Global Information Assurance Certification Paper

Securing Microsoft Small Business Server 2000

Matt Gibson
Oct 12th, 2004

GSEC Practical – Option 1
Version 1.4b

TABLE OF CONTENTS

Summary

By its very nature, Microsoft Small Business Server 2000 is most often employed in small businesses that do not have a large (if any) IT department. This often results in SBS being left in its default configuration, i.e. not secured or hardened in any way.

As all the programs running under the SBS 2000 server have been tweaked to function properly on a single server, following normal hardening guides for individual products can result in a non-functional SBS installation. This paper describes the beginning steps to hardening the core applications of the Small Business Server platform: Windows Server 2000, ISA 2000, Exchange 2000, IIS 5 and Microsoft SQL Server 2000. This paper also provides information on how to effectively manage user passwords, network resources and network topologies while still attempting to provide a secure computing environment.

Introduction to SBS

Microsoft Small Business Server 2000 (SBS) is a network operating system designed for networks between 5 and 50 users. SBS is a version of Windows 2000 Server that has been modified and tightly configured to allow the integration of its network application components: Exchange 2000, Internet Security and Acceleration (ISA) Server 2000 and MS SQL 2000. Microsoft has finely tuned these applications so that they can all run on the same server and still deliver good performance in networks of this size. Small Business Server comes with various 'Wizards' enabling the average "System Administrator" to easily add and configure users and the various server applications. Small Business Server is compressively priced for this market, and is significantly less costly than purchasing each component individually. In addition, the fact that these applications can all be run on one Small Business (network) Server gives small businesses a valuable and effective network operating system platform.

Overview of SBS Applications

Small Business Server is comprised of 5 main applications: Windows 2000 Server, IIS 5.0, ISA Server 2000, Exchange 2000 and Microsoft SQL server 2000. These components have all been tweaked by Microsoft to function on a single server, as normally they would/should all be installed on their own dedicated server.

Windows 2000 Server

As the underlying OS for SBS 2000, Windows 2000 Server provides the user and file level functionality. Windows 2000 Server also includes Internet Information Server (IIS) 5 which provides Web, FTP and News server functionality.

IIS 5

Internet Information Server (IIS) 5 provides Web (Http & Https), FTP and news (NNTP) functionality. Technically, IIS is part of Windows 2000; however for the purposes of this paper, it will be treated as a separate entity.

ISA Server 2000

Internet Security and Acceleration (ISA) Server 2000 is a firewall, proxy and caching suite. While it is an optional install, unless there is an equivalent soft/hardware firewall currently in place, not installing this component will severely degrade the security of your SBS 2000 install. Even if there is a firewall already in place, consider still installing ISA 2000, as it provides both caching and proxy functionality, not to mention the added security provided by having two separate firewalls.

Exchange 2000

Exchange 2000 provides the e-mail functionality for SBS 2000. It integrates with Windows 2000 Server and Active Directory to provide mailboxes for users, and offers the ability to host and access POP3 accounts, provide SMTP routing and host IMAP clients.

MS SQL Server 2000

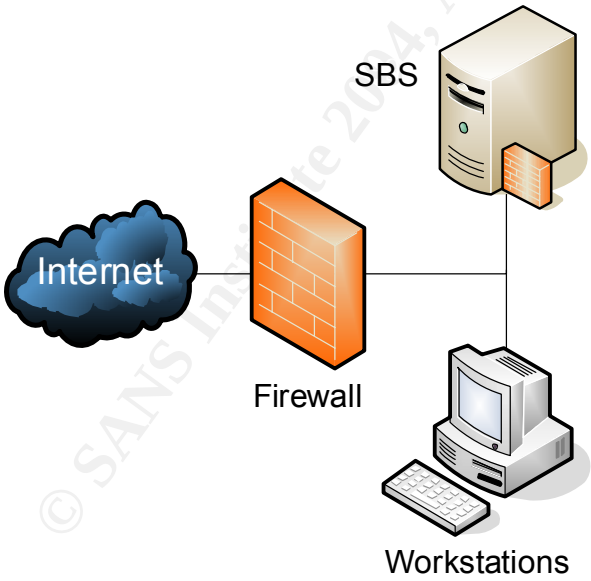
Microsoft SQL Server 2000 is an enterprise grade database server, and provides database capabilities for websites, desktop applications and other uses. Like the rest of the products in SBS 2000, it has been tweaked to run concurrently on the same server as the rest of the SBS 2000 components.

Secure Networking

Network Topology

The SBS server is most often placed into one of three different types of network topologies.

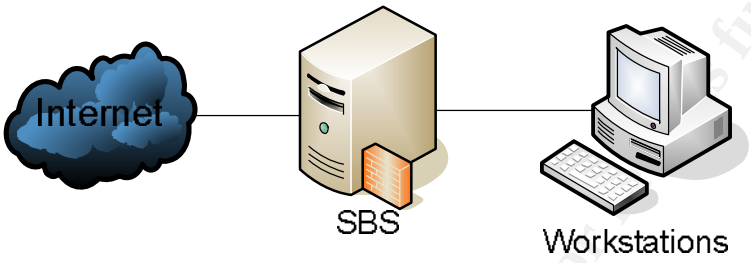
1) **One Adapter**



The single adapter configuration is potentially the least secure of all the SBS network configurations, due to the fact that ISA can only be used for its caching components, and not its firewall or proxy components. Far too often, the firewall (if any) used in this topology is only a basic NAT/PAT router, with no proxying or access control list capabilities. Unless the firewall can provide advanced ACL capabilities, this configuration should not be used. If a hardware firewall must be used (corporate policy), then it should ideally be

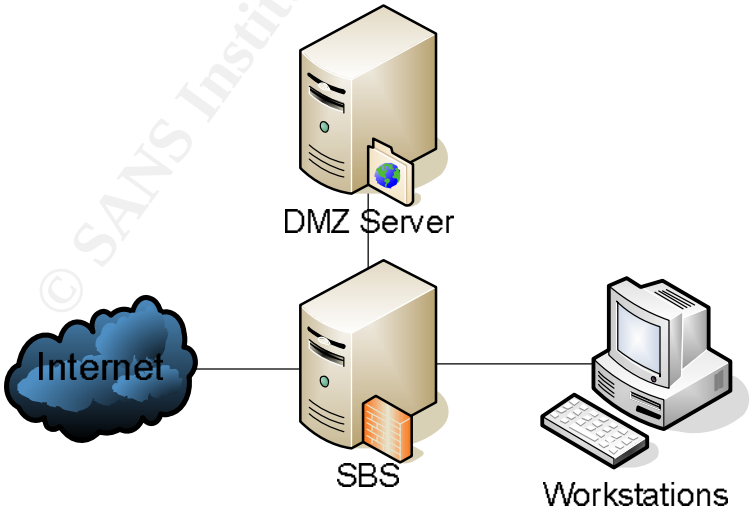
used in conjunction with ISA, not as a replacement for it. This configuration should be avoided at all costs, as it does not provide any advantages over the two NIC configuration, while coming at a higher security risk.

