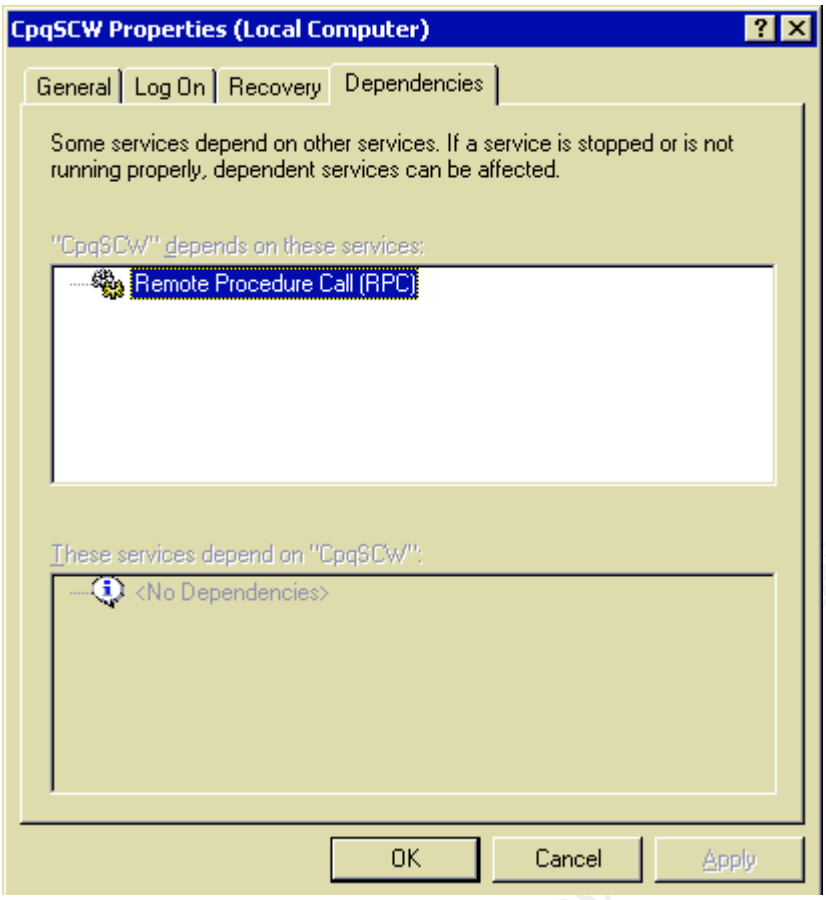
With these Compaq services installed, which are not included in the normal security lockdown procedures guides, the dependency list for each service was reviewed to determine which service might need to run and not be disabled as some lockdown lists might suggest. Below are two examples:

This example (Figure 2.12) required that other Compaq, SNMP and Event Log services be running to enable the service to function.



(Figure 2.12)

This example (Figure 2.13) required that only the RPC service be running.



(Figure 2.13)

Services Items Changed

Computer Browser – Maintains an up-to-date list of computers on the network. Lockdown documentation suggests that this service be disabled, however with this template being applied to servers within our NT domain environment it is required that the server be accessed and the server may access the network through My Network Places, Windows Explorer, etc. This service was set to “Automatic.”

Automatic Updates – This service can be installed when running Microsoft Auto Update. In a domain where service packs, security patches and hot fixes are tested in a controlled test area and reviewed by the application support team prior to being installed, allowing Auto Update to install patches in the background is not acceptable and detrimental to maintaining a controlled server environment. If installed the Auto-Update Icon can be found, in the Control Panel. This service was set to “Disabled”

IIS Admin – This service was disabled so that if IIS was installed it would be disabled until IIS has been hardened or the MS IIS Lockdown Tool has been run. The basic install of IIS contains parts that are vulnerable and should not be left running and available for attack. If at a later date this server becomes an IIS server and I had a template created specifically for an IIS server, I would apply the template over the template used in this document to adjust the additional services. Templates can be cumulative. Note: If IIS is not required it should be uninstalled.

Print Spooler – This service manages the local print queue and print jobs locally and remotely. If the Print Spooler service was disabled, users of the server would not be able to print. During testing I found that when I connected to the server via Terminal Services that I could not print from the server due to this service being disabled. Printing is used on many of our servers so this service was set to automatic.

