# Global Information Assurance Certification Paper

# Centrally Administering Windows XP Security
# A Case Study

**GIAC Certification GSEC Practical**
**Scott C. Zentz**
**Version 1.4b Option 2**

## Abstract

As budget cuts leave fewer IT personal in many companies while security threats continue to increase, it has become more critical then ever to manage security in a timely but efficient manner. In recent years, many vendors have improved their utilities that allow Administrators to centrally manage patches, services, and other aspects required to help meet the ongoing security demand. In this case study the Author will consult with a group of Administrators to gain information about their network, and perform various scans to determine the current state of the network. The Author will determine the target system configuration based on scan results, consultations with the Administrator and users, and SANS TOP 20 most critical internet security vulnerabilities. Recommendations will be made on how the Windows XP desktops can be centrally administered.

After the target configuration is determined, the Author will then use variety of utilities to control essential security configurations. First, the Group Policy Management Console will be used to apply account policies, local policies and enable/disable services on Windows XP desktops. Second, UpdateEXPERT (6.2) will be used to deploy patches and generate reports. Third, NTsyslog will be used to send logs to a centralized log server that will run the Kiwi Syslog Daemon. Finally**,** a Symantec AntiVirus Server will be configured to propagate virus definitions and use the Symantec System Control Center to verify definitions are updated and desktops are clean of viruses and worms. With the utilization of these products, the security aspects of the laptops and desktops can be centrally managed and the network can be up to date and secure.

## Case Study Environment Before

The Author of this paper is a consultant that the Administrators have hired to determine the risk associated with the network and categorize them accordingly. Identified security risks will be prioritized based on the SANS top 20 Most Critical Internet Security Vulnerabilities[1]. Once the areas have been defined the Author can concentrate on what type of centralized utilities will be used to increase the efficiency of deploying updates.

The GIAC Statistics Department is an educational facility that performs various analyses on datasets. These datasets currently do not fall under HIPPA regulations but the Administrators would like to be prepared in the event that they are required to be HIPPA compliant. The physical network in the facility is completely controlled by a separate group called Network Technology Alliance (NTA). The department resides in one building that is split up into 8 suites with common space to each suite. Each suite contains 5 -10 offices, with each office containing 1 - 6 computers. This Department has hosted their own services in house for the past 12 years. They have one Netware 5.1 server that hosts all file and print services. There are a total of about 90 -100 desktops and laptops combined, of which the majority are running Windows XP Pro (SP1). There are also a few desktops still running Windows 2000 Pro (SP4). The server and clients are all running TCP/IP; the server also has IPX installed for a few applications. All clients have the Novell and Microsoft clients installed, as well as File and Printer sharing enabled. The desktops and laptops were configured to obtain an IP address from DHCP but the DHCP server assigns the same address when the lease expired. Before the "consultation", there was no means of centrally managing any security setting, patches, or virus definitions. There was also no means of centrally storing or viewing any logs. If, by chance, any of the desktops were under attack, the Administrators would have no means of knowing unless NTA notified them or a user complained that there was either a problem with their desktop or that the desktop was slow.

The Department already has a site license for Symantec AntiVirus Corporate Edition but not all clients have been updated with the software. This license includes the Server Edition of Symantec AntiVirus but it is not in use. This leaves the management of the clients and their AntiVirus updates decentralized. The current patch management system was also decentralized. When Microsoft released new security patches, the Administrators had to visit each and every desktop to install the patches. Once the patches are installed, there is no means of validating that the patches were applied correctly except by visiting the Windows Update site from each computer. There is also no reporting mechanism that keeps track of which patches were installed on the desktops or laptops at particular times. This information may be crucial to diagnosing problems that may occur after patch installations. Also, there is no centralized log server that is used to collect Security, System, and Application logs. Storing the logs on a central server would give the Administrators a redundant copy of each machine's logs which could be used to detect or prevent an intrusion. Finally, any time the

[1] For more information about SANS Top 20 see http://www.sans.org/top20/

Administrators make a change to their security template, they have to visit each desktop and execute a batch file that applies settings. The Administrators had considered setting up a Windows 2003 server that would host Active Directory services but had not taken any action on the matter. The Author suggested that migrating from a workgroup to an Active Directory Domain would give them the ability to centrally manage all the security settings. The analysis shows that current systems are completely decentralized and settings took days or even weeks to apply critical updates or configuration changes.

Over the last few years, the Administrators of the Windows network have seen how quickly worms and viruses have propagated throughout their network. The amount of time taken to reverse engineer patches has decreased dramatically in the past few years, increasing the importance of applying patches as soon as possible. Below are some of the well known worms with the vulnerability that the worm had exploited and the approximate duration the patch had been available.

Nimda
Microsoft Security Bulletin MS00-078 Released on October 17, 2000[2]
Nimda Detected on September 18, 2001[3]
Duration between patch released and worm detection - 335 Days

SQL Slammer
Microsoft Security Bulletin MS02-39 Released on July 24, 2002[4]
SQL Slammer Detected on January 25, 2003[5]
Duration between patch released and worm detection - 216 Days

Blaster
Microsoft Security Bulletin MS03-026 Released on July 16, 2003[6]
Blaster Detected on August 11, 2003[7]
Duration between patch released and worm detection - 27 Days

SASSER
Microsoft Security Bulletin MS04-011 Released on April 13, 2004[8]
SASSER Detected on April 30, 2004[9]

---

[2] For more information about Microsoft Security Bulletin MS00-078 please see http://www.microsoft.com/technet/security/bulletin/MS00-078.mspx
[3] For more information about the Nimda worm please see http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html
[4] For more information about Microsoft Security Bulletin MS02-39 please see http://www.microsoft.com/technet/security/bulletin/MS02-039.mspx
[5] For more information about the SQL Slammer worm please see http://securityresponce1.symantec.com/sarc/sarc.nsf/html/w32.sqlexp.worm.html
[6] For more information about Microsoft Security Bulletin MS03-026 please see http://www.microsoft.com/technet/security/bulletin/MS03-026.
[7] For more information about Blaster please see http://securityresponse1.symantec.com/sarc/sarc.nsf/html/w32.blaster.worm.removal.tool.html
[8] For more information about Microsoft Security Bulletin MS04-011 please see http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx

Duration between patch released and worm detection - 17 Days

This figure demonstrates that people who wrote these worms were able to reverse engineer the patches much quicker over the past few years. Not being able to respond quickly to security updates is one of the major problems with having decentralized patch management and virus protection.

The Administrators of the network have attempted to take a proactive approach in defeating the malicious code but they have been unsuccessful in applying all of the updates and patches in a timely manner. These untimely update and patch management systems has allowed a few worms and viruses to infect a few of their systems but luckily the malicious code has not yet destroyed any data. This decentralized management has also changed the focus of the Administrators from fixing customer complaints to patching systems, applying needed security settings and containing viruses and worms. The Administrators would like to gain control over this problem so they can minimize the users' downtime, complete users' requests more quickly, and make optimizations to the desktops.

## Case Study Environment During

The Authors goal was to recommend and implement solutions to improve the issues identified with the existing management systems. The Author started out by assessing the existing services and applications by consulting with the Administrators and scanning the network. The output of the scans was analyzed to determine what services may be disabled. Then, the Author had to determine the target system configuration based on the scans, needs of the Administrators and users, and SANS top 20.

The research was performed in order to determine what would best meet the needs of the Administrators with a limited amount of funding. The Author had to view the feature set of the utilities and determine what configuration would best meet the security needs. Throughout each procedure the Administrators were consulted to make sure the proposed solutions were acceptable. Once the target system configuration and utility configuration were defined, the new Windows XP Pro baseline was deployed to the desktops. Each step performed in the process is important to completing the centralized management of the Windows XP client based network. Finally, the Author performed some scans to verify that all machines meet the baseline requirements.

### *Asses existing network services*

[9] For more information about SASSER please see http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html

In order to determine all the services and applications running on the desktops, some scans were performed. First, the author consulted the Administrators to determine what options were available for scanning the network. As always, permission to scan the network must be obtained from the Administrators and anyone else who may be managing the network. After discussing with both of the Administrators, a decision was made that the scans should be performed after hours on and off the local network. Before preparing for the scans, the Author had to alert the Administrators and Networking group NTA that the network will be scanned. The Author supplied information about what IP addresses the scans will originate from, and what IP address range will be scanned. Once the Author receives the ok from all sources, then the scanning could commence.

### *Scan network*

In order to perform a vulnerability assessment, the Author needed to determine what applications were running on all the desktops. The Author had performed a few different scans from the interior network and exterior network. The primary scan utility used was Nmap v3.5[10] . Nmap was used to get a general idea of what services and applications were running on the desktops. The command line option that was used in both interior and exterior scans was nmap –A. The –A option allows nmap to probe for the applications that are running on the open ports. Once the scan was complete the output from Nmap was saved to be used at a later time. Shields Up[11] was used to determine what was being filtered by the border router. The combination of these utilities would reveal enough information to determine what was running and what shouldn't be.

The first set of scans with Nmap was performed on the internal network from two separate desktops to speed up the process. The interior scan of the network will give the Author a true representation of what ports can be mapped. While waiting for the scans to complete the Author used one of the desktops that was not running a firewall and visited GRC's Shields Up website to determine what ports were being blocked by the border router or firewall. Shields Up is a quick, effective, and accurate way to determine what is being blocked/filtered at the border router. Once the scan from Shields Up was complete, a graphical representation of what ports were open, filtered, and closed was displayed. There was also a plain text output available to download from the site. See Figure 1- Shields Up Output for the detailed text output.