2) Two Adapters



The two adapter configuration is the most commonly used SBS network topology. In this configuration, one NIC on the SBS server connects to the internet, while the other NIC on the SBS server connects to the private workstations. In this topology, ISA acts as a firewall, caching server and proxy server. The rest of this paper assumes that the SBS network is configured in a two adapter configuration, as this is the most secure network configuration available.

3) **3 Adapters**



The three adapter (or DMZ) configuration is the least common of the three SBS topologies. With a three NIC topology, one NIC is connected to the internet, and another is connected to the private workstations, like the two

NIC configuration. Where it differs however, is with the addition of a third NIC, to which publicly available servers are connected. Using routing and remote access, the servers in the DMZ zone are given publicly available IP's.

Wireless Access Points

While the details of securing wireless access points are beyond the scope of this paper, with the booming popularity of using wireless access points for internal network connectivity, there are some simple steps to follow that can help secure your network.

Use Encryption

This cannot be stressed enough. MAC address filtering is NOT sufficient for protecting wireless access. It takes a hacker seconds to figure out which MAC addresses are able to connect to the access point, and then spoof one of those addresses. Encryption is necessary to protect the data in transit between the access point and the wireless clients. Out of the two common types of encryption (WAP and WEP), WAP should be used if it is supported by all the clients. WEP has flaws in the encryption scheme that allows eavesdroppers who can view a sufficient amount of encrypted traffic (1-3GB on average) to deduce the WEP key[1].

Put your access points outside of ISA

While at first this may seem counter-productive, it's not. With your access points outside of ISA, anyone who gains access to your network through the access point is now no better off than a would-be hacker, in that they still have to penetrate the ISA firewall before they can access your internal network itself. Legitimate wireless users only need to VPN into the SBS server to access information on the internal network. The VPN connection also serves to provide an additional layer of encryption in addition to the WEP or WPA encryption used by the access points.

Patching

Patching is the single most important thing you can do to your SBS server. You must keep up to date on Windows 2000 patches, ISA 2000 patches, Exchange 2000 patches, MS SQL 2000 patches, and your workstation patches. Now that Microsoft releases their patches on a pre-set schedule, planning patch rollouts has been somewhat simplified. Be warned that some patches do break things in SBS due to the slightly modified versions of Exchange, ISA and MSSQL that run on SBS. If the update/service pack does not include a critical fix, it's prudent to wait a week before patching and see if any problems are brought up in the Microsoft newsgroups. At the time of writing, SBS 2000 service Pack 1A is the latest SBS service pack, and includes both Windows 2000 SP4 and Exchange 2000 SP3. ISA feature pack 1 should also be installed, and then followed up by

ISA service pack 2. After these service packs have been installed, visit www.windowsupdate.com and download all the updates that show up. Visit http://www.smallbizserver.net/Default.aspx?tabid=93 to stay up to date on the available service packs for SBS 2000.

Patching the workstations is just as important as the server. If a workstation becomes compromised, then a devastating attack might be launched from it against the relatively soft "underbelly" of the SBS server. Using third party patch management software, such as Shavlik's HfNetChk Pro[2] or StBernard's UpdateEXPERT[3] can aid in applying patches and checking patch compliance.

Securing SBS Applications

While the details of securing each of the individual applications to a hardened level are beyond the scope of the paper, what follows are a list of best practices to follow when configuring and maintaining an SBS 2000 server.

Windows 2000 Server

Complex Passwords

Sadly enough, most users' passwords are easy to guess. Their passwords, which were supposed to provide security, end up becoming one of the easiest ways to break into the network. Complex passwords can help prevent passwords from being easy to guess. SBS 2000 allows administrators to set password complexity rules that will not allow a user to create a non-complex password. By default, passwords are deemed complex if they contain 3 or 4 of the following character types:

1. Uppercase characters (ABCD…)
2. Lowercase characters (efgh…)
3. Numeric characters (8390…)
4. Non-alphanumeric characters (#&?^…)

To enforce complex passwords:
1) Open the **Domain Security Policy** MMC applet under **Administrative tools**
2) Expand the **Account Policies** item, and then select the **Password Policies** item
3) On the right hand pane, double click on the **Passwords must meet complexity requirements** item, and ensure that both the **Define this policy setting** is checked and the **Enabled** radio button is selected

Password Aging

Password Aging is a setting that a System Administrator can change to affect how long passwords are valid for before they need to be changed. Passwords can have a minimum age, a maximum age and the last number of passwords to

be remembered. For instance, a setting of 1 day for minimum age, 30 days for maximum age and 5 previous passwords means that a user must change their password at least every 30 days, but not more often than every day, and they can't repeat any of the previous 5 passwords. Most System Administrators understand the need for a maximum password age, but many do not specify a minimum password age. Without a minimum password age, a user is free to change their password as often as they like. This becomes a problem, since they can get around the "remember previous passwords" setting simply by changing their password rapidly. For example, if their password was "grandchild", and they couldn't repeat the last 5 passwords, they only have to quickly change their password to "grandchild1" then "grandchild2" and so on, and then finally back to their original "grandchild". This effectively defeats the "remember previous # passwords" setting. By specifying a minimum password age, most users will no go through the trouble of changing their password 5 days in a row just to go back to their original password.

To configure Password Age and Password History:

1) Open the **Domain Security Policy** MMC applet under **Administrative tools**.
2) Expand the **Account Policies** item, and then select the **Password Policies** item.
3) Suggested values are:
   - Minimum Password age = 4
   - Maximum Password age = 30-60
   - Enforce Password history = 3-10
   - Minimum Password length = 8

Account Lockouts

An account lockout policy locks out an account if a certain number of invalid passwords are attempted over a specified time limit for a user. This prevents brute force authentication attempts on users' passwords. Once an account is locked out, an Administrator must unlock it, or it will unlock after another specific amount of time. Be warned: *the Administrator account can NOT be locked out, and so it is a specific target for brute force authentication attempts. Apply proper security auditing settings to detect brute force attempts on the Administrator's password.*

To configure account lockout policies:

1) Open the **Domain Security Policy** MMC applet under **Administrative tools**
2) Expand the **Account Policies** item, and then select the **Account Lockout Policy** item
3) Suggested Values are

- Account Lockout Duration = 30
- Account lockout threshold = 3
- Reset account lockout counter after = 30

Renaming Administrator Account

The Administrator account is one of the accounts that are created by default on an SBS 2000 server, and so hackers know there's a very good chance the user exists, and since they know the user exists, they now know half of the username/password combination required to login. By changing the Administrator login, hackers no longer "know" half of the information, and now must determine both username AND password before they can wreck havoc. One must take care when changing the Administrator's login name, as it's possible that certain services start using the Administrator's credentials. If you change the login name without updating the credentials of these services, they will fail to start.