SNMP and SNMP Trap – Both of these services were needed to enable the sending of messages to our SNMP management server. The use of SNMP (Simple Network Management Protocol) does create security concerns however the cost must be weighed of running the service in comparison to the information gathered from each server. Some IDS applications also use SNMP traps to report intrusion attempts. In these cases the advantages to using SNMP outweighs the risk. This service was set to "Automatic"

Task Scheduler – Lockdown documentation suggests this service be set to "Disabled" however, our servers use scheduled tasks to set server time and run batch jobs to for various tasks. This service was set to "Automatic."

From a clean install of Windows 2000 Server there were a large number of services installed and started by default, not to mention any new services that may be a part of other applications installed at a later date and with that comes the chance of one of the new services being dependant on services that were disabled. This makes understanding the services and what they do even more important. Remember, the more services running, the more vectors of attack there are available.

Registry Changes

I have found through trial and error that the registry setting must be considered and tested very carefully. Items to include the functionality of the server applications, how or if the server interacts with the network, and settings that may interfere with the server booting are important to consider. If these things are not considered the server could be rendered inoperable to the point of needing to re-install the OS.

Important note: Prior to making any changes there should be a back up made of the registry, refer to Microsoft article:

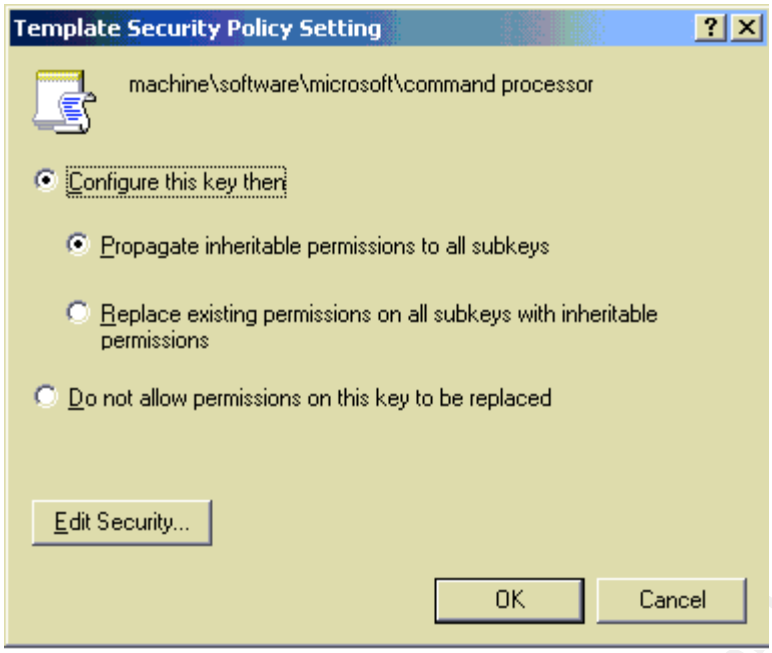
HOW TO: Backup, Edit, and Restore the Registry in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B322755

Understanding the meaning of each registry policy setting is very helpful to properly implement the settings.

(Figure 2.14) appeared when I double-clicked on a security key or right clicked on the key and selected "Security."

1) Propagate Inheritable permissions to all subkeys – This will set the permissions at the selected key and all keys below it. It will also merge these permissions with the permissions already set at the other keys.
2) Replace existing permissions on all subkeys with inheritable permissions – This will set the permissions on the selected key and replace all existing permissions on all keys below with inheritable permissions. It will replace the permissions on each subkey with permissions set at the selected key.

3) Do not allow permissions on this key to be replaced – Will not allow the permissions on the selected key to be replaced.



(Figure 2.14)

File System Changes

From this area the NTFS permissions can be set for all folders. The file and directory NTFS permissions are very important and should be configured to meet the needs of the applications slated to run on the server but given only the minimal NTFS permissions that will allow the application to function but keep intruders out. After I configure a server and release it to the group using it and once they have set up the applications, I review the settings to see if any further adjustments should be made.

Listed below is an example of what I did in adding NTFS permission changes to the registry that will be adjusted when the template is applied. This process can be used to add any folder/directory on the server; this folder is used as an example and also to emphasize the need for securing this particular directory.

The "%systemroot%\repair" directory is one that should be very secure considering the files stored within contain system information, i.e. accounts and passwords.

This was done from the File System area in the template.

1) I right clicked "File System" and selected "Add File"
2) An Add File and Folder window appeared; in the list I selected %systemroot%\repair (usually c:\winnt\repair) and clicked "OK."
3) The Database Security window appeared where the permissions can be set. The "Everyone" group was removed and replaced with the "Administrators" group and the "System" account, both were given Full permissions.