The second set of scans using Nmap took place outside the network. The exterior network scan wouldl give the Author a general representation of what a hacker or script kiddy may be able to map with the Nmap utility. In this scan two different desktops were used on different networks in the event that the scan was blocked at some point in the network. This scan was performed to see what hackers would see if they performed a scan. Even though a hacker or script kiddy can only map certain ports

[10] For more information about Nmap (3.5) Please see http://www.insecure.org/nmap
[11] For more information about Shields Up Please see http://grc.com/

from the exterior of the network, it is possible for the hacker or script kiddy to compromise a machine on the network and use it as a proxy for an attack.

### *Analyze output from scanners*

During the analysis of the scans, it was determined that the network was a mixed 2000/XP network in a workgroup. The border router was configured to block ports 1-19, 69, 135, 137-139 and 445 as shown in Figure 1- Shields Up Output.

```
 ---------------------------------------------------------------------------------------
GRC Port Authority Report created on UTC: 2004-04-22 at 12:42:25
Results from scan of ports: 0-1055
5 Ports Open
1026 Ports Closed
  25 Ports Stealth
--------------------
1056 Ports Tested
Ports found to be OPEN were: 111, 427, 1025, 1027, 1038
Ports found to be STEALTH were: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12,
                    13, 14, 15, 16, 17, 18, 19, 69, 135, 137, 138, 139, 445
Other than what is listed above, all ports are CLOSED.
TruStealth: FAILED - NOT all tested ports were STEALTH,
- NO unsolicited packets were received,
- A PING REPLY (ICMP Echo) WAS RECEIVED.
---------------------------------------------------------------------------------------
```

**Figure 1- Shields Up Output**

The scan that was performed outside with Nmap revealed very little information but this does not mean that a hacker could not compromise any of the desktops or laptops. Figure 2 – Nmap Scan from External Network is a sample of what the output from Nmap looked like from of the machines scanned on the network.

```
---------------------------------------------------------------------------
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-07 19:33 EDT
Interesting ports on desktop35.giac.edu (10.0.0.35):
 (The 1647 ports scanned but not shown below are in state: closed)
Port       State       Service
1/tcp      filtered    tcpmux
2/tcp      filtered    compressnet
3/tcp      filtered    compressnet
4/tcp      filtered    unknown
5/tcp      filtered    rje
6/tcp      filtered    unknown
7/tcp      filtered    echo
8/tcp      filtered    unknown
9/tcp      filtered    discard
10/tcp     filtered    unknown
11/tcp     filtered    systat
12/tcp     filtered    unknown
13/tcp     filtered    daytime
```

```
14/tcp    filtered   unknown
15/tcp    filtered   netstat
16/tcp    filtered   unknown
17/tcp    filtered   qotd
18/tcp    filtered   msp
19/tcp    filtered   chargen
21/tcp    filtered   ftp
69/tcp    filtered   tftp
135/tcp   filtered   loc-srv
137/tcp   filtered   netbios-ns
138/tcp   filtered   netbios-dgm
139/tcp   filtered   netbios-ssn
445/tcp   filtered   microsoft-ds
1025/tcp  filtered   NFS-or-IIS
1433/tcp  filtered   ms-sql-s
1434/tcp  filtered   ms-sql-m
5000/tcp  open       UPnP
-------------------------------------------------------------------------------
```

**Figure 2 – Nmap Scan from External Network**

The output from the scan in Figure 3 - Nmap Scan from Interior Network shows that there were a few potential risks that could lead to future compromises. **These ports included 1025/tcp, 1027/tcp and 5000/tcp.** Here is the output from the scan that was performed in the interior of the network.

```
-------------------------------------------------------------------------------
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-07 19:35 EDT
Interesting ports on desktop35.giac.edu (10.0.0.35):
 (The 1647 ports scanned but not shown below are in state: closed)
PORT     STATE    SERVICE      VERSION
21/tcp   filtered ftp
135/tcp  open     msrpc        Microsoft Windows msrpc
139/tcp  open     netbios-ssn
445/tcp  open     microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open     msrpc        Microsoft Windows msrpc
1032/tcp open     msrpc        Microsoft Windows msrpc
5000/tcp open     upnp         Microsoft Windows UPnP
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or
Windows XP, Microsoft Windows XP SP1
-------------------------------------------------------------------------------
```

**Figure 3 - Nmap Scan from Interior Network**

The interior scan of the network revealed that most of the desktops and laptops had a default installation of Windows XP and Windows 2000 with a firewall. This was the case for the majority of the machines, but there were a few machines that were running applications that the Author does not have permission to reveal in this paper.

## *Determine target system configuration*

The target system configuration consists of only the services, applications, and limited file system permissions that are needed for the users and Administrators to perform their day to day jobs. All services, applications, and file system rights will be applied to Active Directory based groups as opposed to individual users to reduce the time spent on applying configurations. Once each group configuration is determined then only the appropriate users will be members of these groups. Please refer to the section GPMC on how to centrally administer the configurations.

Determining the target system configuration was the lengthiest process throughout the entire assessment. In each step, the "Microsoft's Best Practices (Least Privileges)[12]" was used to ensure that everyone has access only to what they need. The following procedure was used to increase the security of the target configuration. First, disable the services based on required functionality. Second, determine proper file system rights based on required functionality. Third, determine what groups will need to be created and what users will need to be added to each group. Fourth, grant the Active Directory groups access only to what they need on the local desktop and Active Directory. Finally, determine what applications are needed for each group. The following sections describe each of these steps in detail.

After each step in the process was complete, the Administrator and a few select users tested to verify that the configuration would give them full functionality in their day to day jobs. Problem determination would be much more difficult if all configurations were applied to the users at once.

## *Disabling services*

With the analysis from the scans and information from the Administrators, it was determined what applications were running and what services could be disabled. Once the disabled services were determined, two Group Policy Object's were created to disable the services. The two Group Policy Objects will be applied to the two different groups that are list in Figure 4 - Disabled Services. More about applying the Group Policy Objects will be explained later in the section Centralized management with the Group Policy Management Console. See Figure 4 - Disabled Services for a list of disabled services.

| Disabled | Group |
|---|---|
| Alerter | (Everyone Group) |
| ASP.NET State Service | (Everyone Group) |
| Automatic Updates | (Everyone Group) |

[12] Microsoft Corporation "Microsoft's Best Practices (Least Privileges)" <http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_seconceptsbp.asp>

| | |
|---|---|
| Background Intelligent Transfer Service | (Everyone Group) |
| Clipbook | (Everyone Group) |
| Network DDE | (Everyone Group) |
| Network DDE DSDM | (Everyone Group) |
| Remote Desktop Session Manager | (Everyone Group) |
| WebClient | (Everyone Group) |
| TCP/IP Netbios Helper | (Everyone Group) |
| System Restore Service | (Everyone Group) |
| Windows Image Acquisition Service | (Everyone Group) |
| SSDP Discovery Device | (Everyone Group) |
| Application Layer Gateway Service | (Everyone Group) |
| Fast User Switching Compatibility | (Everyone Group) |
| Error Reporting Service | (Everyone Group) |
| Fax Service | (Everyone Group) |
| Indexing Service | (Everyone Group) |
| Infrared monitor | (Everyone Group) |
| Internet Connection Sharing | (Everyone Group) |
| IPSEC Policy Agent | (Everyone Group) |
| Machine Debug Manager | (Everyone Group) |
| Messenger | (Everyone Group) |
| NetMeeting Remote Desktop Sharing | (Everyone Group) |
| NT LM Security Support Provider | (Everyone Group) |
| Portable Media Serial Number Service | (Everyone Group) |
| QoS RSVP | (Everyone Group) |
| Remote Access Auto Connection Manager | (Everyone Group) |
| Remote Access Connection Manager | (Everyone Group) |
| Remote Registry Service | (Everyone Group) |
| Routing and Remote Access | (Everyone Group) |
| Run As Service | (Everyone Group) |
| Smart Card | (Everyone Group) |
| Smart Card Helper | (Everyone Group) |
| SSDP Discovery Service | (Everyone Group) |
| Task Scheduler | (Everyone Group) |
| Telephony | (Desktop Group) |
| Telnet | (Everyone Group) |
| Uninterruptible Power Supply | (Everyone Group) |
| Universal Plug and Play | (Everyone Group) |

**Figure 4 - Disabled Services**

The reason that only the “Desktops Group” should have the Telephony service disabled is because there are some mobile users with laptops that use their modems when traveling. This will also eliminate the possibility of any desktops having rogue modem connections into the network. After the Services were disabled on a test machine, a scan was performed to see what would still be seen on the network. The output from the scan revealed there were still a few services accepting connections.

---

```
Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-06-07 16:25 EDT
Interesting ports on desktop35.giac.edu (10.0.0.35): (The 1655 ports scanned but not shown below are in state:
closed)
PORT    STATE    SERVICE      VERSION
21/tcp  filtered ftp
135/tcp open     msrpc        Microsoft Windows msrpc
139/tcp open     netbios-ssn
445/tcp open     microsoft-ds Microsoft Windows XP microsoft-ds
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Profession or Advanced Server, or
Windows XP, Microsoft Windows XP SP1
---------------------------------------------------------------------------------------------
```

**Figure 5 - Nmap Scan After Services Were Disabled**

If Figure 3 - Nmap Scan from Interior Network and Figure 5 - Nmap Scan After Services Were Disabled are compared, the disabled ports can be determined. Although a lot of services had been disabled to close just few ports, a scan from the external network would look like all ports were filtered. Disabling these services is another proactive measure that should be taken in the "Defense in Depth" model.

### *Research proper file system rights*

Applying proper file system rights is critical for functionality of every user but the users should not have more rights then necessary. To determine the file system rights the Author used the "Microsoft's Best Practices (Least Privileges)". Once the file system permissions were determined, a Group Policy Object was created to apply the permissions. This will be explained later in the section Centralized management with the Group Policy Management Console. The first step performed was to remove "Everyone" from the ROOT of all drives, then, add the local and domain admin groups to the ROOT of the drive and set the permissions to full control. The permissions for Domain Users group was given Modify, Read & Execute, List Folder Contents, Read, and Write for the following directories, %System Drive%\Windows\temp, %System Drive%\temp, and %System Drive%\Documents and Settings\all users\. Applying these permissions will strengthen the file system permissions and give the users and Administrators the level of access needed to perform their day to day jobs.