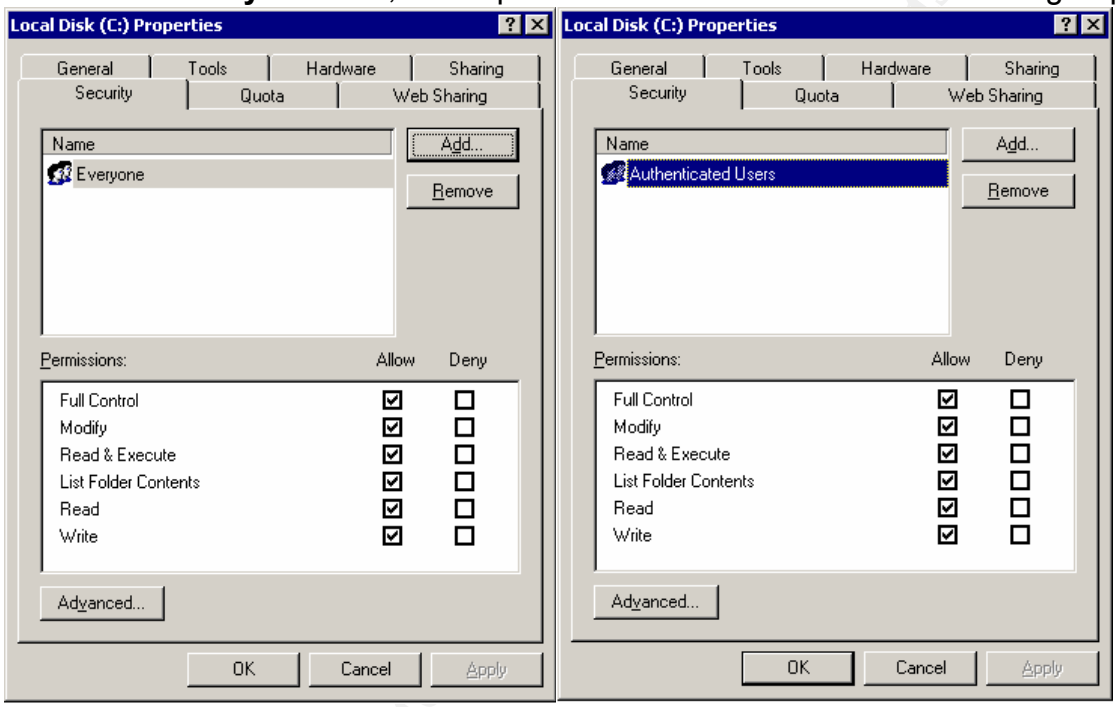
Renaming the Administrator account is *not* a failsafe way of hiding it from malicious users. Each account has a security identifier (SID). The SID for the default Administrator account ends in -500, and that won't change no matter what happens to the account, so don't count on a renamed Administrator account as your only line of defense.

Keeping usernames and e-mail addresses different

Besides knowing that the Administrator user more than likely exists, hackers can also assume with a fairly good degree of certainty that most users' usernames are the same as their e-mail addresses. This again, like the default existence of the Administrator account, allows the hacker to deduce half of the information required to log on as this user without doing any work. By adding information to the users' login name (the number of the month they were born in for example); the hacker no longer "knows" their username.

Replacing the "Everyone" group

By default, the **Everyone** group has full access to all the system drives. This isn't a good thing, since it allows anyone on the inside of the network to access almost anything they want on the server, simply by accessing the administrative shares. Even if you fully trust your internal users (which you never should), remember that the **Guest** user is part of the **Everyone** group. At the least, remove the **Everyone** user, and replace it with the **Authenticated Users** group.



Principle of Least Privilege

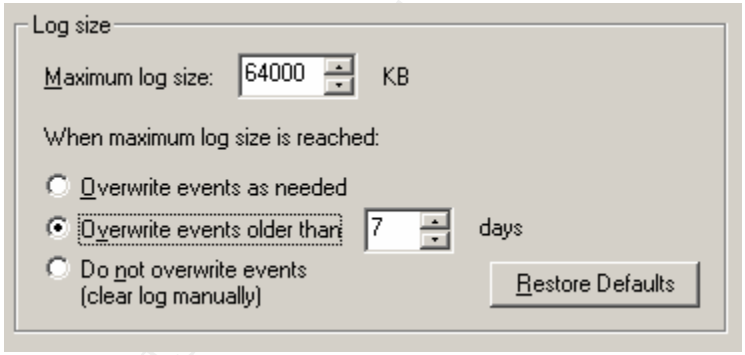
On a moderate sized network, keeping track of who has permission to access what, and who should have what permissions is not an easy job. It's because of this difficulty that some administrators just give everyone full rights on the server. Most often this occurs in small businesses where there is a small number of close employees. "Rob in shipping has been with the company for years" they'll say, "He wouldn't mess around with the accounting files". With this reasoning in place, Rob ends up having full access to everything on the network. Even if Rob turns out to be a perfectly honest guy, perhaps not everything that runs on this computer is. Perhaps Rob's antivirus settings (if he even has an antivirus program) aren't up to date, and he manages to contract a computer virus. This virus is a particularly nasty one, and likes to delete files it finds on attached network drives. This is a large problem, because the company that Rob works for only has one network share, and it houses all the company data in different sub-folders. Instead of Rob only having access to the Shipping folder, he has

access to the Accounting, Manufacturing and Payroll folders. The virus, using Rob's rights, starts to delete files on the network share, and pretty soon there are no files left. Had Rob's network administrator assigned rights using the principle of least privilege, only the contents of the Shipping folder would have been affected by the virus, which is still a problem. This is much less of a problem however than losing the entire contents of the company share.

Changing Event Log Retention Settings

By default, SBS allocates a whopping 512kb to each of the 6 event logs and sets them all to "Overwrite events as needed". This isn't nearly enough space, given how fast some of the logs can generate entries, and since "Overwrite events as needed" is selected, critical events may be overwritten before they're viewed. Each event log should be set to at least 64MB, and perhaps more. You want each event log at a minimum to be able to store a week's worth of logs. It's important to back up old logs and not just delete them or let them be overwritten. If it's determined that the server was compromised two weeks ago, and the oldest security log entry is from last week, then there's a problem. To expand the size of an event log:

1) Open up the event viewer (**Start** -> **Programs** -> **Administrative Tools**)
2) Right click on an event log and select **Properties**
3) Change the **Maximum log size** to 64000 (or higher)
4) Select the **Overwrite events older than** radio button, and set the spinner to **7**



Ensure that 64MB is enough to store 7 days of events. If it's not, then increase the **Maximum log size** value until it is. Saving/Backing up an event log is also a smart idea. To save an event log, right click on an event log, and select **Save Log File as…**. Event logs should be saved at least on the same schedule that they're set to overwrite on.