4) The “allow inheritable permissions from parent to propagate to this object” checkbox was selected and was removed. If I had not removed the checkmark the permissions that I had just set would have been changed to the permissions of the parent folder.
5) On the Template Security Policy Setting window I selected “Replace existing permissions on all subfolders and files with inheritable permissions” and clicked “OK.” This sent the NTFS permissions to the files and directories within the folder to protect them from unauthorized access.

3.0 After Snapshot

Server Scanning

Running UpdateExpert to Confirm Changes

UE was run again, I selected “Reports” – “Conformance Report” the report was displayed to verify the install. The list below shows that there were no servers under the category of “Does Not Conform” but the server “BLADE18” was listed under the “Conforms” category and there were no patches required.

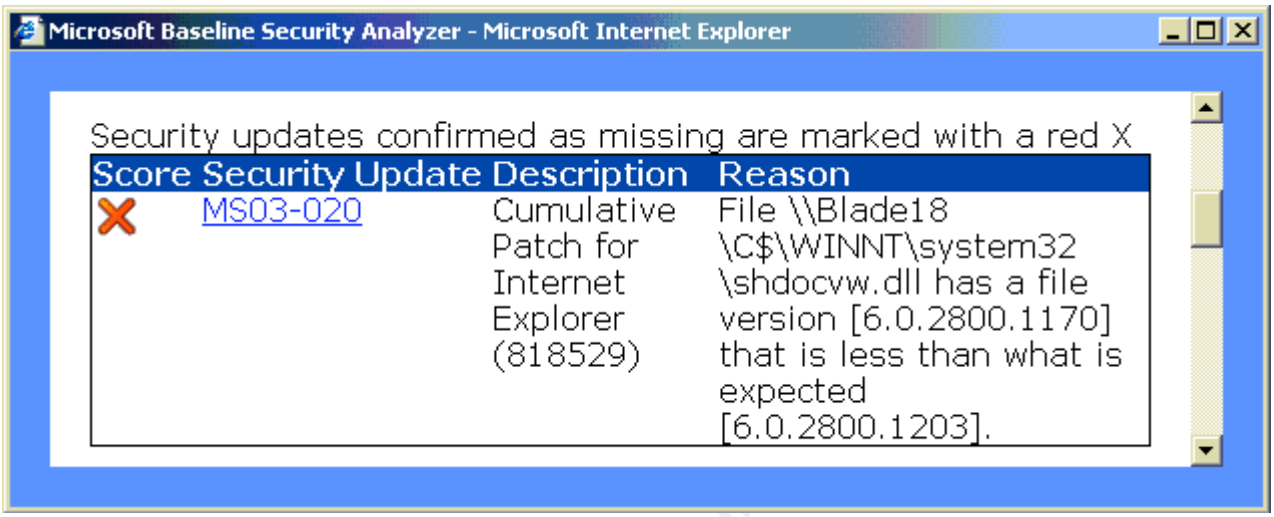
UpdateExpert Conformance Report

Group	UpdateEXPERT Conformance Report		
Machine Name	Operating System	Service Pack	
QArticle	Description		
Does Not Conform			
MICROSOFT WINDOWS NETWORK			
Conforms			
MICROSOFT WINDOWS NETWORK			
BLADE18	Windows 2000 Server	Service Pack 3	

Next from the Windows Desktop I selected “Start” – “Windows Update”, once the scan was complete the MS webpage displayed a message stating that no updates were required.