The next step was to compose a list of all the applications that will be used on the desktops and laptops, then determine what application will be assigned to which Active Directory group. This list consisted of the name of the application, directory where the application is installed, group that will have access, and permissions the group will have. The Author consulted with the Administrators and was provided with a list of applications that was categorized in groups. It was determined that there should be a total of 3 groups for the applications. These groups consisted of Everyone, Staff, and Engineers. All the applications will be installed on the baseline and the file system permissions will either allow or deny access to those programs.

| Program | Directory | Group | Permissions |
|---|---|---|---|
| Office XP Pro | c:\program files\officexp | Everyone | Read, Read & Execute, List Folder Contents |
| Adobe reader | c:\program files\acroread | Everyone | Read, Read & Execute, List Folder Contents |
| Mozilla | c:\program files\mozilla | Everyone | Read, Read & Execute, List Folder Contents |
| Winzip | c:\program files\winzip | Everyone | Read, Read & Execute, List Folder Contents |
| AutoCAD | c:\program files\AutoCAD | Engineering | Read, Read & Execute, List Folder Contents |
| AutoCAD | c:\program files\AutoCAD | Staff | DENY Full Control |
| MatheMatica | c:\program files\MatheMatica | Engineering | Read, Read & Execute, List Folder Contents |
| MatheMatica | c:\program files\MatheMatica | Staff | DENY Full Control |
| Matlab | c:\program files\matlab | Engineering | Read, Read & Execute, List Folder Contents |
| Matlab | c:\program files\matlab | Staff | DENY Full Control |
| Visio | c:\program files\visio | Engineering | Read, Read & Execute, List Folder Contents |
| Visio | c:\program files\visio | Staff | DENY Full Control |
| VB Toolkit | c:\program files\toolkit | Staff | Read, Read & Execute, List Folder Contents |
| VB Toolkit | c:\program files\toolkit | Engineering | DENY Full Control |
| Citrix ICA client | c:\program files\Citrix | Staff | Read, Read & Execute, List Folder Contents |
| Norton AntiVirus | c:\program files\NAVNT | Everyone | Read, Read & Execute, List Folder Contents |

**Figure 6 - List of Programs and Permissions**

During the installation of Windows XP, the setup wizard installed some Windows Components. It was determined that these applications will not be used and should be removed from the system. These Windows components are Outlook Express, Netmeeting, Windows Messenger, Windows Media Player, and MSN Explorer. All of these Windows Components have the option to be uninstalled except Netmeeting. These programs can be removed by going to Control Panel -> Add/Remove Programs -> Windows Components, and unchecking each of the components that are not in use. Although the applications were removed from within the Windows Components installer, all the programs files still resided in the same directory they originated in except MSN Explorer. Since the executables and .dll's still resided on the system, the Author recommended setting additional file system permission. Below is a detailed list of the permissions that were applied.

| Prgrams to Remove | Existing Directory After Uninstall | Group | Permissions |
|---|---|---|---|
| Outlook Express | C:\Program Files\Outlook Express | Everyone | DENY Full Control |
| Windows Media Player | C:\Program Files\Windows Media Player | Everyone | DENY Full Control |
| Windows Messenger | C:\Program Files\Messenger | Everyone | DENY Full Control |
| Netmeeting | c:\Program Files\NetMeeting | Everyone | DENY Full Control |

**Figure 7 - Removed Programs and Permissions**

Once the applications in Figure 6 – List of Programs Installed were installed and the settings have been applied, the author executed all the applications to see if there were any errors. In this case there were no errors but if errors would have occurred, most applications will give detailed enough information to determine which specific file a user may require write permissions to.

### *Determine group permissions to Active Directory*

When determining the proper user permissions, it's always safe to use "Microsoft's Best Practices (Least Privileges)". The first thing to determine is what users will need what type of access to the Active Directory (AD). Throughout the rest of this paper the Author will refer to Active Directory as AD. Since none of the users would need permissions to make changes to AD, the permissions from the default group Users would suffice. The permissions on the Users group was set to "Read All Properties", List Contents", and "Read Permissions", which gives the users the proper access needed. The Administrators will need sufficient privileges to manage all aspects of the directory. With this information the Author determined that there will be 2 groups used in delegating permissions to the AD. The groups that were used were Domain Admins and Users. The Administrators' accounts were added to the Domain Admin Group, and all the users accounts were already added to the Users group by default when the accounts were created. The Administrators will only use the Enterprise Administrator account when necessary.

The Author recommended a few other changes to increase the security of the accounts in Active Directory. These recommendations consisted of renaming the Administrator, Guest, and Support accounts to something that looks like a normal account. Then, create new accounts named Administrator, Guest, and Support and Deny Full Control to the top level of the domain. Disable the Support and Guest accounts, then create a 14+ character pass phrase on the fake Administrator account as well as the Guest account and Support account. Even though the Guest account and Support account are disabled it's best to give those accounts a long pass phrase. Finally Delete the Descriptions from the original accounts and copy them to the fake Administrator, Guest, and Support accounts. This is just an added security benefit that follows the defense in depth model[13].

### *Verification / Testing*

After disabling the long list of services, and changing the file system permissions and user rights, the Author wanted to follow up with a small group of users and the Administrators to make sure that the configuration changes were acceptable. For the next week the users and Administrators worked on the desktop as they would have normally worked and found that the system configuration was acceptable with only a few minor changes. These changes cannot be described in this paper because they apply to an application that the Author does not have permission to discuss. At this point the permissions configurations were ready to be applied the entire group. These settings will applied via GPO which will be discussed in the section Centralized Management with the Group Policy Management Console.

[13] Kathy Ivens "Securing the Administrator Account" <http://www.winnetmag.com/Windows/Article/ArticleID/40721/40721.html>. (December 2003)

## *Antivirus infrastructure*

Now the Antivirus Infrastructure will be determined and deployed. When setting up the Antivirus Infrastructure, it is very important to carefully plan how the clients and server should be configured to achieve the best overall protection. It was predetermined that Symantec Antivirus Corporate Edition (8.1) would be used for the antivirus server and clients. The author had to setup the Symantec Antivirus Server and Clients, and the Symantec System Control Center, determine the most suitable way to deploy updates, determine how the server and clients would be configured, and finally, setup the Alert Management System.

The Author used the existing Netware 5.1 server for the Symantec AntiVirus Server[14]. The configurations were performed from a central workstation using a logon that had administrative rights on all the desktops, laptops, and the Netware server. The primary tools that were used were the Symantec Systems Center Console (SSCC) snap-in for Microsoft's Management Console[15] (MMC) and Symantec Antivirus Corporate Edition CD. Throughout the rest of this section the Author will refer to the Symantec System Center Console, Microsoft Management Console and Symantec Antivirus as SSCC, MMC and SAV respectively. The process was started by deploying the SAV server and clients.

## *Deployment of the SAV server and client*

Symantec has done an outstanding job with the utilities that they have developed to deploy the server, clients, and the SSCC. The Symantec Antivirus Corporate Edition CD allows deployment of the SAV server and clients directly from any desktop. First, the SAV server was set up with the latest version (8.1) and Live Update was run to update the virus definitions to the latest available. Once the server set up was complete, it was possible to install the managed clients. The reason that the server had to be installed first was because the clients would be configured as "Managed Clients" in order for the clients to be managed they must be associated to a server. Next, the utility on the CD called "NT Remote Client Install" was used to remotely install the managed version of the SAV client on all of the workstations. Using the utility in Figure 8 - Selecting Clients to be Managed, browse for the SAV server and select the clients and add them, then click finish and the selected clients will begin the installation of the managed clients.

[14] Symantec Corporation "Symantec Antivirus Corporate Edition 8.1" <http://www.symantec.com/region/can/eng/product/sav_ce/>

[15] Microsoft Corporation "Microsoft Management Console Overview White Paper" http://support.microsoft.com/default.aspx?scid=kb;en-us;271950 (June 3, 2003)

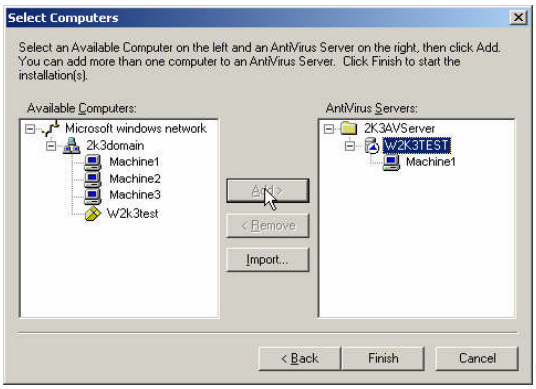



**Figure 8 - Selecting Clients to be Managed**

This only takes a few minutes to install one client but can take much more time depending on how many clients are being deployed. Once the client installation is complete, the computer in the SSCC snap-in like Figure 9 - Managed Client in SSCC will be ready to be configured.