Security Event Log Settings

The security event log doesn't show much by default. That's because the **audit policy** settings in the **Domain Controller Security Policy** are for all intents and

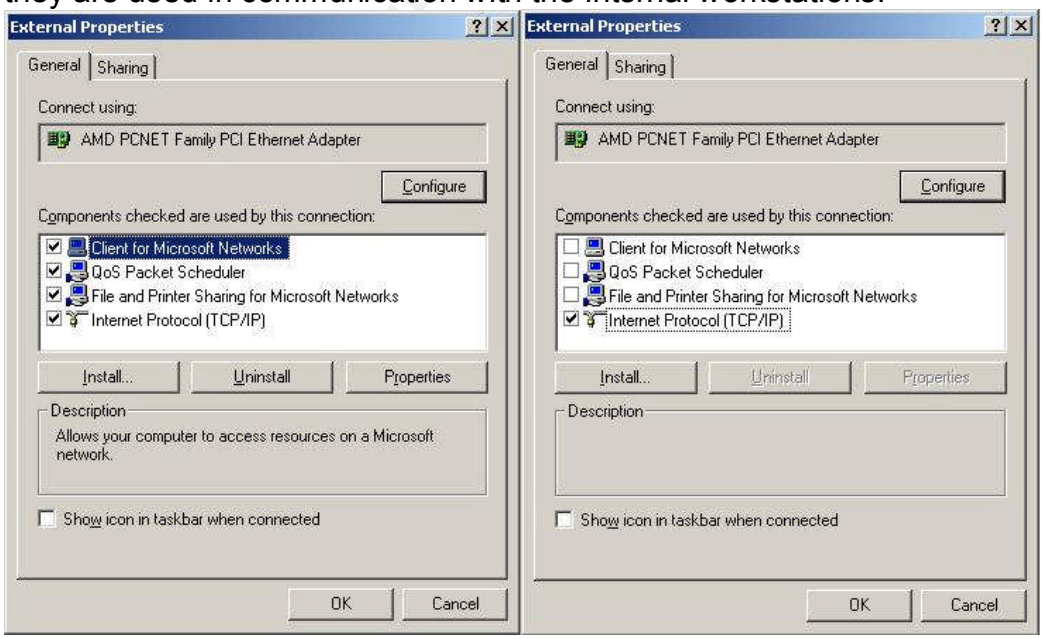
purposes, useless by default. While it might be tempting to enable both success and failure auditing on all the items, realize that too much information can just as easily be as bad as too little. If 20,000 security log entries are generated per day (which isn't as difficult as one might think), there's no way an Administrator is going to be able to keep on top of them all. Rather, selectively enable the audit policies so that the security log is filled with as much useful information as possible, and as little chaff as possible.

Suggested settings:

- Audit account login events = Failure
- Audit account management = Success & Failure
- Audit directory service access = No auditing
- Audit logon events = Failure
- Audit object access = No auditing
- Audit policy change = Success & Failure
- Audit privilege use = Failure
- Audit process tracking = No auditing
- Audit system events = Success & Failure

Removing network bindings from external NIC

By default, SBS enables all the protocols on all of the network adapters. This is highly insecure, and should be changed immediately. Uncheck everything excluding **Internet Protocol (TCP/IP)** from the external adapter. Do not uninstall the protocols, since this would remove them from all network adapters on the server. It is safe to leave all the protocols enabled on the internal adapter, as they are used in communication with the internal workstations.



Security Policies

There are a number of adjustments that can be made under the **Security options** section of the **Local Policies** node of the **Domain Controllers Security Settings** MMC panel.
Recommended Settings:

- Additional restrictions on anonymous connections = Do not allow enumeration of SAM account or shares
- Allow system to be shut down without having to log on = Disable
- Digitally sign client communication (when possible) = Enable
- Do not display last user name in logon screen = Enable
- LAN Manager Authentication Level If all (2000 & XP) = Send NTLMv2 response only \ refuse LM
- Rename Administrator Account = <New Administrator Account name>
- Secure Channel: Digitally encrypt secure channel data (when possible) = Enable
- Secure Channel: Digitally sign secure channel data (when possible) = Enable
- Send unencrypted password to connect to third-party SMB servers = disable
- Shutdown system immediately if unable to log security audits = disable

If your network is solely composed of clients running Windows 2000 and above, you can also make these changes:

- Digitally sign client communication (always) = Enable
- Digitally sign server communication (always) = Enable
- Secure Channel: Digitally encrypt secure channel data (always) = Enable
- Secure Channel: Digitally sign secure channel data (always) = Enable
- Secure Channel: Require secure (Windows 2000 or later) session key = Enable

Do NOT make the above changes if you have any operating system other than Windows 2000, Windows XP or Windows 2003 on your network. These changes will remove the ability of previous operating systems to access file shares and other network resources on your SBS server.

Don't surf from the server

With the growing number of exploits attacking Internet Explorer[4], and the fact that the person who uses the server most likely does so as an Administrator, surfing from the SBS server isn't the smartest thing to do. If a file is required on the server, download it from a workstation and put it on the server via a shared

folder. This way the server is not directly put at risk if a browser vulnerability is exploited. On a similar note, while in some small networks, it's tempting to allow the use of the server as a workstation, it can significantly erode network security if it's allowed.

IIS 5

Securing IIS is one of the most important things you can do on an SBS server. SANS rates IIS 5 as the number 1 vulnerability on a windows system[5], and it's no wonder. Just one look at the number of vulnerabilities that attack IIS 5[6], and it's obvious that this is one of best avenues of attack for hackers. There is one sure fire way to secure IIS, and that's to disable it. If you don't plan to use Outlook Web Access, provide an intranet, or publish a public web page (which isn't a good idea on SBS to begin with), then you're better off uninstalling IIS.

To uninstall IIS:

1) Open **Add/Remove Programs**
2) Click on **Add/Remove Windows Components**
3) Uncheck **IIS** from the list
4) Press **Next**

If you require IIS, and have determined that the risk of operating is worth it, then there are a number of ways that IIS can be secured against malicious users. Before getting into utilities to help secure IIS, there are some changes that can be done within IIS to help increase its security.