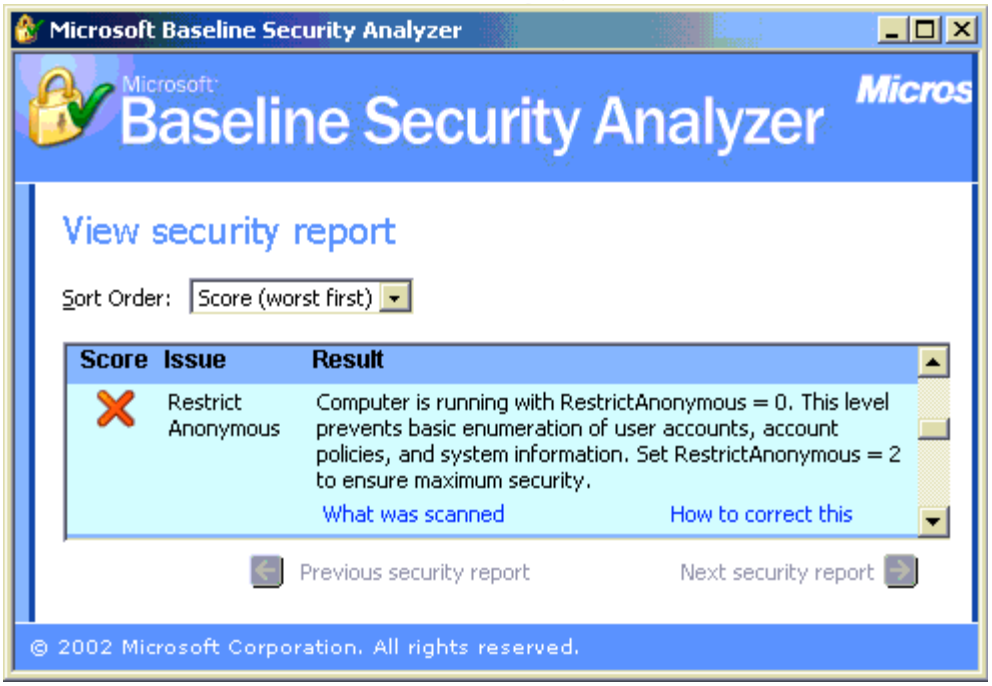
Running MBSA to Confirm Changes

MBSA was run again, (Figure 3.1) shows how it looked with all the patches installed. From the results we see that the MBSA program found one patch that may not have been installed, or it could not verify that it was installed. To verify within UpdateExpert I reviewed the Machine Report, which lists the patches and the date installed, to see if the patch was listed, it was not so I downloaded the individual patch and it was installed.



(Figure 3.1)

Scanning the server using MBSA there was also one registry issue that required attention. (Figure 3.2)



(Figure 3.2)

Within MBSA the “How to Correct This” selection states:

Restrict Anonymous Users Issue

The **RestrictAnonymous** registry setting controls the level of enumeration granted to an anonymous user. If **RestrictAnonymous** is set to 0 (that is, the default setting), any user can obtain system information, including: user names and details, account policies, and share names. Anonymous users can use this information in an attack against your system. The list of user names and share names could help potential attackers identify who is an administrator, which computers have weak account protection, and which computers share information with the network.

Solution

To restrict anonymous connections from accessing this system information, change the **RestrictAnonymous** security settings. You can do this through the Security Configuration Manager snap-in (setting is defined in the Local Policies portion of the default security templates), or through a registry editor. You can change the registry setting from 0 to 1 in Microsoft Windows NT 4.0, or from 0 to 1 or 2 in Windows 2000:

0 - None. Rely on default permissions

1 - Do not allow enumeration of Security Accounts Manager (SAM) accounts and names

2 - No access without explicit anonymous permissions (not available on Windows NT 4.0)

Caution: Before you set this value to 2, see article Q246261, "How to Use the RestrictAnonymous Registry Value in Windows 2000." It is recommended that you do not set this value to 2 on Domain Controllers or Small Business Servers (SBS) in mixed-mode environments (e.g., networks with downlevel clients). In addition, client machines with **RestrictAnonymous** set to 2 should not take on the role of master browser. Please refer to the Knowledge Base articles below for more details on configuring **RestrictAnonymous** on Domain Controllers and Windows 2000 environments to understand potential compatibility issues when using this setting.

Additional Information

The **RestrictAnonymous** registry key controls the level of enumeration granted to an anonymous user. This key can be set to any of the following values:

0 - None. Rely on default permissions

1 - Do not allow enumeration of SAM accounts and names

2 - No access without explicit anonymous permissions (not available on Windows NT 4.0

Note: In Windows XP there is a new registry setting (**EveryoneIncludesAnonymous**) that controls whether permissions given to the the built-in Everyone group apply to anonymous users. By default, permissions granted to the Everyone group do not apply to anonymous users in Windows XP, which therefore provides the same level of anonymous user restrictions as the RestrictAnonymous setting in previous Windows operating systems. The **EveryoneIncludesAnonymous** setting can be configured through the Security Configuration Manager snap-in (setting is defined in the Local Policies portion of the security template) on Windows XP Professional systems, or through a registry editor. This setting is located within the

same registry key as **RestrictAnonymous** (see the Knowledge Base articles below for registry path information).

Additional Resources

Restricting Information Available to Anonymous Logon Users (Q143474) (Windows NT 4.0)

How to Use the RestrictAnonymous Registry Value in Windows 2000 (Q246261)

The server is now up to date on all patches and verified using MBSA, UpdateExpert and Windows Update. All patches have been logged and documented. Logging the changes will aid in troubleshooting if there are any difficulties with applications installed at a later date.