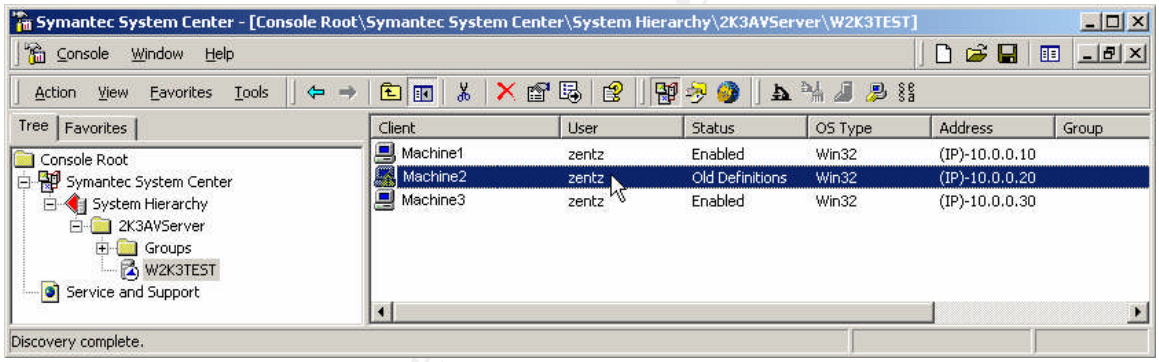



**Figure 9 - Managed Client in SSCC**

## *Symantec System Center Console*

The Symantec System Center Console (SSCC) is a utility that can be used to administer all the managed SAV clients and servers, and can also be used to view the individual event logs and histories. The SSCC has the ability to distribute configurations in three different ways: apply updates to all desktops, apply updates to groups, and apply updates to individual desktops. In order to install this utility, browse the Symantec AntiVirus Corporate Edition CD and click on “setup.exe”. Then a menu will appear with options to install various items. Select Install Antivirus Tools, then select Install Symantec System Center and the installation will begin. A prompt will be displayed to select various components to install and the directory where to install the SSCC. These components are: Alert Management System, Symantec Antivirus Snap-In, Symantec Client Firewall Snap-In, AV Server Rollout Tool, and NT Client Install Tool. All settings are checked except the Symantec Client Firewall Snap-In. Finally the default directory is selected and the installation starts.

The SSCC has 3 options to configure managed clients. These options are to manage all clients, manage groups, and manage selected clients. To apply updates to all machines, right click on the SAV server -> All Tasks -> Symantec Antivirus and there will be a list of options to choose from. To apply updates to a group of machines, a group must first be added. To do so, open the SSCC, browse to the Symantec System Center -> System Hierarchy -> right click on the server, select Unlock Server Group, and supply the SAV Server password. Now, click on groups and in the right pane right click and select new group. Give the group a name that corresponds with the machines that will be added to the group such as desktop or laptops. Then the machines must be added to the group. To add a machine to a group select the SAV server and in the right pane select all the clients that will be added. Now, left click on one of the highlighted clients and drag it to the corresponding group. Then right click on the group you want to change configurations on and select -> All Tasks -> Symantec Antivirus and there will be a list of options to choose from. To apply configurations to select clients, right click on the client(s) and select -> All Tasks -> Symantec Antivirus and there will be a list of options to choose from.

The SSCC provides the ability to view event logs, scan history, and virus history, but are somewhat cumbersome to view in medium to large networks. This is because logs have to be viewed from each client in the SSCC. The remedy for this is problem is the Alert Management Server (AMS), which will be discussed later in this paper. To view the logs, right click on one of the clients, select All Tasks -> Symantec Antivirus -> Logs, then select either Event log, Scan History, or Virus history. There is also an additional option to view Scan Sweep History which can be viewed by a right click on the server and selecting All Tasks -> Symantec Antivirus -> Logs -> Virus Sweep History. The SSCC will now give the Administrators the ability to centralize the administration of the Antivirus Infrastructure.

### *Determine the best way to deploy updates*

Symantec offers five different options to download and deploy updates. These deployment methods range from centralized to decentralized to a mix of both. The first option is for the clients to use their own Live Update services. With this method each individual client contacts Symantec's Live Update site via a service that runs on each client. This service can be configured to update on a daily, weekly, or monthly basis and the specific time of day can be specified or can be set to a random time.

The second option is to setup a SAV server. The SAV server will first run the Live Update service then, deploy the updates to all the managed clients. This option will save some bandwidth because the clients will use the SAV server for their updates instead of each individual client connecting to the Live Update site. The server can be configured to check for updates as often as every 15 minutes or as infrequently as once a month.

The third option is to set up a centralized Live Update server. With this option there are two different ways to deploy updates. In both options the Live Update Server will download the updates. The first option will have the Live Update server send the updates to the SAV server, and then the SAV server will deploy the updates to the clients. In the second option, the Live Update server will deploy the updates to the SAV server and the clients. With these options there is an additional single point of failure such that if the SAV server were unavailable then the clients would not receive their updates.

The fourth option is to manually download the Intelligent Updates and execute them on the server. Intelligent Updates are almost always available a day or two before the Live Update version is available. This keeps the virus definitions on the clients and server a day or two ahead of the Live Update version of the definitions. Here's how to use the Intelligent Updates, first, the updates have to be downloaded from ftp://ftp.symantec.com/public/english_us_canada/antivirus_definitions/norton_antivirus/navup8.exe then executed. As soon as the updates installation finishes, the SAV server automatically deploys the update(s) to all the managed clients. Symantec also offers Intelligent Updates for the clients if the SAV server is inaccessible. These intelligent updates must be installed on each and every machine. These methods take a little more of the Administrator's time but will detect any malicious code a day or two before the Live Update version.

The Final option is to automate the Intelligent Updates on the SAV server with a batch file called cegetter.bat and cescript.txt that Symantec offers from http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002091816510548?Open&src=ent&docid=2002103012571948&nsf=ent-security.nsf&view=9d94c8571a91ba4788256bf3007f62b5&dtype=corp&prod=Symantec%20AntiVirus%20Corporate%20Edition&ver=8.x&osv=&osv_lvl=. This batch/script automatically logs into Symantec's FTP site, downloads the definitions and installs them. This eliminates the burden of the Administrators having to keep track of when the update was released. The batch/script is the most effective approach in saving the Administrator's time and having the most current virus definitions. The script itself does not automatically run so a scheduled task was set to run every 6 hours. As soon as the updates installation finishes, the SAV server automatically deploys the update(s) to all the managed clients. If there are other clients that are off line at that time, they will be updated as they come online.

### *SAV client configuration*

The client configuration will eliminate the ability of a user to change configurations and give the client needed protection. All client configurations will be managed via the SSCC. Here is the list of client configurations; Real time protection will be mandatory on all workstations and servers. The clients were locked from the users so they cannot change the settings. Full Client scans will occur once a week on

Thursdays at 12:00PM. Files will be automatically scanned by the real time protection when they are accessed or modified. The Symantec AV service was password protected so that a user or malicious code would not be able to disable it or uninstall Symantec Antivirus.

### *SAV server configuration*

Every aspect from installation to configuration of the SAV Server can be managed with the SSCC snap-in. The server group was configured to use a password in order to use the SSCC to connect to SAV server and clients. The server will use the same configurations as listed in the "Client Configuration" section with the exception of when the Full Server scan will occur. This scan should not be performed during the time the backup is being performed. A few test scans determined that the scans should take no more then 1-2 hours even if the disk array on the server was at full capacity. The SAV server was configured to perform a full scan every night at 8:00PM.

Next, Symantec's Alert Management System (AMS) was installed and configured on the SAV server. Throughout the remainder of this paper the Author will refer to the Alert Management System as AMS. The AMS is an added feature built in to the Symantec AntiVirus Corporate Edition which can be utilized to alert Administrators. The AMS can be configured by right clicking on the SAV server group then selecting All tasks -> AMS -> configure as shown in Figure 10 - AMS Configuration.

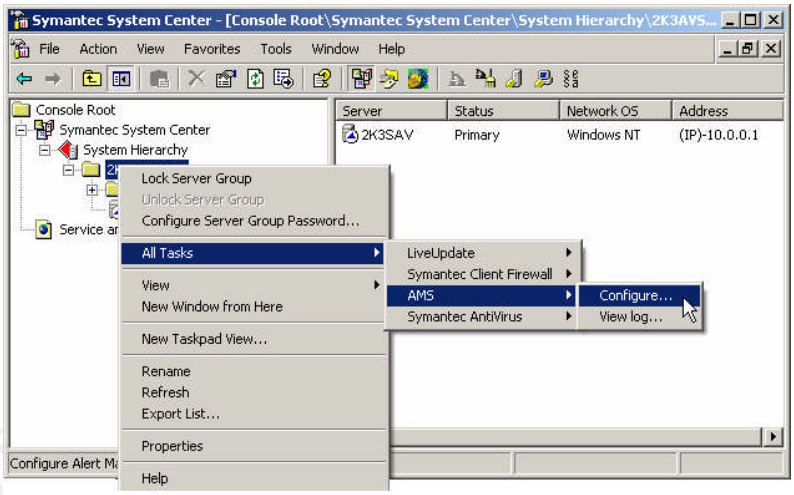



**Figure 10 - AMS Configuration**

The AMS gives the clients and server the ability to send various alerts to specified Windows clients or to all Windows clients. The AMS was configured so when a virus is found it will log the event, email the Administrators, and send an alert to the Administrators' desktop. There are a few other alerts that can be logged as well. These alerts include configuration changes, Default Alert, Symantec Antivirus Startup/Shutdown, Scan Start/Stop, and Virus Definition File Update. If the

Administrators decide to change any settings in the future they also have the ability to broadcast messages, send a page, run a program or send an SNMP trap. The following figure shows the available options for alerts.

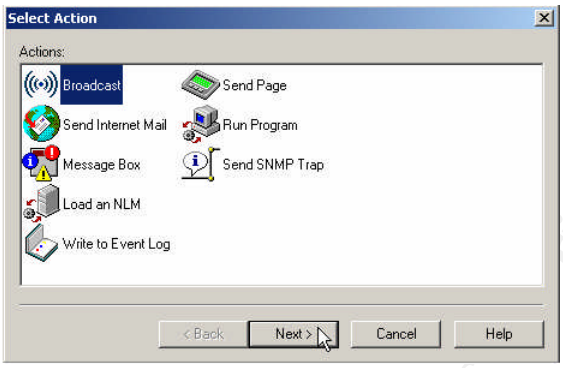



**Figure 11 - Alert Management Options**

Since the Administrators only want to be alerted when a virus is detected it was highly recommended that they at least log everything else to the event log for a potential later use. These final settings completed the deployment and configurations of the Antivirus Infrastructure.