Turn off un-needed IIS Services

If you don't require a certain bit of functionality from IIS, then disable it. All too often the Administrative website and the default FTP site are left running in IIS. While ISA will prevent external access to the Administrative website unless a packet filter is specifically created to allow it, internal users have access by default. While no systems administrator wants to have to distrust their own users, it's a sad fact that attacks come from both inside and outside a company. By deleting the Administrative website and the default FTP site (again, unless you require FTP functionality), you significantly reduce your threat profile.

Enable IIS Logging

While enabling logging doesn't reduce the chance of being compromised, it does potentially enable the detection of a successful compromise; and also enables the Administrator to see how the IIS services are being used, and what requests are being sent to them. Being able to see which attacks (if any) are being attempted, and what levels of traffic the server deals with on a daily basis enables a base line of "normal" levels to be defined.

To enable IIS logging:

1) Open up the **Internet Services Manager** (Start -> Administrative tools)
2) Right click on the website for which logging is to be enabled and select **Properties**
3) On the **Web Site** tab, ensure that the **Enable Logging** checkbox is checked, and press the **Properties** button
4) Change the **Log file directory** from the default to point to another partition

IISLockdown

IIS lockdown[7] is a Wizard developed by Microsoft for hardening IIS5 installations. Microsoft has this to say about the wizard:

> IIS Lockdown Wizard functions by turning off unnecessary features, thereby reducing attack surface available to attackers. To provide in-depth defence or multiple layers of protection against attackers, URLScan, with customized templates for each supported server role, has been integrated into the IIS Lockdown Wizard.[8]

To install & configure IIS Lockdown:

1) Download IIS Lockdown from http://www.microsoft.com/technet/security/tools/locktool.mspx
2) Run the downloaded file on the server.
3) When you come to the **Select Server Template** screen, select the "Small Business Server 2000" item, and press **Next**
4) Ensure that the **Install URLScan filter on the server** checkbox is checked and press **Next**
5) The installer will then list the changes that will be applied, and press **Next**
6) When the lockdown has finished, the report of what exactly was changed is available by pressing the **View Report** button
7) Exit the installer

UrlScan

URLScan is installed by IISLockdown, and deserves a section all to its own. URLScan is basically a URL filtering proxy. URLScan intercepts requests to IIS, and parses them apart, then either sends them through to IIS or denies them based on the rules you've provided URLScan with. For example, it's trivial to tell URLScan to deny any requests for any EXE or COM files, or even to disallow the use of the ampersand (&) character. While UrlScan is configured automatically by IISLockdown, it's good to take a look over the configuration file for URLScan, and familiarize yourself with the different options and files that are excluded. The URLScan configuration file is located at

C:\WINNT\system32\inetsrv\urlscan\urlscan.ini. There is one option that isn't enabled by default, and that's the **AlternateServerName** option. Filling in a value here changes how IIS identifies itself. While TCP fingerprinting[9] can still determine the underlying OS, this option will foil simple banner grabbing attempts. Besides, it's just fun to have IIS respond that it's an Amiga 500.

Move the wwwroot folder

The **wwwroot** folder which is the root of the default IIS website folder system is by default installed in *c:\Inetpub\wwwroot*. Having the wwwroot folder on the system partition is a serious security flaw, and it should be moved to a separate partition. Take for example the Double Decode IIS exploit[10]. With this exploit, a hacker could move back up the file system, to the system root (C:\) and then into any directory they wished. There is however, no *known* way to change the partition, and so they would be effectively stuck on a partition with no execute rights, and so have no way of launching an attack on the rest of the system. While the exploit in question has been patched, there are sure to be other exploits that accomplish the same effect. The other consideration for moving the wwwroot folder is a denial of service (DOS) attack. If the wwwroot folder is located on the system partition, and a hacker manages to gain upload access to the website somehow, it's quite possible for the hacker to fill the system partition with files and lock up the server due to low disk space.

ISA Server 2000

Removing Anonymous Access

ISA by default doesn't require a user to provide authentication to browse the web. This enables anonymous users, or programs that cannot authenticate (or do not wish to) to also gain access to the internet. From a security standpoint, this isn't acceptable, as all users who should be accessing the internet should have proper credentials, and if they don't, why don't they? To require users to provide authentication to browse the internet:

1) Open up **ISA Management** (Start -> Programs -> Microsoft ISA Server)
2) In the MMC panel that opens, right click on **<Server name>** (Just under **Servers an Arrays**) and select **Properties**
3) Select the **Outgoing Web Requests** tab
4) Check the Ask unauthenticated users for identification checkbox

Proper Packet Filters

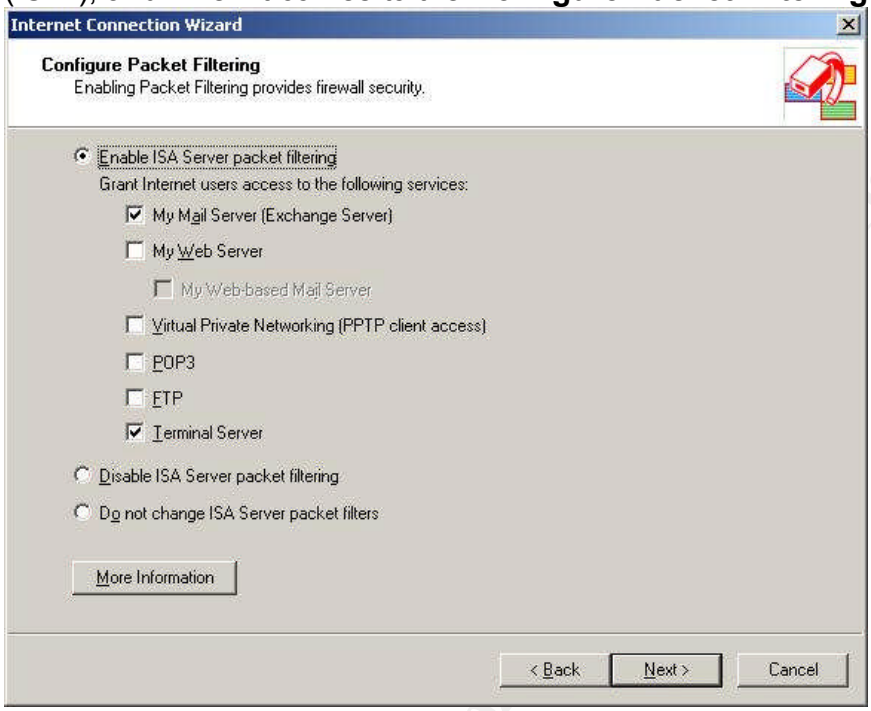
A firewall is useless unless the packet filters are properly configured. The easiest way to configure a firewall is to close all inbound traffic, and see what

breaks. This is somewhat simplified by already knowing what services an SBS server offers, and opening those ports by default.