Running LANguard to Confirm Changes

Once the procedures outlined above were complete the server was once again scanned, using LANguard to verify the results, the scan showed that:

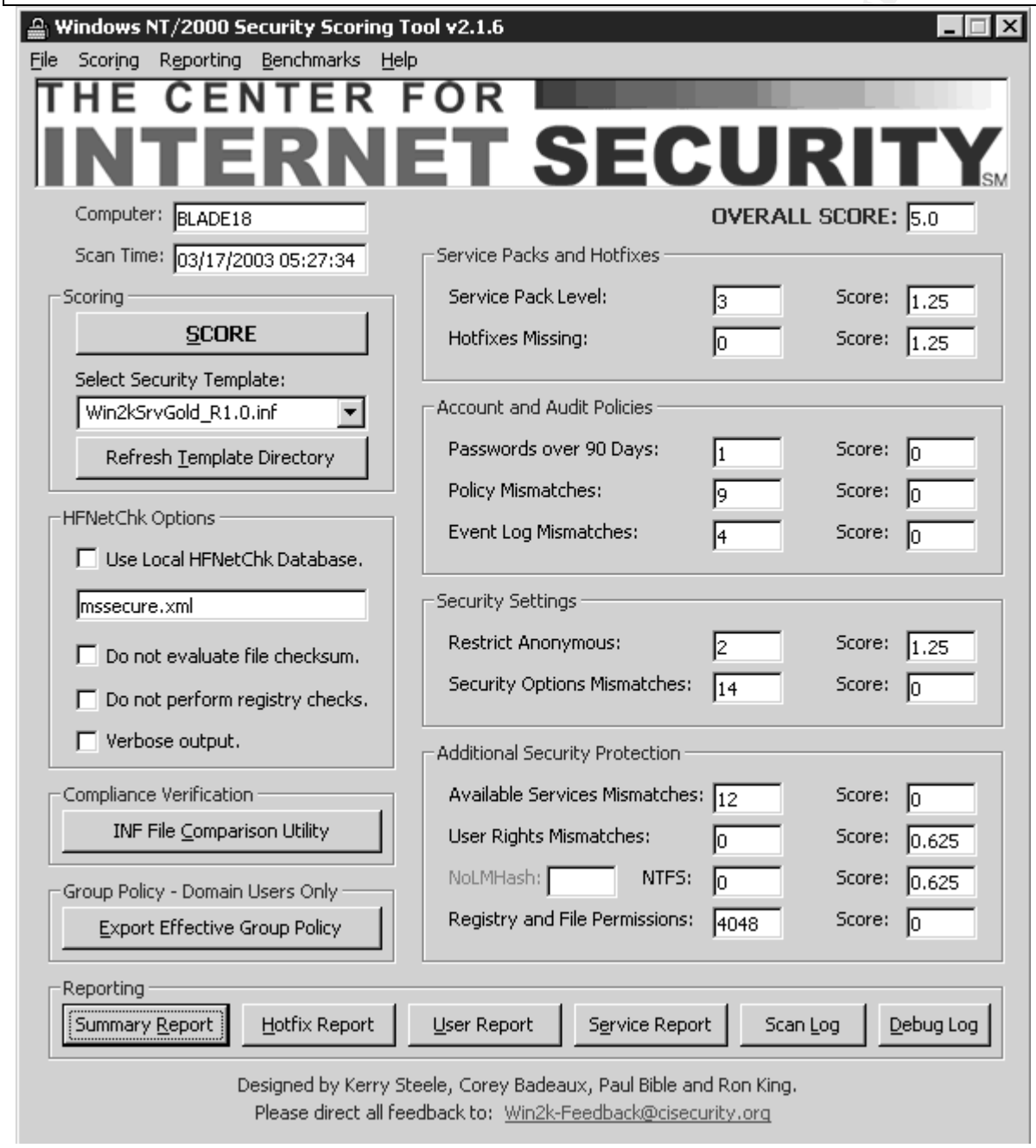
1) Administrator account was renamed and a strong password was assigned.
2) Admin shares were removed.
3) Password Policy settings were secure.
4) Services that were unused or unnecessary were disabled.
5) There were vulnerable ports listed but the IDS agent, BlackICE, will be installed to protect these ports from misuse or attack.
    - There are other methods of closing these ports and preventing access but it may hinder the progress of the project team. To keep these ports accessible BlackICE allows an IP range and a port to be specified, i.e. "192.0.0.0–192.255.255.254: 3389." This example shows how BlackICE will allow only servers within the specified IP range to use Terminal Services, port 3389. (Specifying that this is a TCP port is done in a different location on the BlackICE window.) The IDS agent is installed after this procedure due to the fact that the scans could be blocked and any vulnerabilities that may have been missed could be hidden, which is good for production but I would rather make sure I close everything I can before the IDS agent is installed, thus more layers to the onion…
6) Terminal Services were installed, this service is used by administrators to remote manage the server. The IDS agent, like the example above states, will also cover this.
7) Security patches were up to date.
8) The "Guest" account was renamed, disabled and a strong password was assigned.