## *Syslog infrastructure*

The Author then planed the Syslog Infrastructure and how it will be deployed. The Syslog infrastructure is a client/server model such that when a client generates a log, a copy of the log is stored locally on the machine and a copy is also sent to a central Syslog server. The Syslog Infrastructure consisted of NTsyslog[16] running on the clients and Kiwi Syslog[17] running on the server. NTsyslog is a free utility that will send Application, System, and Security logs to a centralized Syslog server. Kiwi Syslog is a product that can run as either a service or non service that will collect logs and parse them based on scripts that the user defines. Kiwi Syslog is also a freeware utility but a more configurable version is available to purchase that was used in this infrastructure.

The BSD Syslog protocol (described in RFC 3164)[18] was originally developed for various platforms such as UNIX, Linux Cisco IOS, and other platforms. Kiwi Syslog (service edition) utilizes this protocol for use on Windows NT/2000/XP to view, capture and store logs. The idea behind setting up NTsyslog on the clients and Kiwi Syslog as a central log server is to detect attacks, compromises, and problems with software. If an attack is detected early enough, the Administrator may be able to block communication from an attacker to a desktop. Centralizing the management of Event logs also gives

[16] For more information about NTsyslog please see http://sourceforge.net/projects/NTsyslog/
[17] For more information about Kiwi Syslog please see http://www.kiwisyslog.com/info_syslog.htm
[18] For more information about RFC 3164 Please see http://www.faqs.org/rfcs/rfc3164.html

the Administrators an additional copy of the logs and eliminates the need of viewing the logs at each individual machine. First the Author has to determine the Syslog server configuration, then the client configuration was determined, then the log priority will be determined and finally the Author developed the plan how to deploy the clients.

### *Determine server configuration*

The Kiwi Syslog server will be a machine whose only task is to receive logs. The machine that was used is an unused desktop machine that is a Pentium 3 450 with 256MB SDRAM, 10GB hard drive and a 10/100 Mb Network card. The machine was setup with Windows XP (SP1), Outpost firewall[19], and Kiwi Syslog (service edition). This firewall on the desktop had connections limited to the network that it resides on and will block traffic from all ports except the syslogd port 514. These configurations can be achieved with a firewall and a very limited install. In addition to the central log server, the Administrators have requested that logs are also sent to both Administrators' desktops, providing additional fault tolerance if there is a problem with the log server.

Once Windows XP was installed with all the latest patches (from CD), installation of Kiwi Syslog and Outpost Firewall could begin. A prompt for the auto-configuration wizard will be displayed during the installation of Outpost Firewall (2.1). This wizard will automatically configure firewall rules based on most of the applications that are installed on the machine. Since the Author's preferred configuration of the Syslog server is to only accept connections from machines on the subnet 10.0.0.0/24, the wizard was bypassed to make a custom rule set. Once the installation was complete, the firewall could be configured. To begin the configuration of Outpost, First, open Outpost and there will be list of open ports with their corresponding application. To configure each port, right click on the port and select create rule, a screen with options will appear. Since the preferred setup was to accept incoming connections from syslogd_service.exe and within the subnet 10.0.0.1 - 10.0.0.254, a rule was configured with those properties. Outpost was also configured to block all other inbound and outbound connections.

Outpost stores its logs by default in C:\Program Files\Agnitum\Outpost Firewall\log. This directory will have the following permissions: Local and Domain Admin will have Full Control, and Service will have Read, Extended read, Create Files /Write Data, Create Folders / Append Data, Write, Write Extended and Read Permissions. The reason the permissions were changed on the System account is because even if a hacker finds a weakness in the Syslog Daemon they would not be able to easily delete the logs.

### *Determine client configuration*

[19] For more information about Outpost Firewall please see http://www.agnitum.com/products/outpost/

Before NTsyslog is installed to all the workstations, it must be determined what will be logged, where the logs are stored, and the priority of the logs. Since this is a network of about 90 -100 Windows XP desktops, NTsyslog was setup to log everything and Kiwi Syslog was used to parse out all the information that did not need to be viewed. This is normally not recommended in larger networks but in this case it eliminated the time spent on determining a baseline for the NTsyslog configuration. Logging everything will also reduce the overhead of continually changing the NTsyslog configurations and could potentially catch something out of the ordinary.

### *Log priority*

Log priority is an important aspect of the Syslog Infrastructure. If two logs are received simultaneously and one has to be dropped then the log priority will determine which log is dropped. The reason that the log is dropped is because the Syslog service is based on the transmission protocol UDP which is connectionless based. This means that if packets are dropped or corrupt there is no means for retransmitting the erroneous or lost packets.

When the priority of the logs was setup, security was highest priority, system was second priority, and application was last in priority. Since this may change over time, these priorities can be easily changed with a simple registry entry that can be deployed with a GPO.

### *Client setup*

All Windows clients will have NTsyslog installed, which can be found at the following URL <http://sourceforge.net/projects/NTsyslog/>. NTsyslog can be easily installed, configured, and maintained remotely with a GPO that runs a customizable batch file. The batch file must reside in either the logon or logoff scripts under user configuration. Some prep work needed to be done before deploying NTsyslog. First, the NTsyslog files were extracted from the zip file that was downloaded. Second, the extracted files were placed in a directory to which everyone has read access. Third, the Author wrote a batch file that will check to see if the NTsyslog.exe file already existed in a particular directory. If the NTsyslog executable did not exist, the script copies the files to the local desktop, then installs and configures NTsyslog. The registry file used was created by installing NTsyslog, then exporting the registry key HKEY_LOCAL_DESKTOP\SOFTWARE\SaberNet. The registry file in Figure 13 – NTsyslog Registry Configuration has the default settings for the NTsyslog clients. The settings in the registry file can be customized based on the Administrators needs. For a sample of the batch and registry files please refer to Figure 12 - NTsyslog Batch Install Script and Figure 13 – NTsyslog Registry Configuration.

---

```
REM ### Begin NTsyslog.cmd installation file ###
REM ### Check to see if NTsyslog exists, if exists then bail, if not then install and configure ###
if exist c:\local\NTsyslog\NTsyslog.exe exit
```

```
REM ###Copy Files###
xcopy "\\10.0.0.1\apps\NTsyslog\NTsyslog\*.*" c:\local\NTsyslog\ /y /q /e /v /i
REM ### Configure NTsyslog - These configurations must be in place before NTsyslog starts ###
regedit /s "\\10.0.0.1\apps\NTsyslog\config.reg"
REM ### Install NTsyslog ###
c:
cd \local\NTsyslog\
NTsyslog -install
REM ### Start NTsyslog Service ###
net start NTsyslog
exit
REM ### End NTsyslog.cmd installation file ###
```

---

**Figure 12 - NTsyslog Batch Install Script**

---

```
### Begin NTsyslog registry configuration file ###
Windows Registry Editor Version 5.00

[HKEY_LOCAL_DESKTOP\SOFTWARE\SaberNet]
"Syslog"="10.0.0.20"

[HKEY_LOCAL_DESKTOP\SOFTWARE\SaberNet\Syslog]
"LastRun"=dword:408c1a22

[HKEY_LOCAL_DESKTOP\SOFTWARE\SaberNet\Syslog\Application]
"Information"=dword:00000001
"Information Priority"=dword:00000029
"Warning"=dword:00000001
"Warning Priority"=dword:00000029
"Error"=dword:00000001
"Error Priority"=dword:00000029
"Audit Success"=dword:00000001
"Audit Success Priority"=dword:00000029
"Audit Failure"=dword:00000001
"Audit Failure Priority"=dword:00000029

[HKEY_LOCAL_DESKTOP\SOFTWARE\SaberNet\Syslog\Security]
"Information"=dword:00000001
"Information Priority"=dword:00000029
"Warning"=dword:00000001
"Warning Priority"=dword:00000029
"Error"=dword:00000001
"Error Priority"=dword:00000029
"Audit Success"=dword:00000001
"Audit Success Priority"=dword:00000029
"Audit Failure"=dword:00000001
"Audit Failure Priority"=dword:00000029

[HKEY_LOCAL_DESKTOP\SOFTWARE\SaberNet\Syslog\System]
"Information"=dword:00000001
"Information Priority"=dword:00000029
"Warning"=dword:00000001
"Warning Priority"=dword:00000029
```

```
"Error"=dword:00000001
"Error Priority"=dword:00000029
"Audit Success"=dword:00000001
"Audit Success Priority"=dword:00000029
"Audit Failure"=dword:00000001
"Audit Failure Priority"=dword:00000029
### END NTsyslog registry configuration file ###
--------------------------------------------------------------------------------
```

**Figure 13 – NTsyslog Registry Configuration**

Once the configurations were complete, a GPO was created to deploy NTsyslog. The Syslog Infrastructure was now ready for deployment.

## *Centralized management with the Group Policy Management Console*

The next step in the process was to setup the Group Policy Management Console[20] (GPMC). The Group Policy Management Console is a utility that has the ability to control all group policy related tasks.[21] Group Policies Objects can only be applied to Windows 2000/XP/2003 in Active Directory. Throughout the remainder of this paper the Group Policy Management Console and Group Policy Object's will be referred to as GPMC and GPO's respectively. The GPMC gives the Administrators the ability to centrally administer most settings in Windows 2000/XP/2003. Here is a list of the Computer and User configurations that can be centrally administered:
Computer Configurations: Software Installations, Startup and Shutdown scripts, Account Policies, Local Policies, Event Logs, Restricted groups, System Services, Registry, File System, Public Key Policies, Software Restriction Policies, and IP Security Policies.
User Configurations: Software Installation, Remote Installation Services, Logon and Logoff Scripts, Public Key Policies, Software Restriction Policies, Folder Redirection, and Internet Explorer Maintenance. In addition to all the control over configurations, there is also a reporting tool that will allow an administrator to export the current settings into an HTML or XML based file. These files can be used to keep records of all the changes to the GPO's over time. Before the desktop settings could be managed with the GPMC each desktop that had to be managed must be added to the Domain. Throughout this section of the paper instructions will be given on what the Author had performed and why.