By default, ISA on SBS 2000 can have the following packet filter rules, depending on what services were selected to be allowed to pass through ISA during the ICW wizard.

Local Port	Remote Port	Protocol	Direction	Use
80	All	TCP	Inbound	HTTP
443	All	TCP	Inbound	HTTPS
113	All	TCP	Inbound	IDENTD
68	67	UDP	Both	DHCP
110	All	TCP	Inbound	POP3
All	110	TCP	Outbound	POP3
25	All	TCP	Inbound	SMTP
All	25	TCP	Outbound	SMTP
3389	All	TCP	Inbound	RDP
All	3389	TCP	Outbound	RDP
All	53	UDP	Send/Receive	DNS

The first step is to see what filters are currently enabled, and how those correspond to your actual needs. Often servers have ports opened for services that are not currently being used. This is a security risk, as only those services needed for operation should be exposed to the internet. The easiest way to configure only the services you require is to run the Internet Connection Wizard (ICW), and when it comes to the **Configure Packet Filtering** page,



only check the boxes that you require. Most servers will only require **My Mail Server (Exchange Server)** and **Terminal Server** to be checked. The **My Mail Server** checkbox will create rules for SMTP traffic to and from the server, while the **Terminal Server** checkbox will create rules for Remote Desktop Protocol (RDP). **My Web Server** is needed if you want outside access to OWA or websites on your SBS server. Creating your own packet filters is possible, and quite necessary if you require third party programs to traverse the ISA firewall. The danger lies in how those packet filters are set up. The biggest danger is packet filters of the following type:

Local Port	Remote Port	Protocol	Direction
All	1433	TCP	Inbound

A simple mistype and this packet filter now allows all inbound packets as long as the source port is 1433. Packet filters should never use the **Both** direction, unless the **Apply this packet filter to** option is set to **Only this remote computer**. Be aware that this is not foolproof, as IP addresses can be spoofed.

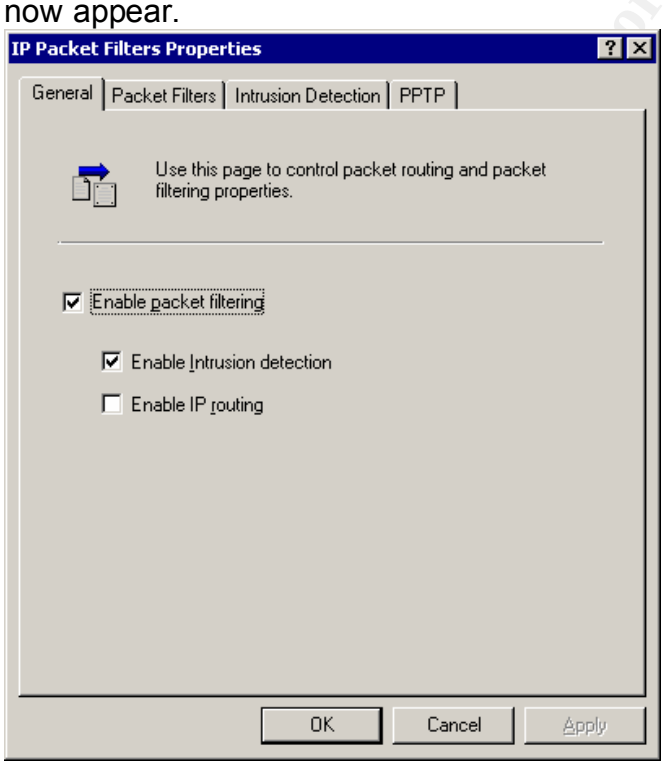
Many Administrators understand the need to filter the traffic entering the network (ingress filtering), but too many fail to filter traffic leaving the firewall (egress

filtering), since by default all traffic is allowed to pass outbound through the firewall. Here is a list of some egress filters that you might want to apply to your ISA server. Basically the rule is, "If that type of traffic shouldn't leave your network, create an egress filter to block it".

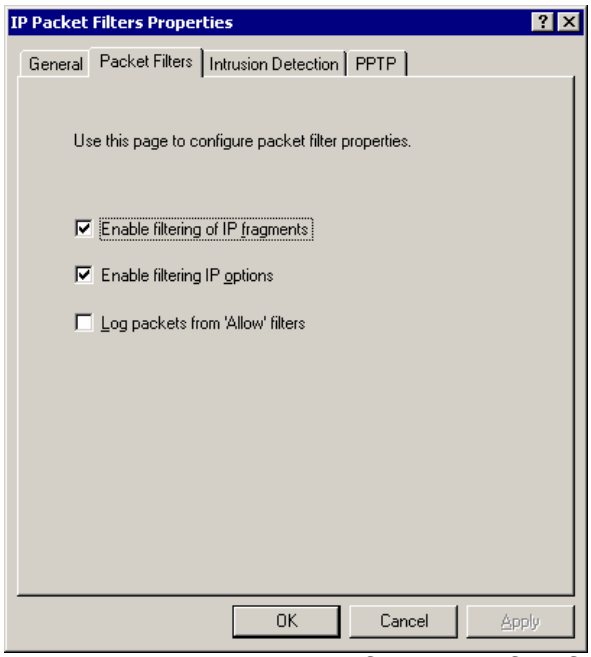
Local Port	Remote Port	Protocol	Direction	Reason
All	NetBIOS	TCP	Outbound	NetBIOS
All	1433-1434	TCP	Outbound	MSSQL
All	5000	UDP	Outbound	Upnp
All	3389	TCP	Outbound	RDP

Intrusion Detection

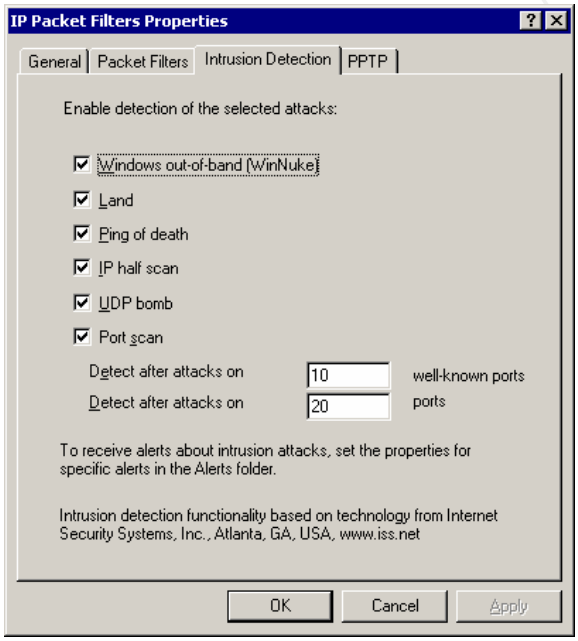
One feature of ISA that isn't enabled by default is that of Intrusion Detection. To access the Intrusion Detection system, expand the ISA item under the Administrator Console, then expand **Servers and Arrays** and then expand **<computer name>**. Now expand **Access Policies** then right click on **IP Packet Filters** and select **Properties**. The **IP Packet Filters Properties** window should now appear.