Running CIS tool to Score Changes

The CIS tool then was run (Figure 3.3) using both the MS-baseline.inf and the Win2kSrvGold.inf files to get a comparison of the results. The resulting score from both INF files improved from a 2.5 to a 5.0 out of a score of a score of 10.0. The remaining five points difference falls under the heading of "acceptable risk" meaning that the ease of use, application functionality and user

accessibility outweighs the risk of not eliminating the remaining vulnerabilities. Another item that will offset the risk is the addition of an IDS client such as BlackICE (which has evolved into RealSecure Server Sensor by Internet Security Systems to which we are transitioning), which will monitor inbound and outbound traffic coming across the NIC (Network Interface Card) of the server and block, log and send alerts on packets that are seen as malicious.

RealSecure® Server Sensor Server Protection - Protects the underlying operating system preventing attackers from exploiting operating system and application vulnerabilities through log audit analysis, monitoring, locking and the baseline of files for system integrity, firecell blocking for unused ports/services, and automated vulnerability assessment for identification of known vulnerabilities. REF: http://www.iss.net/products_services/enterprise_protection/rsserver/protector_server.php



(Figure 3.3)

Using a Check List to Document Changes

I used a checklist to document the changes made to the server for a few reasons.

- The application project teams can review the changes that may affect the application they are building or implementing.
- In the event the changes made create functionality problems with the server or applications, it is much easier to track down the problem with a list in hand.
- For a record of the changes made to the server. If there are adjustments made to the configuration at a later date the details can be added to the document to create a running record.
- During a security audit the auditing team can review the documented procedures.

As previously mentioned, after I have configured a server and released it to the Development group and they have set up the applications and configured the server for production, I review the settings to see if any adjustments should be made. I am restating this to stress its important.

I have come to the realization that with the implementation of security lockdown configuration procedures must come the full support of management and ISO (Information Security Office). With these areas being in full agreement of the tasks required all development groups must abide by the procedures created to secure all servers prior to production. In the thrusts of progress involving server based application project teams many security related items are overlooked, not always purposely but still overlooked. Communication comes into play, with the use of access request forms, server lockdown request forms, lockdown checklists and final pre-production checklists, all changes are communicated to the appropriate parties.

Conclusion

Out of all the security tools I have come to use, diligence is the one most needed.

There are a growing number of threats reaching every corner of the computer industry creating an environment that nearly ensures that, given time, an unsecured computer will be compromised and there are no servers immune to intrusion. The items covered in this practical, once implemented, have greatly decreased the chances of intrusion by creating a good "Defense in Depth" strategy.

The goal of the methods covered in this practical were to be successful in:

1) Creating a manageable and functional lockdown solution.
2) Meeting the specifications of the corporate policy.
3) Maintaining good business practices and communication with those involved.
4) Creating a strong "Defense in Depth" strategy.

Considering all the variables of locking down a server and many possible changes that could be made, then include the fact that the Windows 2000 server, in an NT 4.0 domain, is required to exchange information with the NT 4.0 servers, it can all seem quite an intimidating task. Even though I had performed many server lockdowns, I found that after attending the SANS Security Essentials course, I was much better equipped with the knowledge needed to complete a more secure server lockdown strategy and apply that knowledge to take the many odd shaped pieces to this security puzzle and place them in a logical order to create a complete picture.

Appendix A

Template Custom Settings

The listings in this Appendix are taken from the Security Configuration and Analysis tool.

Account Policies

Password Policy	24 remembered, minimum age 2 days, maximum age 42 days, minimum length 8 characters, passwords must meet complexity requirements
Account Lockout	Duration 30 minutes, threshold 5 invalid attempts, reset account lockout counter after
Kerberos	Not used in an NT domain.