First, some GPO's were created and named corresponding with the settings that were applied in the GPO. For instance, the file system GPO for staff was labeled File System (Staff). The author created a GPO for each task and labeled it accordingly. This was done to limit the amount of confusion over what GPO applied a particular setting or settings. This method can also be useful in diagnosing problems with GPO's by

[20] The Group Policy Management Console can be found at the following URL http://www.microsoft.com/downloads/details.aspx?FamilyID=c355b04f-50ce-42c7-a401-30be1ef647ea&DisplayLang=en

[21] For more information about Administration with the Group Policy Management Console please see http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx

disabling them one by one. The Author will now give instructions in the following sections on how to centrally administer disabling services, file system permission, NTsyslog deployment, and finally, security settings.

In order to disable services described in the “Disabling services” section, two GPO's were created and applied to specific AD groups. The AD groups that will be used are Everyone and Desktops. In order for a GPO to be applied to a machine the user must have read permissions to the GPO. If the read permissions are removed then the GPO will not be applied to the machine. This will give the Administrators the ability to control who will receive the GPO without creating multiple OU's.

Here are the steps the Author performed in order to disable the services based on groups. First, the two GPO's were created and labeled Disabled Services (Everyone), and Disabled Services (Desktop). Second, right click on the GPO Disabled Services (Everyone) and Click edit, now browse to Computer Configuration -> Windows Settings -> Security Settings -> System Services. To disable a service right click on the service, select properties, and select disable. This had to be performed on each and every service that was disabled. Now, the Author referenced the list of disabled services that was created in “Figure 4 - Disabled Services” and applied the disabled services to the corresponding GPO's (Disabled Services (Desktop) and Disabled Services (Everyone)). Then the Active Directory Users and Computers tool was used to create a group called Desktops. A list of all the desktops on the network is compiled and added to the group Desktops. Using the GPMC, a link for the Disabled Services (Everyone) GPO and the Disabled Services (Desktop) GPO were created at the top level of the Domain. When the GPO is created, by default the Authenticated Users group is delegated the following permissions: List Contents, Read All Properties, Read Permissions, and Apply Group Policy. These delegation permissions will suffice for the Disabled Services (Everyone) GPO but not for the Disabled Services (Desktop) GPO. The Disabled Services (Desktop) GPO was delegated to only to the Desktop Group with the following permissions: List Contents, Read All Properties, Read Permissions, and Apply Group Policy. The Authenticated Users Group is Removed from delegation. Once this process is complete, verify that the settings have been applied to a machine that is in the Domain.

Now the file system permission GPO will be created and configured. The File System permissions that were described in “Research proper file system rights” were applied with one GPO. Here are the steps the Author performed in order to apply the File System permissions. First, open the Active directory Users and Computers utility and create two groups named Staff and Engineers. These groups were created in the Groups OU, and the proper users were added to the groups. Second, the GPMC was opened and a GPO was created and labeled File System Permissions. Third, right click on the GPO and click edit, and browse to Computer Configuration -> Windows Settings -> Security Settings -> File system. Fourth, right click in the right pane and select add file, browse to one of the directories that permissions will be applied to and click ok. A security tab will popup that has that can be used to change the permission. Once all the file system permissions are applied according to Figure 6 - List of Programs and

Permissions then a link to the File System GPO is created at the top level of the Domain. Once the file system permissions were applied, the NTSYSLOG GPO will be configured.

The NTsyslog GPO was created to automatically deploy the NTsyslog client to all the XP desktops without the Administrators' or Author's intervention with the Staff or Engineers. This was relatively easy because the configuration of the client was already been determined and the scripts were ready. First, using the GPMC the GPO is created and labeled NTsyslog. Second, right Click on the GPO and Click edit, and browse to User Configuration -> Windows Settings -> Scripts. Right click on the Logon script, and click properties. The properties for the logon script now appears, click on the show files button and exporer will opend to the directory where the scripts reside in the GPO. Copy the NTsyslogInstall.cmd file and place it in the folder that is shown. Close explorer and click on Add, then browse and select the NTsyslogInstall.cmd file and click Open then ok. Make sure that the batch file points to a shared directory located on the machine that was specified in the NTsyslog section. Also double check the permissions on the folder where NTsyslog resides. Now make a link to the NTsyslog GPO at the top level of the Domain. Once the NTsyslog GPO is complete, the file Default Domain GPO would be edited to meet the needs of the GIAC Statistics Department.

The Default Domain Policy is a GPO that was created and applied by default when AD was setup. Most of the settings in the Default Domain Policy already meet the security requirements of the network and the SANS TOP 20. The Author made some additional changes to the Default Domain Policy that will further strengthen the security of the Domain. Figure 14 - Group Policy Settings is a list of the settings that were modified in the Default Domain Policy.

| **Account Policies** | **Effective Policy** |
|---|---|
| Minimum password length | 8 |
| | |
| **Audit Policy** | **Effective Policy** |
| Audit Account Logon events | Success/failure |
| Audit Logon events | Success/failure |
| Audit policy change | Success/failure |
| Audit privilege use | Success/failure |
| | |
| **User Right Assignments** | **Effective Policy** |
| Access this computer from the network | Administrators Group and Administrator |
| Add workstation to domain | Administrators Group and Administrator |
| Back up files and directories | Administrators Group, Administrator and Backup Operators |
| Change system time | Administrators Group and Administrator |
| Deny Access to this computer from the network | Guests Group, Guest and Anonymous logon |
| Deny logon as a batch job | Guests Group, Guest and Anonymous logon |
| Deny logon as a service | Guests Group, Guest and Anonymous logon |

| | |
|---|---|
| Deny logon locally | Guests Group, Guest and Anonymous logon |
| Load and unload drivers | Administrators Group and Administrator |
| Manage auditing and security log | Administrators Group and Administrator |
| | |
| **Security Options** | **Effective Policy** |
| Accounts: Rename Guest account | Dmarks |
| Audit the access of global system objects | Enabled |
| Domain member: Digitally encrypt or sign secure channel data (always) | Enabled |
| Domain Member: Maximum machine account password age = 90 days | |
| Domain Member: Require strong (Windows 2000 or later) session key | Enabled |
| Interactive logon: Number of previous logons to cache (in case domain controller is not available) | 8 |
| Interactive logon: Prompt user to change password before expiration | 14 days |
| Network access: Do not allow enumeration of SAM accounts | Enabled |
| Network access: Do not allow enumeration of SAM accounts and shares | Enabled |
| Network access: Let everyone permissions apply to anonymous users | Disabled |
| Network access: Named Pipes that can be accessed anonymously | Disabled |
| Network access: Shares that can be accessed anonymously | Disabled |
| Network security: LAN Manger authentication level | Send NTLMv2 response only\refuse LM & NTLM |
| Recovery Console: Allow automatic administrative logon | Disabled |
| | |
| **Event Log** | **Effective Policy** |
| Prevent local guests group from accessing application log | Enabled |
| Prevent local guests group from accessing security log | Enabled |
| Prevent local guests group from accessing system log | Enabled |
| | |

**Figure 14 - Group Policy Settings**

Now that all the GPO's had been applied, the Author then configured UpdateEXPERT.

## *UpdateEXPERT patch deployment*

UpdateEXPERT 6.2 (UE) is a very powerful and flexible utility that can be utilized as a central point to research, manage, and report on patches. Throughout the remainder of the paper the Author will refer to UpdateEXPERT as UE. This utility can deploy patches for all of the Windows operating systems, Internet Explorer, Exchange servers, SQL servers, IIS servers, ISA servers, XML web services and will even update all the Office products. The desktops can be administered with or without Agents.

UE has the flexibility to manage a Microsoft Workgroup, Domain, Active Directory, a selected group or a filtered profile. The UE console can remotely patch systems with either pre-configured patches or a custom fix. There are also reporting tools that allow the Administrators to generate conformance, error, deployment, error detection, and validation reports. The UE console also has a built-in research pane which generates a list of all supported patches for all platforms and supported programs. In addition to the research pane, there is a built-in browser where selecting a particular patch opens a particular KB or Q article in Microsoft's Knowledge Base. Throughout this section of the paper, instructions will be given on what the Author had performed and why.

### *General Setup*

In this particular scenario the workgroup was fewer than 100 workstations. It was decided that patches will be deployed to groups of desktops at a time. The Author will setup several groups based on office locations in their corresponding suites. First, UE must be installed to a workstation on the network. After the installation is complete, UE is executed and the operator is prompted for a user name, password and domain. After the credentials were complete, UE continued by enumerating the specified Domain (2k3Domain). Before the unmanaged clients were converted to managed clients, the console needed to be updated with the latest database. This was done to ensure that the console had the latest list of patches. To update the console database, click on Help in the application menu then, click on Update Database Now. Once the database was updated, the console restarted. Now that the UE console was updated, unmanaged clients could be converted to managed clients. Initially all the workstations were marked as unmanaged as seen in Figure 15 - UE Unmanaged Client.

**Figure 15 - UE Unmanaged Client**

To change the client to a managed client, right click on the particular client or the Domain and select Manage Selected. Now the clients can be queried. To do this, right click on the client or Domain and select query. Once the query has completed, a list of patches for each machine is compiled. To view the list of patches that are installed and not installed on the machine, click on the machine and view the list. Now that all the desktops were queried, they could now be added to groups. Since there are about 10-15 desktops per room the groups were added based on suite number. When a patch or

several patches are available, the Administrators can deploy the patches then notify the users in the suite to reboot their desktops.