Ensure that **Enable Intrusion detection** is checked, and click on the **Packet Filters** Tab.



Ensure that both **Enable filtering of IP fragments** and **Enable filtering IP options are selected**. While you *can* select **Log packets from 'Allow' filters**, this will GREATLY increase the size of your packet filter logs, and require a fair bit more CPU power. I personally only use this option when I'm debugging packet filters. Now click on the **Intrusion Detection** tab.



Every checkbox on this tab should be checked, unless you have a very good reason for not doing so. The two values for port scan attacks can be reduced (or increased) to any number you wish, but ISA will generate more alerts with lower values. With the Internet becoming a more and more dangerous place, port scans are a very common thing. As long as ISA is blocking them, they're not

something to be overly worried about. The default values of 10 and 20 are perfectly sufficient in this case.

E-mail Alerts

One nice feature of ISA is that it can be set to notify you if a certain alert occurs. Alerts can be anything from Port scans to Pop3 buffer overflows to Services starting and stopping. These alerts can serve as early warnings to problems (or intrusions), and help you quickly resolve problems.

To configure ISA to alert by e-mail:

1) Open up **ISA Management** (Start -> Programs -> Microsoft ISA Server)
2) Expand the **Monitoring Configuration** node, and click on **Alerts**
3) For each Alert you wish to receive an e-mail for, right click on the alert, and select **Properties**
4) Select the **Actions** tab, and check the **Send e-mail** checkbox.
5) Insert the proper information in the relevant fields, and press **Test** to double check everything.

Cleaning the Local Address Table

By default, the Local Address Table (LAT) where all the IP ranges that are considered to be "safe" are located; contains a number of private IP ranges: 10.X, 192.168.X, 172.16.X, 172.31.X and the subnet of the private network NIC, if it isn't already one of those ranges. By removing all but the range of addresses that are actually in use on the private side of the SBS server, ISA's ability to know which traffic is foreign is increased.

Exchange 2000

Securing against relaying

One of the biggest problems on the internet today (at least with regards to e-mail) is that of SPAM or UBE (Unsolicited Bulk E-mail). One of the tools spammers use to send their torrents of e-mail is a poorly configured mail server. While by default, SBS 2000 doesn't allow relaying from the outside network, it's quite simple to enable relaying by mistake when you're trying to allow outside users to send e-mail (relay) through your SBS server. To properly configure Exchange to allow outside users to send mail through your Exchange server, follow these steps:

1) Open up the Exchange System Manager
2) Expand the **Servers** node, and expand the node below it (the name of your SBS server)
3) Expand the **Protocols** node, and then the **SMTP** node
4) Right click on **Default SMTP Server** and select **Properties**
5) Select the **Access** tab, and press the **Relay** button

6) Ensure that the **Only the list below** radio button is selected, and that the only two entries are the external adapter's IP, and the internal address range
7) Ensure that the **Allow all computers who…** checkbox is checked

Stopping Non-Delivery receipt generation

A Non-Delivery receipt is defined in RFC821[11] as

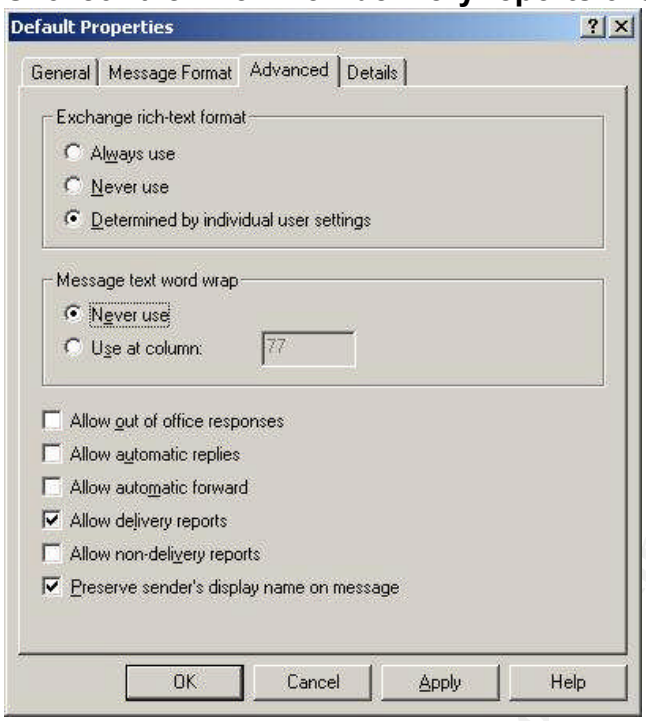
> If a server-SMTP has accepted the task of relaying the mail and later finds that the forward-path is incorrect or that the mail cannot be delivered for whatever reason, then it must construct an "undeliverable mail" notification message and send it to the originator of the undeliverable mail (as indicated by the reverse-path).

In a perfect world, this wouldn't be a problem. If you send an e-mail to rob@test.com, and the server determines after receiving it that there IS no rob@test.com (but it accepted it without complaining), then it would send you an e-mail telling you that it couldn't deliver it after all (and give you a copy of the original e-mail), and it would use your "from" line to determine how it should send you that e-mail. However, since there is (currently) no authentication performed on the "from" line, spammers are free to send spam to a server using your "from" address. When the server attempts to send an NDR, it's going to send the NDR to you, not the spammer, since it was from your e-mail address that the original mail claims to have been sent from. These NDRs also clog up your outbound queues, as spammers will often use non-existent "from" addresses, which means your server repeatedly tries to send the NDR until they finally age out of the queue. Stopping NDR generation does go against RFC821; however this is becoming the norm, not the exception.

To stop Exchange NDR generation:

1) Open up the Exchange System Manager
2) Expand the **Global Settings** node
3) Left click on **Internet Message Formats**
4) Double click on the **Default** entry on the right hand pane
5) Select the **Advanced** tab

6) Uncheck the **Allow non-delivery reports** checkbox



Securing POP3

SBS uses POP3 to enable external users to download their mail from Exchange. However, by default, POP3 sends the username, password and e-mail body in cleartext, meaning that anyone who is capable of monitoring the transmission media (Ethernet, Wireless etc) can glean the username and password (at least) from the traffic. Encrypting POP3 traffic is relatively simple, but involves the use of a SSL certificate. Describing how to acquire and set up an SSL certificate is beyond the scope of this article, but can be accomplished with either a third party certificate authority (Thawte, VeriSign) or through the installation of "Certificate Services" on the SBS Server. Once you've got a certificate installed, follow these steps to require all POP3 communication to be performed over a secure channel.