Local Policies

Audit Policies	Default Settings	Custom Settings
Audit account logon events	Failure	Success, Failure
Audit account management	Success, Failure	Success, Failure
Audit directory service access	Failure	Not defined
Audit logon events	Failure	Failure
Audit object access	No auditing	No auditing
Audit policy change	Success, Failure	Success, Failure
Audit privilege use	Failure	Failure
Audit process tracking	No auditing	No auditing
Audit system events	Success, Failure	No auditing

User Rights Assignment	Default Settings	Custom Settings
Access this computer from the network	Not defined	Administrators, Users
Add workstations to domain	Not defined	Authenticated Users
Back up files and directories	Not defined	Administrators
Bypass traverse checking	Not defined	Users
Change the system time	Not defined	Administrators
Create a pagefile	Not defined	Administrators
Deny access to this computer from the network	Not defined	Guests
Deny logon locally	Not defined	Guests
Force shutdown from a remote system	Not defined	Administrators
Increase quotas	Not defined	Administrators

Increase scheduling priority	Not defined	Administrators
Load and unload device drivers	Not defined	Administrators
Log on locally	Not defined	Administrators
Manage auditing and security log	Not defined	Administrators
Modify firmware environment values	Not defined	Administrators
Profile single process	Not defined	Administrators
Profile system performance	Not defined	Administrators
Remove computer from docking station	Not defined	Administrators
Restore files and directories	Not defined	Administrators
Shut down the system	Not defined	Administrators
Take ownership of files or other objects	Not defined	Administrators

Security Options	Default Settings	Custom Settings
Additional restrictions for anonymous connections	Do not allow enumeration of SAM accounts and shares	No access without explicit anonymous permissions
Allow server operators to schedule tasks (domain controllers only)	Not defined	Disabled
Allow system to be shut down without having to log on	Not defined	Disabled
Automatically log off users when logon time expires	Not defined	Enabled
Clear virtual memory pagefile when system shuts down	Disabled	Enabled
LAN Manager Authentication Level	Send NTLM response only	Send LM & NTLM responses
Message text for users attempting to log on	Not defined	This system is restricted to authorized users for legitimate business purposes and is subject to audit and monitoring. Actual or attempted unauthorized access, use or modifications of computer systems is a violation of federal and state laws. Information obtained on this server is proprietary to

		(Company Name) and its subsidiaries and affiliates. Use of such information is restricted to purposes for which access has been authorized, and all information must be kept confidential in accordance with state and federal privacy laws.
Message title for users attempting to log on	Not defined	Company Name - Access Restricted
Number of previous logons to cache (in case domain controller is not available)	10 logons	2 logons
Rename administrator account	Not defined	Not defined – Should be done manually using a different name at each server
Rename guest account	Not defined	Not defined – Should be done manually using a different name at each server
Restrict CD-ROM access to locally logged-on user only	Disabled	Enabled
Restrict floppy access to locally logged-on user only	Disabled	Enabled
Shut down system immediately if unable to log security audits	Disabled	Disabled
Smart card removal behavior	Lock Workstation	No Action
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled	Enabled
Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation
Unsigned non-driver installation behavior	Silently succeed	Warn but allow installation

Event Log

Settings for Event Logs	Default Setting	Custom Setting
Maximum application log size	5120 kilobytes	10240 kilobytes

Maximum security log size	5120 kilobytes	10240 kilobytes
Maximum system log size	5120 kilobytes	10240 kilobytes
Retention method for application log	Not defined	As needed, separate Syslog server will collect logs to allow logs to be overwritten.
Retention method for security log	Not defined	As needed, separate Syslog server will gather logs to allow logs to be overwritten.
Retention method for system log	As needed	As needed, separate Syslog server will gather logs to allow logs to be overwritten.
Shut down the computer when the security audit log is full	Not defined	Disabled

System Services

Settings for System Services **Custom Setting**

Service Name	Startup	Permission
Alerter	Disabled	Configured
Application Management	Disabled	Configured
Automatic Updates	Disabled	Configured
ClipBook	Disabled	Configured
COM+ Event System	Manual	Configured
Computer Browser	Automatic	Configured
DHCP Client	Automatic	Configured
Distributed File System	Disabled	Configured
Distributed Link Tracking Client	Automatic	Configured
Distributed Link Tracking Server	Disabled	Configured
Distributed Transaction Coordinator	Automatic	Configured
DNS Client	Automatic	Configured
Event Log	Automatic	Configured
Fax Service	Disabled	Configured
File Replication	Disabled	Configured
FTP Publishing Service	Disabled	Configured
IIS Admin Service	Disabled	Configured
Indexing Service	Manual	Configured
Internet Connection Sharing	Disabled	Configured