### *Adding clients to the console*

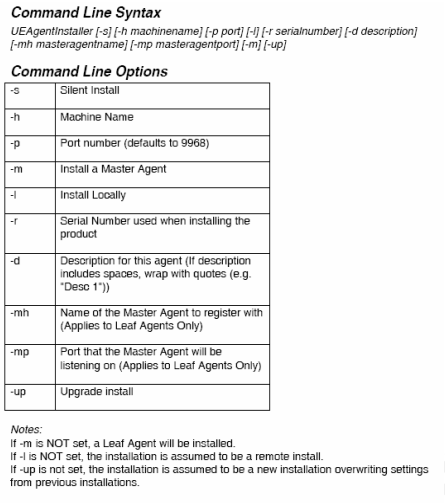
When adding clients to the UE console, there are a few different options that must be considered. The first option is to add a Workgroup, Domain or Active Directory. The second option is to add each desktop by IP address. The third option is to add the clients as Leaf Agents. When the Author consulted with the Administrators, it was determined that all of their desktops obtained their IP from DHCP but obtained the same address every time a lease expired.

In this scenario, it was determined that the desktops and laptops will have different configurations. The desktops will be added by IP address and managed as Leaf Agents. The laptops will be added by their NETBIOS name, and then managed as Leaf Agents. The reason that the Author chose to use Leaf Agents is because the Leaf Agent will use its own encryption algorithm to establish communications with the console. If Leaf Agents were not used, then each client would rely on the following services for communications: RPC, Remote Registry, Netlogon, and Server[22]. To start this process, the IP addresses of each desktop will have to be collected. Then all desktops are added and then moved to the appropriate group by suite number. Then all the laptops were added and placed in their appropriate group. Next, the Leaf Agent would be installed from the UE console to each and every desktop and laptop. This is some what a lengthy process but adds significant value to the security infrastructure and will ultimately save time.

### *Master and Leaf Agent installation*

The Master and Leaf agents can be installed by various methods. The UE console has a built-in utility that can remotely install leaf agents to managed clients. The only caveat with this utility is that only one leaf agent may be installed at a time. Installing the agent from the console is the Author's method of choice even though it's a little cumbersome to install the agent to 90 - 100 desktops. The Author prefers using the console to install the agent because the console verifies each file as it's transmitted across the wire, then verifies the installation completed successfully. The UE agent installer has built in command line options that can be used to install the clients via GPO. Figure 16 - Agent Command Line Options refers to UE's deployment guide page 18 that has the entire list of command line options and the associated syntax.

[22] St.Bernard Software "What ports and services does UpdateEXPERT use?" <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/Installation/UE0270.htm >. (No Date)



***Command Line Syntax***

*UEAgentInstaller [-s] [-h machinename] [-p port] [-l] [-r serialnumber] [-d description] [-mh masteragentname] [-mp masteragentport] [-m] [-up]*

***Command Line Options***

| | |
|---|---|
| -s | Silent Install |
| -h | Machine Name |
| -p | Port number (defaults to 9968) |
| -m | Install a Master Agent |
| -l | Install Locally |
| -r | Serial Number used when installing the product |
| -d | Description for this agent (If description includes spaces, wrap with quotes (e.g. "Desc 1")) |
| -mh | Name of the Master Agent to register with (Applies to Leaf Agents Only) |
| -mp | Port that the Master Agent will be listening on (Applies to Leaf Agents Only) |
| -up | Upgrade install |

*Notes:*
If -m is NOT set, a Leaf Agent will be installed.
If -l is NOT set, the installation is assumed to be a remote install.
If -up is not set, the installation is assumed to be a new installation overwriting settings from previous installations.

**Figure 16 - Agent Command Line Options**

### *Master and Leaf Agent encryption*

The Master and Leaf agent system is a system used to encrypt all communications between the Master and Leaf agent. This can be used to send updates to remote desktops in an encrypted channel. The information below gives detailed information about what encryption is used during each step in establishing a connection.

"For Master Agent to Leaf Agent communications, we use a key exchange algorithm based on 512-bit **El Gamal** PKI to establish a session key and to authenticate both endpoints, and then we use 56-bit **Blowfish** encryption in CBC mode for packet traffic. Whenever communication is established between the Master Agent and Leaf Agent, a new key pair is negotiated and exchanged for that session."[23]

Without the agents, each client would have to have the following services running in order to receive updates: Server, Workstation, RPC, Scheduler, Service Control Manager and Remote Registry Service. [24]

### *Agent settings*

The Leaf agent runs as the Local System account on each local desktop. The leaf agent by default uses port 9968 but if needed the ports may be changed to any other unused port. There are three different options that allow the agents to be configured. These options are to use either Global agents, Individual agents, or a mix of both. The Global agent settings are used as templates for all of the agent settings. To view the Global Agent settings please refer to Figure 17 - Global Agent Settings.

---

23 St. Bernard Software "What kind of encryption does UpdateEXPERT use" <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/DMZ/UE0072.htm>
24 St. Bernard Software - Pg 4 in UpdateEXPERT Deployment Guide <http://www.stbernard.com/products/docs/ue_deployguide.pdf>

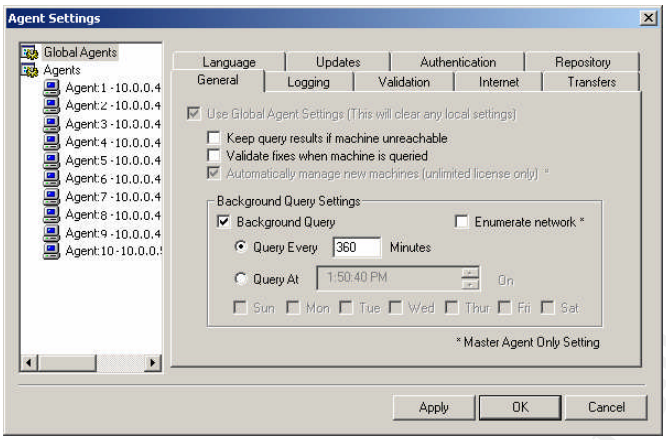



**Figure 17 - Global Agent Settings**

All Leaf agents use the Global Agents template by default. This reduces the amount of time an administrator would have to spend on configuring individual agent settings. In Figure 18 - Individual Agent Settings all the settings are grayed out; this is because the global settings template is being used. If one or more leaf agents need different settings then the “Use Global Agent Settings” may be unchecked. Each Leaf Agent installation can be configured to customized settings if the Global template does not meet the needs of the particular desktop.

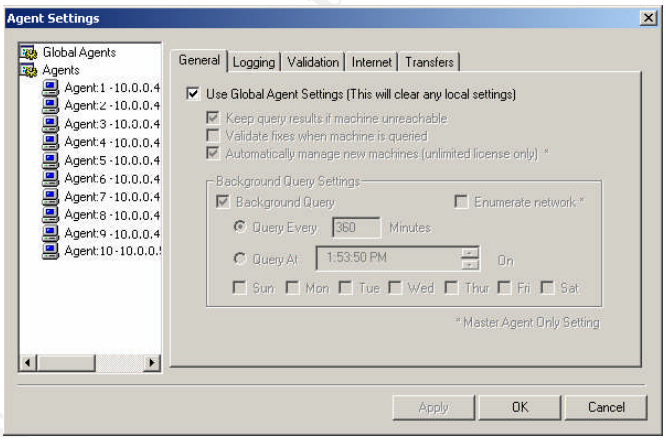



**Figure 18 - Individual Agent Settings**

In Figure 19 - Individual Agent Settings, the tabs Language, Updates, Authentication, and Repository are missing because these were settings that the Master Agent uses. The majority of the settings that are applied with the Global Template will be used to minimize the amount of configuration needed. The laptops will have a slightly different configuration so a separate group was configured for them. These settings will reduce the amount of bandwidth used when connecting remotely. To make the configuration changes to the laptops first, uncheck “Use Global Agent Settings” in the General Tab, uncheck “Background Query Settings” in the Transfer tab, and uncheck “Allow download even when connection speed is 56k or less.” The reason for this

change is so if a user connects to the internet via 56k or less, the UE agent will not use up any of the limited bandwidth the user has. In the event there is a critical patch that is needed immediately the user will be contacted and the patch will be deployed.

When the leaf agent templates are changed they will automatically be updated as often as needed but by default the setting is 360 minutes. Figure 19 - Applied Agent Settings is a list of configurations that was set in the corresponding tabs:

---

1. General –
    a. Validate fixes when desktop is queried
    b. Background Query

2. Logging –
    a. Log Queries
    b. Log Authentications
    c. Log Validation

3. Validation –
    a. Versions Match Exactly
        i. Check Size
        ii. Check Checksum

4. Internet – No Changes

5. Transfers –
    a. Concurrent transfers: 10
    b. Maximum transfer bandwidth usage: Unlimited
    c. Download files from master agent
    d. Allow UpdateEXPERT to download patches to this computer
    e. Allow downloads even when connection speed is 56k or less.

6. Language Options – No Changes

7. Updates –
    a. Automatically update database and software
    b. Check database settings every 360 Minutes

8. Authentication –
    a. Agent User – User System Context

9. Repository –
    a. Change repository to c:\UpdateExpert\Patches

---

**Figure 19 - Applied Agent Settings**

These final settings complete the installation and configuration of all the centralized management utilities. The Administrators will now deploy the baseline to the clients.

## *Deploy baseline*

Now that the changes to the baseline were completed, the Administrators could deploy the baseline to all the client desktops and laptops. The Administrators were using Symantec Ghost (7.5)[25] multicast sessions to deploy Ghost images to the desktops. The Administrators also used Microsoft's free utility SYSPREP[26] and included an answer file to eliminate the need for someone to walk through the installation as the desktops booted up. The Author felt this was a quick and efficient method and did not recommend any changes.