1) Open up the Exchange **system manager** (Start -> Programs -> Microsoft Exchange)
2) Expand the **Servers** node, then the **<Server name>** node
3) Expand the **Protocols** node, then the **POP3** node
4) Right click on **Default POP3 Virtual Server** and select **Properties**
5) Press the **Certificate** button and Press **Next**
6) Select **Assign an existing certificate** and press **Next**
7) Select the certificate you wish to use from the list and press **Next**
8) Press **Next** then press **Finish**
9) The certificate is now installed, now press the **Communication** button
10) Check the **Require Secure Channel** checkbox
11) Press **Ok**

Require HTTPS to access OWA

Outlook Web Access or OWA is one of the best features in SBS. It provides a web based interface to a user's Exchange mailbox, and enables the user to read and send e-mails through any web browser. By default, OWA is accessible over HTTP and HTTPS. Many users however either forget, or do not understand the need for connecting over a secure (HTTPS) connection, and so will connect over an unencrypted (HTTP) connection, thereby putting their login credentials at risk, since they are being sent un-encrypted. Requiring users to connect over HTTPS removes this security risk. Configuring HTTPS connections does require an SSL certificate, and as with securing POP3, the details of obtaining and installing the certificate are beyond the scope of this paper. Once an SSL certificate has been installed:

1) Open up the **Internet Services Manager** (Start -> Administrative tools)
2) Expand the default website, then right click on the **Exchange** folder
3) Click on the **Directory Security** tab
4) Click on **Edit**, and check the **Require Secure Channel** checkbox.
5) Press **Ok**

MS SQL Server 2000

Microsoft SQL Server 2000 has the infamous position of being exploited by the fastest growing Internet worm of all time[12]. The SANS Top 20 Vulnerabilities list lists it #4 out of the top 10 Windows vulnerabilities[13]. By default, ISA blocks access to ports 1433 and 1434, so it is not possible to access MSSQL from outside the ISA firewall. While this protects MSSQL from external attackers, it is still necessary to harden MSSQL.

SA Authentication / Windows Authentication

For the highest level of security, Windows authentication should be used in place of SA authentication[14]. With Windows authentication, only authorized SBS users can access the MS SQL server, and malicious users have to know both the username and then password, rather than already knowing the SA "username". Failure auditing should also be enabled, so that failed SQL logins are logged, and brute force attacks can be detected.

To configure Windows authentication and failure auditing:

1) Open **Enterprise Manager** (Start -> Programs -> Microsoft SQL Server)
2) Expand down until you reach **(local) Windows NT**
3) Right click on **(local) Windows NT** and select **Properties**
4) Select the **Security** tab and change **Authentication** to **Windows Only**
5) Change **Audit level** to **Failure**

Strong SA password

Even if SA authentication has been disabled, a strong SA password is still a good idea, in case dual authentication is re-enabled at a later date[14].

To change SA password:

1) Open **Enterprise Manager** (Start -> Programs -> Microsoft SQL Server)
2) Expand down until you reach **(local) Windows NT**
3) Expand **Security**
4) Select **Logins**
5) Right click on **sa** in the right hand pane and select **Properties**
6) Change the **Password** value to reflect the new password

The Workstations

Removing Local Admin Rights

Along the same lines as "Principle of Least Privilege" is the fact that many users are running as Administrators on their workstations. Due to poor programming in the past, many programs required administrative rights to run. This is most often no longer the case, and most programs run fine as a normal user. If there are programs that do require administrative rights to run, it is possible to run them under an Administrator account by using the **Run As** command (Right Click -> Run As…). Running needlessly as a user with Administrative rights means that any malware or viruses that infect the system, do so with administrative rights, and can infect the machine more severely than they would if they were running under non-administrative rights.

Using secure Operating Systems

Windows ME, 98 and 95 not considered secure operating systems for a number of reasons. They allow full access to the local machine by pressing **cancel** at the login screen, they do not support NTFS as a local file system, they are nearing the end of their useful support from Microsoft[15], all users run as the equivalent of local administrator, they cannot be controlled from group policy, and they use "Lanmanhash" for network authentication. These flaws, and more all add to the insecurity that is inherent in the 9X series of operating systems from Microsoft. Use at least Windows 2000 workstations, and ideally Windows XP SP2 workstations.

References

1. Fluhrer, Scott, Mantin, Itsik, and Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4", http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf

2. Shavlik Technologies. "Patch Management with Shavlik HFNetChkPro™", http://www.shavlik.com/default.aspx

3. StBernard Software. "UpdateEXPERT", http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

4. Common Vulnerabilities and Exposures. "Search for Internet Explorer 6", Oct 10th 2004, http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=Internet+Explorer+6

5. SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities", Oct 10th 2004, http://www.sans.org/top20/#w1

6. Common Vulnerabilities and Exposures. "Search for IIS 5.0", Oct 10th 2004, http://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=iis+5.0

7. Microsoft Corp. "IIS Lockdown Tool (version 2.1)", http://www.microsoft.com/windows2000/downloads/recommended/iislockdown/default.asp

8. Microsoft Corp. "Microsoft Security: IIS Lockdown Tool", http://www.microsoft.com/technet/security/tools/locktool.mspx

9. Fyodor. "Remote OS Detection via TCP/IP Fingerprinting", http://www.insecure.org/nmap/nmap-fingerprinting-article.html

10. Microsoft Corp. "Microsoft Security Bulletin MS01-026", http://www.microsoft.com/technet/security/bulletin/MS01-026.mspx

11. Jonathan B. Postel. "RFC 821 – Simple Mail Transfer Protocol", http://www.faqs.org/rfcs/rfc821.html

12. Moore, David, Paxson, Vern, Savage, Stefan, Shannon, Colleen, Staniford, Stuart and Weaver, Nicholas. "The Spread of the Sapphire/Slammer Worm", http://www.cs.berkeley.edu/~nweaver/sapphire/

13. SANS Institute. "The Twenty Most Critical Internet Security Vulnerabilities", Oct 10th 2004, http://www.sans.org/top20/#w4

14. Microsoft Corp. “Securing SQL Server 2000 Resource Guide”, http://www.microsoft.com/technet/security/chklist/sql2ksrg.mspx

15. Microsoft Corp. “Windows 98, Windows 98 Second Edition, and Windows Millennium Support Extended”, http://support.microsoft.com/default.aspx?scid=fh;[LN];LifeAn1