Intersite Messaging	Disabled	Configured
IPSEC Policy Agent	Disabled	Configured
Kerberos Key Distribution Center	Disabled	Configured
License Logging Service	Disabled	Configured
Logical Disk Manager	Automatic	Configured
Logical Disk Manager Administrative Service	Manual	Configured
Messenger	Disabled	Configured
Net Logon	Automatic	Configured
NetMeeting Remote Desktop Sharing	Disabled	Configured
Network Connections	Manual	Configured
Network DDE	Disabled	Configured
Network DDE DSDM	Disabled	Configured
NT LM Security Support Provider	Disabled	Configured
Performance Logs and Alerts	Manual	Configured
Plug and Play	Automatic	Configured
Print Spooler	Automatic	Configured
Protected Storage	Automatic	Configured
QoS RSVP	Disabled	Configured
Remote Access Auto Connection Manager	Disabled	Configured
Remote Access Connection Manager	Disabled	Configured
Remote Procedure Call (RPC)	Automatic	Configured
Remote Procedure Call (RPC) Locator	Manual	Configured
Remote Registry Service	Automatic	Configured
Removable Storage	Automatic	Configured
Routing and Remote Access	Disabled	Configured
RunAs Service	Disabled	Configured
Security Accounts Manager	Automatic	Configured
Server	Automatic	Configured
Smart Card	Disabled	Configured
Smart Card Helper	Disabled	Configured
smtpsvc	Disabled	Configured
snmp	Disabled	Configured
snmptrap	Disabled	Configured

System Event Notification	Automatic	Configured
Task Scheduler	Automatic	Configured
TCP/IP NetBIOS Helper Service	Automatic	Configured
Telephony	Disabled	Configured
Telnet	Disabled	Configured
Terminal Services	Automatic	Configured
Uninterruptible Power Supply	Disabled	Configured
Utility Manager	Disabled	Configured
w3svc	Disabled	Configured
Windows Installer	Manual	Configured
Windows Management Instrumentation	Automatic	Configured
Windows Management Instrumentation Driver Extensions	Manual	Configured
Workstation	Automatic	Configured

References:

HIPPA: The Health Insurance Portability and Accountability Act of 1996
http://www.cms.gov/hipaa/hipaa2/default.asp or http://www.hipaadvisory.com/

GLBA: Gramm-Leach-Bliley Act of 1999
(http://www.cms.gov/hipaa/hipaa2/default.asp or http://www.hipaadvisory.com/) or
(http://www.senate.gov/~banking/conf/confrpt.htm)

Strong passwords
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/windows_password_tips.asp

GFI LANguard Network Security Scanner http://www.gfi.com/lannetscan/

Center for Internet Security http://www.cisecurity.org/

Security Operations Guide for Windows 2000 Server:
http://www.microsoft.com/brasil/security/content/resources/resources/SOG_download.pdf

Microsoft Baseline Security Analyzer:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/tools/mbsahome.asp

Microsoft Network Security Hotfix Checker:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=34935A76-0B20-4F91-A0DE-BAAF969CED2B

How to Install Multiple Windows Updates or Hotfixes with Only One Reboot:
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q296861

Managing Security Hotfixes
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tips/sechotfx.asp

HFNetChkLT:
http://www.shavlik.com/pHFNetChkLT.aspx

UpdateEXPERT:
http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

Microsoft Solution for Securing Windows 2000 Server:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/Windows/SecWin2k/08patman.asp

Microsoft Baseline Security Analyzer:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/MBSAhome.asp

Step-by-Step Guide to Using the Security Configuration Tool Set
http://www.microsoft.com/windows2000/techinfo/planning/security/secconfsteps.asp

CIS Benchmark Security Scoring Tool
http://www.cisecurity.org/bench_win2000.html

National Security Agency Security Recommendation Guides
http://www.nsa.gov/snac/win2k/download.htm

Apply Predefined Security Templates in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;309689

HOW TO: Apply Predefined Security Templates in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;en-us;309689

Services permissions
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/standard/sys_srv_permissions.asp

Restricting Information Available to Anonymous Logon Users
http://support.microsoft.com/default.aspx?scid=kb;en-us;Q143474

How to Use the RestrictAnonymous Registry Value in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb;EN-US;q246261

RealSecure Server Sensor by Internet Security Systems
http://www.iss.net/products_services/enterprise_protection/rsserver/protector_server.php

HOW TO: Backup, Edit, and Restore the Registry in Windows 2000
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B322755

Book: Todd, Chad. “Hack Proofing Windows 2000 Server”, Syngress Publishing Inc., 2001