## *Upgrade Windows 2000 to Windows XP*

Before the deployment of the new baseline, there were still a few machines that were running Windows 2000 (SP4) that the Author recommended upgrading. The reason the Author recommended the upgrade is because there are some features within Windows 2003 AD that will not work on Windows 2000 such as not allowing specified files to be executed or only allowing specified applications to be executed. In addition to the lack of control from AD the Administrators may decide to use Remote Desktop to administer a desktop which is not offered in Windows 2000.

## *Perform final scan*

To verify that all the desktops had been updated with the baseline and were configured with the target configuration a scan was performed. This scan was only performed on the interior of the network. First the Administrators and Networking group (NTA) were notified that the scan would take place. The scan that was performed used the same utility as used in the initial scans (Nmap).

### Analyze output from scanner

After reviewing the output from the scan the Author had found a port had been opened at some point in deploying the desktops. The port that was opened was 427/TCP svrloc. Figure 20-Final Scan Output is a sample of the output performed in the scan.

---

Starting nmap 3.50 ( http://www.insecure.org/nmap/ ) at 2004-04-07 19:35 EDT

---

[25] For more information about Symantec Ghost 7.5 please see <http://service1.symantec.com/SUPPORT/ghost.nsf/8477deaaaafc102288256b1e00704619/ab822ed852dc4b7b88256a5c007b8962?OpenDocument&src=bar_sch_nam>

[26] Microsoft Corporation "Windows XP Service Pack 1 Deployment Tools" <http://www.microsoft.com/downloads/details.aspx?FamilyID=7a83123d-507b-4095-9d9d-0a195f7b5f69&DisplayLang=en> (August 29, 2002)

```
Interesting ports on desktop35.giac.edu (10.0.0.35):
 (The 1647 ports scanned but not shown below are in state: closed)
PORT      STATE    SERVICE      VERSION
21/tcp    filtered ftp
135/tcp   open     msrpc        Microsoft Windows msrpc
139/tcp   open     netbios-ssn
445/tcp   open     microsoft-ds Microsoft Windows XP microsoft-ds
427/tcp   open     svrloc?
1025/tcp  open     msrpc        Microsoft Windows msrpc
1032/tcp  open     msrpc        Microsoft Windows msrpc
5000/tcp  open     upnp         Microsoft Windows UPnP
Device type: general purpose
Running: Microsoft Windows 95/98/ME|NT/2K/XP
OS details: Microsoft Windows Millennium Edition (Me), Windows 2000 Professional or Advanced Server, or
Windows XP, Microsoft Windows XP SP1
------------------------------------------------------------------------------
```

**Figure 20-Final Scan Output**

The Author did some research and determined that the opened port had surfaced due to the installation of the Novell Client. This client had apparently been installed after the Author had configured the baseline. This open port was acceptable since it was needed to be able to connect to the Netware 5.1 server. This completes the final configurations of all the centralized management utilities.

## Case Study Environment After

In this case study the Administrators identified the need to centrally administer the security of all the desktops. The Author feels that he found the most suitable solution for the GIAC Institution that would give the Administrators the ability to centrally administer most of the high risk areas for a minimal cost.

The Administrators can now spend more time completing customers' requests as opposed to visiting each desktop to apply security updates, AntiVirus updates, and installing patches. The Staff and Engineers have also benefited from this centralized management such that the Administrators are no longer occupying their computer.

The overall security was enhanced in quite a few different ways. First, the patch management was converted from decentralized to centralized. Also there was no record of which desktop was patched or when it was patched. This was fixed with the utility UpdateEXPERT 6.2. UpdateEXPERT minimized the challenge of scheduling time with Staff and Engineers to visit each and every desktop. This increased the availability of the desktops to the users and minimized the amount of time the Administrators spent installing patches, UE also added the needed reporting to aid in diagnosing problems after installing patches. This centralized management of patches reduced the total amount of time the vulnerability resided the desktop from days or weeks to minutes.

The problem with centrally administering virus definitions and alerting the Administrators when a client found a virus was fixed with a few utilities. These utilities

include Symantec System Center Console (SSCC), Alert Management System (AMS) and Symantec AntiVirus (SAV) server which gave the Administrators the ability to push out Intelligent Updates, configure client settings centrally and most importantly to be alerted when a virus was found on a desktop. The automation of the Intelligent Updates minimized the 1 – 2 day lag between the time Symantec released the Intelligent Updates and Live Update definitions. The Administrators will also use the SSCC to make sure that all the desktops are running the latest version of the AntiVirus software available and verify their definitions are up to date.

The problem with applying security settings on each workstation manually was resolved with by setting up Windows 2003 running an Active Directory Domain and configuring GPO's. The AD Domain in conjunction with the Group Policy Management Console (GPMC) minimized the time the Administrators had to visit the user's workstation. The GPMC allowed the Administrators to easily view the policies that were applied in a format that is very readable. The GMPC also allows the Administrators to save the current settings in HTML and XML format for analysis at a later time. The combination of the Active Directory Domain with the GMPC further reduced the workload on the Administrators and enhanced the overall security of the desktops.

There are still vulnerabilities with this network as with most other networks such as there are minimal defenses to a 0 day exploit dependant on the attack vector. The steps that were performed to minimize this vulnerability were disabling as many services as possible, minimizing the installation of the desktops, and limiting user access. These modifications will also minimize the inadvertent or intentional installation of P2P software, spyware, and malware. The Author also gave the Administrators some links to websites and mailing lists so they can keep up to date with their security practices and be notified if there are any measures to take in the event that malicious code spread throughout the internet.

In conclusion the Author feels that the most efficient system was put in place within the cost constraints. The vulnerabilities were minimized by virtue of the management utilities that were setup to reduce the amount of visits to the desktops. These utilities accomplished 4 important tasks: increased the user's availability to the computers, decreased the workload on Administrators, provided documentation about systems configurations, and increased the overall security of desktops.

## References

SANS Institute "SANS Top 20"
<http://www.sans.org/top20/> (October 8, 2003)

Microsoft Corporation "Microsoft Security Bulletin MS00-078"
<http://www.microsoft.com/technet/security/bulletin/MS00-078.mspx>. (October 17, 2000)

Symantec Corporation ”For more information about the Nimda worm please see <http://securityresponse.symantec.com/avcenter/venc/data/w32.nimda.a@mm.html>. (*February 01, 2004)*

Microsoft Corporation “Microsoft Security Bulletin MS02-39 please see <http://www.microsoft.com/technet/security/bulletin/MS02-039.mspx>. (January 31, 2003)

Symantec Corporation ”For more information about the SQL Slammer worm please see <http://securityresponse.symantec.com/avcenter/venc/data/w32.sqlexp.worm.html>. (*June 06, 2004)*

Microsoft Corporation “Microsoft Security Bulletin MS03-026 please see <http://www.microsoft.com/technet/security/bulletin/MS03-026.mspx>. (September 10, 2003)

Symantec Corporation ”For more information about Blaster please see <http://securityresponse1.symantec.com/sarc/sarc.nsf/html/w32.blaster.worm.removal.tool.html>. (*April 1, 2004)*

Microsoft Corporation “Microsoft Security Bulletin MS04-011 please see <http://www.microsoft.com/technet/security/bulletin/MS04-011.mspx>. (May 4, 2004)

Symantec Corporation ”For more information about SASSER please see <http://securityresponse.symantec.com/avcenter/venc/data/w32.sasser.worm.html>. (*May 26, 2004)*

Microsoft Corporation “Microsoft's Best Practices (Least Privileges)” <http://www.microsoft.com/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/Default.asp?url=/resources/documentation/WindowsServ/2003/enterprise/proddocs/en-us/sag_seconceptsbp.asp>. (No Date Available)

Kathy Ivens “Securing the Administrator Account” <http://www.winnetmag.com/Windows/Article/ArticleID/40721/40721.html>. (December 2003)

Microsoft Corporation “Windows XP Security Guide” <http://www.microsoft.com/downloads/details.aspx?FamilyId=2D3E25BC-F434-4CC6-A5A7-09A8A229F118&displaylang=en>. (January 24, 2004)

Symantec Corporation ”How to automatically update Symantec AntiVirus Corporate Edition 8.x definitions without using Live Update” <http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2002091816510548?Open&src=ent&docid=2002103012571948&nsf

=ent-security.nsf&view=9d94c8571a91ba4788256bf3007f62b5&dtype=corp&prod=Symantec%20AntiVirus%20Corporate%20Edition&ver=8.x&osv=&osv_lvl=>. (4 April 2004).

Symantec Corporation “When to use the Intelligent Updater instead of Live Update” <http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713?OpenDocument&src=sec_web_nam>. (May 28, 2004)

St. Bernard Software “UpdateEXPERT Supported patches that can be managed” <http://www.stbernard.com/products/docs/ue_supported_patches.pdf>

St. Bernard Software “What kind of encryption does UpdateEXPERT use” <http://www.stbernard.com/products/support/updateexpert/uetechfaqs/UpdateEXPERT6.x/DMZ/UE0072.htm> (No Date Available)

St. Bernard Software - Pg 4 in UpdateEXPERT Deployment Guide <http://www.stbernard.com/products/docs/ue_deployguide.pdf>

Microsoft Corporation "Group Policy Management Console" <http://www.microsoft.com/downloads/details.aspx?FamilyID=c355b04f-50ce-42c7-a401-30be1ef647ea&DisplayLang=en>. (November 21, 2003)

Jim Lundy, Microsoft Corporation “Administering Group Policy with Group Policy Management Console” <http://www.microsoft.com/windowsserver2003/gpmc/gpmcwp.mspx>. (April 2003)

Microsoft Corporation “Windows 2003 Technical Reference” <http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/?frame=true>. (No Date Available)

## Figure References